Valutazione di impatto
Data Protection Impact Assessment (DPIA)

Ente	**Azienda ULSS 3 Serenissima**

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

Nome del trattamento	**Studi osservazionali o sperimentazioni cliniche con farmaco, dispositivo medico o altro ("Ricerca")**

21/01/2026

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

Versione 2026.01

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. 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).

Art. 35 par. 3 GDPR	**Check**	**Note**
Viene svolta una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche	NO	
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	SI	possibile in alcuni studi
Viene svolta una sorveglianza sistematica su larga scala di una zona accessibile al pubblico	NO	

Art. 35 par. 4 GDPR - All. 1 provv. Garante n. 467 11/10/2018 [doc. web n. 9058979]	**Check**	**Note**
1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"	NO	
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull' interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi)	NO	
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.	NO	
4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti)	SI	possibile in alcuni studi
5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8)	NO	
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)	SI	
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01	SI	possibile in alcuni studi
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.	SI	possibile in alcuni studi
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment)	SI	
10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse	SI	possibile in alcuni studi
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento	NO	
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	SI	possibile in alcuni studi

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
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 della **RICERCA SCIENTIFICA** nella sua accezione più ampia, condotta dall'Ente nei limiti ed in attuazione dei suoi compiti istituzionali, sia nel caso in cui sia Promotore dello Studio, sia che svolga la funzione di Centro Partecipante o Sperimentale dello Studio. La DPIA si applica, per richiamo, anche all'attività svolta dagli Sperimentatori Principali (PI). 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") e simili, comprendendo, salva diversa valutazione che l'Ente si riserva di condurre: 1) studi sperimentali ed interventistici (ad es. di farmaco/di dispositivo); 2) studi osservazionali (retrospettivi/prospettici). Tendenzialmente, il singolo Studio viene valutato e considerato in relazione: - alla finalità che persegue, come da Protocollo; - alla raccolta o meno del consenso per la conduzione dello Studio: nel quale ultimo caso l'Ente si riferisce alla disciplina normativa specificamente prevista per tale caso (vedi sezione specifica).						
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 ritiene opportuno procedere, preliminarmente, con una **valutazione di impatto unica**, avente ad oggetto trattamenti simili che presentino rischi analoghi. 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. [...] 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." A tale proposito, i trattamenti cui si riferisce il presente documento riguardano tutti attività di **RICERCA**, nell'accezione sopra descritta, nei limiti ed in attuazione dei compiti istituzionali dell'Ente. I trattamenti sono quindi considerati, in quest'ottica, 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 un'unica valutazione di impatto. Laddove i rischi fossero viceversa diversi e disomogenei per taluni Studi in particolare, 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, che andrà ad affiancarsi in profondità alla presente DPIA. **Ciò, in particolare, laddove gli Studi si riferiscano, in tutto o in parte, ad interessati per cui non è stato raccolto il consenso, per cui una DPIA specifica potrà accompagnare la presente DPIA unica, potendo la presente nondimeno restare valida ed efficace quale valutazione di impatto di tipo trasversale.**						
Finalità		Studi e sperimentazioni cliniche.	Ricerca medica, biomedica ed epidemiologica.	Ricerca scientifica.	Finalità di interesse pubblico e sanità pubblica.	Come da Protocollo.		
Dati trattati		DCOM: dati anagrafici	DCOM: codice fiscale	DPART: dati relativi alla salute		DPART: dati genetici	Ogni altro dato necessario alla conduzione dello Studio secondo il Protocollo.	
Interessati coinvolti		Pazienti	Minori	Persone Fragili	Caregiver	Volontari sani		
Interesse legittimo (se applicabile)	**Non Applicabile (N/A)**							
Destinatari		Dipendenti ed altri incaricati interni	Comitato Etico/Autorità regolatorie	Promotore	Centro Partecipante / Sperimentale	Vanderbilt University (REDCap)	Eventuali responsabili del trattamento/ Altri, se e come da Protocollo.	La comunicazione e il trasferimento dei dati per i trattamenti connessi alla presente valutazione d' impatto può avvenire previa sottoscrizione di un accordo specifico e comunque, in coerenza con quanto previsto dalla normativa vigente e pattuito nel protocollo di Ricerca.
Periodo di conservazione		fino all'obbligo di legge, come da Protocollo	5 anni	7 anni	25 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 è meglio definito e descritto nel singolo Protocollo di Ricerca che deve intendersi parte integrante della presente DPIA.	In linea generale l'attività di Ricerca prenderà in esame i dati personali, compresi i dati di natura particolare, raccolti attraverso varie fonti, tra cui: a) interessati; b) cartelle cliniche ed ambulatoriali; c) database e applicativi; d) open data; e) dataset prodotti da soggetti pubblici o privati, nazionali o internazionali; f) database interni ed esterni; g) biobanche; h) applicativi informatici; i) dispositivi elettronici.	In ossequio alle procedure e ai regolamenti Aziendali, il riconoscimento dei soggetti reclutati avviene attraverso sistemi tradizionali, quali ad esempio la carta di identità o altro documento di riconoscimento. Negli studi retrospettivi l' identificazione può essere effettuata anche attraverso codificazioni derivanti da numeri nosologici o codici di pseudonimizzazione assegnati in fase di rilevazione e registrati in appositi Database.	Nelle ricerche che coinvolgono più di un centro partecipante/collaborante (ad es. negli studi multicentrici) il coinvolgimento di altri soggetti pubblici o privati può essere regolato da atti giuridici che definiscono compiti e responsabilità. L'attività di Ricerca di tipo multicentrico prevede la partecipazione di soggetti pubblici o privati (anche appartenenti a enti no profit e di volontariato) nelle modalità previste dal protocollo di Ricerca	Saranno osservati gli standard normativi previsti per il settore, nonché le eventuali integrazioni richieste dal Comitato Etico.		
Risorse utilizzate		Sistemi Informativi Aziendali.	Piattaforma REDCap (Vanderbilt University)	Altre risorse come da Protocollo				
Codici di condotta (se applicabile)	**Non Applicabile (N/A)**	Non vi sono codici di condotta, ma standard normativi (vedi sotto).						
		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	

Standard o Linee Guida applicabili	**Applicabile**	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?	**DIPENDE**	Negli studi senza consenso è già presente la valutazione di un Comitato Etico e la consultazione non aggiungerebbe informazioni utili alla DPIA.	Negli studi con consenso la consultazione può essere svolta in via preliminare.					
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, ivi compresi gli standard applicabili e le linee guida.						

Necessità e Proporzionalità

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	Le finalità di ogni trattamento sono specificamente indicate dal Protocollo e meglio esplicitate nell'informativa.	La finalità è l'obiettivo perseguito dallo Studio che viene condotto, come da Procollo.	La finalità è la conduzione della Ricerca medica, biomedica ed epidemiologica, a seconda del Protocollo.	La finalità è la conduzione dell'attività di Ricerca scientifica, a seconda del Protocollo.	La finalità è il perseguimento dell'interesse pubblico e di sanità pubblica, a seconda del Protocollo.		
Il trattamento è lecito (art. 6 GDPR + art. 9 GDPR se applicabile)?	SI	Vedi celle qui sotto						
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. 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 Codice Privacy:** Il consenso non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione ed è condotta e resa pubblica una valutazione di impatto. Inoltre non è 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 della 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. 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, standone comunicazione al Garante.	Il consenso dell'interessato non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea. Negli altri casi, quando non è possibile acquisire il consenso degli interessati, i titolari del trattamento devono documentare, nel progetto di ricerca, la sussistenza delle ragioni, considerate dal tutto particolari o eccezionali, per le quali 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, tra le quali in particolare i seguenti.	1. I **motivi etici** riconducibili alla circostanza che l' interessato ignora la propria condizione. Rientrano in questa categoria le ricerche per le quali l'informativa sul trattamento dei dati da rendere agli interessati comporterebbe la rivelazione di notizie concernenti la condizione dello studio la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi (possono rientrare in questa ipotesi, ad esempio, gli studi epidemiologici sulla distribuzione di un fattore che predica o possa predire lo sviluppo di uno stato morboso per il quale non esista un trattamento).	2. I **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 e 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.	3. **motivi di salute riconducibili alla gravità dello stato clinico** in cui versa l'interessato a causa del quale questi è impossibilitato a comprendere le indicazioni rese nell' informativa e a prestare validamente il consenso. In tali casi, lo studio deve essere volto al miglioramento dello stesso stato clinico in cui versa l' interessato. Inoltre, occorre comprovare che la finalità dello studio non possano essere conseguite mediante il trattamento di dati riferiti a persone in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso o con altra metodologia di ricerca. Ciò, avuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché all' attendibilità dei risultati conseguibili in relazione alle specifiche finalità dello studio. Con riferimento a tali motivi, deve essere acquisito il consenso delle persone indicate nell' art. 82, comma 2, lett. a), del Codice come modificato dal d.lgs. n. 101/2018. Ciò, fermo restando che sia resa all'interessato l'informativa sul trattamento dei dati non appena le condizioni di salute glielo consentano, anche al fine dell'esercizio dei diritti previsti dal Regolamento.	In tali casi, il titolare del trattamento oltre ad adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, e acquisire il parere favorevole del competente comitato etico a livello territoriale sul progetto di ricerca come previsto dall'art. 110 del Codice, deve accuratamente motivare e documentare, nel progetto di ricerca, la sussistenza delle ragioni etiche o organizzative per le quali informare gli interessati e quindi acquisire il consenso, risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, se del caso documentando altresì i ragionevoli sforzi profusi per tentare di contattarli. Nei predetti casi, 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 del Regolamento, dandone comunicazione al Garante.**
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	SI	Art. 9.2.j) GDPR: il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, par. 1 GDPR, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l' essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell' interessato.	**art. 110-bis Codice Privacy:** 1. Il Garante può autorizzare il trattamento ulteriore di dati personali, compresi quelli dei trattamenti speciali di cui all'articolo 9 GDPR, a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività 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, a condizione che siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in conformità all'articolo 89 GDPR, comprese forme preventive di minimizzazione e di anonimizzazione dei dati. 2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del trattamento ulteriore dei dati personali da parte di terzi, anche sotto il profilo della loro sicurezza. 3. Il trattamento ulteriore di dati personali da parte di terzi per le finalità di cui al presente articolo può essere autorizzato dal Garante anche mediante provvedimenti generali, adottati d'ufficio e anche in relazione a determinate categorie di titolari e di trattamenti, con i quali sono stabilite le condizioni dell'ulteriore trattamento e prescritte le misure necessarie per assicurare adeguate garanzie a tutela degli interessati. I provvedimenti adottati a norma del presente comma sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana. 4. Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 GDPR.					
Studi che perseguono finalità di interesse pubblico e sanità pubblica	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.g) GDPR: il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell' Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;	Art. 9.2.j) GDPR: il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;	art. 2-sexies Codice Privacy	u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;	v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;	
I dati personali sono adeguati, pertinenti e limitati (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).				
La conservazione è limitata (art. 5, par. 1, lett. e GDPR)?	SI	Il periodo di conservazione dei dati di origine ripenda 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 della tempistiche valutate durante la stesura del progetto e in accordo alla normativa vigente. Il tempo di conservazione dei risultati e degli altri dati della Ricerca è indicato nel Protocollo.	5 anni	7 anni	25 anni		I dati contenuti nelle fonti, di cui sopra, seguono il ciclo di vita proprio definito dalla normativa di settore (massimario di scarto).	Ogni altro diverso termine di legge compatibilmente con il Protocollo.	
Le informazioni sono fornite all'interessato (art. 12, 13 e 14 GDPR)?	SI	Gli interessati sono informati mediante informativa resa 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 la 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 (art. 15 GDPR)?	SI	Il diritto può essere esercitato mediante richiesta specifica ai recapiti indicati nella informative. L'Ente rende riscontro entro un mese ai sensi dell'art. 12 GDPR, salvo proroga comunicata ai sensi e nei casi previsti dalla medesima disposizione.						
È garantito il il diritto di rettifica e/o integrazione (art. 16 GDPR)?	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 (art. 17 GDPR)?	SI	Il diritto può essere esercitato nei casi previsti dalla disposizione in oggetto, mediante richiesta specifica ai recapiti indicati nella 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 (art. 18 GDPR)?	SI	Il diritto può essere esercitato nei casi previsti dalla disposizione in oggetto, mediante richiesta specifica ai recapiti indicati nelle informative. L'Ente rende riscontro entro un mese ai sensi dell'art. 12 GDPR, salvo proroga comunicata ai sensi e nei casi previsti dalla medesima disposizione.						
È garantito il il diritto di portabilità (art. 20 GDPR)?	SI	Il diritto può essere esercitato nei casi previsti dalla disposizione in oggetto (in particolare, se lo Studio è condotto con il consenso dell'interessato), mediante richiesta specifica ai recapiti indicati nelle informative. L'Ente rende riscontro entro un mese ai sensi dell'art. 12 GDPR, salvo proroga comunicata ai sensi e nei casi previsti dalla medesima disposizione.						
È garantito il il diritto di opposizione (art. 21 GDPR)?	SI	Il diritto può essere esercitato nei casi previsti dalla disposizione in oggetto, mediante richiesta specifica ai recapiti indicati nelle informative. L'Ente rende riscontro entro un mese ai sensi dell'art. 12 GDPR, salvo proroga comunicata ai sensi e nei casi previsti dalla medesima disposizione.						
È garantito il diritto 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 nei casi previsti dalla disposizione in oggetto, mediante richiesta specifica ai recapiti indicati nelle informative. L'Ente rende riscontro entro un mese ai sensi dell'art. 12 GDPR, salvo proroga comunicata ai sensi e nei casi previsti dalla medesima disposizione.	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. 23/2025, 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.					
Sono osservate le regole previste per il trattamento dei dati personali da parte dei responsabili per conto del titolare (art. 28 GDPR)?	SI	Il trattamento svolto per conto del titolare da parte di uno o più responsabili del trattamento è soggetto alla stipula di un contratto di responsabile del trattamento ai sensi dell'art. 28 GDPR e secondo il contenuto previsto da tale disposizione						
Sono osservate le garanzie riguardanti trattamenti internazionali (capo V GDPR)?	SI	Si invoca il consenso dell'interessato, specificamente raccolto, se lo Studio si svolge sulla base giuridica del consenso.	Decisione di adeguatezza	Clausole contrattuali standard (SCC)	Regole vincolante di impresa (binding rules)	Data Privacy Framework EU-USA	Salvo sia prevista anonimizzazione.	Il tutto come previsto dal Protocollo.
È attivata la consultazione preventiva del Garante (art. 36 GDPR)?	N/A	La consultazione preventiva del Garante è attivata se ed in quanto si rientri nei casi di cui all'art. 36 GDPR.	Se lo Studio è svolto senza consenso nell'ambito dell'art. 110 Codice Privacy, della DPIA viene data comunicazione al Garante.					

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	
2	Allagamento	Ambientale	ID		2	3	6,000	
3	Crollo o altro fattore naturale/fisico	Ambientale	ID		2	3	6,000	
4	Furto di archivi o di singoli dati	Umana	RID		3	5	15,000	
5	Accesso non autorizzato	Umana	RI		3	4	12,000	
6	Comunicazione non autorizzata	Umana	R		3	4	12,000	
7	Diffusione non autorizzata	Umana	R		3	5	15,000	
8	Modifica dati non autorizzata	Umana	RID		3	5	15,000	
9	Distruzione dati non autorizzata	Umana	ID		3	5	15,000	
10	Perdita dati o dispositivo contenente dati	Umana	RID		3	4	12,000	
11	Diffusione credenziali accesso	Umana	R		3	4	12,000	
12	Vittima di phishing o altra manipolazione	Umana	RID		4	5	20,000	
13	Altro trattamento illecito doloso	Umana	RID		3	3	9,000	
14	Altro trattamento illecito colposo	Umana	RID		3	3	9,000	
15	Mancata soddisfazione dei diritti	Umana	RID		2	5	10,000	11,897
16	Cessazione rapporto / turnover	Umana	RID		2	3	6,000	
17	Attacco informatico	Tecnica	RID		4	5	20,000	
18	Virus informatico	Tecnica	RID		4	5	20,000	
19	Intromissione nel sistema	Tecnica	RID		4	5	20,000	
20	Danno tecnico informatico	Tecnica	RID		2	5	10,000	
21	Malfunzionamento informatico	Tecnica	RID		2	5	10,000	
22	Malfunzionamento tecnico	Tecnica	RID		2	4	8,000	
23	Altri fattori di divulgazione dati	Tecnica	R		3	4	12,000	
24	Altri fattori di corruzione dati	Tecnica	I		3	4	12,000	
25	Altri fattori di indisponibilità dei dati	Tecnica	D		3	4	12,000	
26	Mancata consapevolezza privacy	Organizzativa	RID		3	4	12,000	
27	Inosservanza principi/adempimenti privacy	Organizzativa	RID		3	4	12,000	
28	Carenza di personale/Turnover elevato	Organizzativa	RID		2	3	6,000	
29	Altre inefficienze organizzative	Organizzativa	RID		3	3	9,000	

RISCHIO INERENTE (ORIGINARIO)	MEDIO

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	**MEDIO**												
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	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 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	4,500
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	
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	4,125
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	
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	4,000
H.2	È 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	
H.4	È 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	

#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
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	4,500
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	È 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	È prevista l'autenticazione a due fattori	Medio	SI	Verifica doppio passaggio (two-step verification - verifica a due fattori)									5	
K.8	Sono previste forme di autenticazione del dispositivo in rete	Alto	SI	Controllo degli accessi logici									5	
L	**Registrazione e monitoraggio**													
L.1	Si provvede all'eventuale registrazione dei file di log, nel rispetto del divieto di controllo a distanza dei lavoratori laddove applicabile (art. 4 Statuto dei Lavoratori Legge 300/1970)	Basso	SI	Misure di tracciabilità (log etc.)									4	4,300
L.2	Sono previste modalità di protezione dei file di registro, contrassegnati con data e ora, da manomissioni e accessi non autorizzati. Criteri di determinazione dell'ora (UTC)	Basso	SI	Controllo degli accessi logici									4	
L.3	Si provvede all'eventuale registrazione degli accessi e degli interventi degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta/cancellazione/modifica dei diritti utente	Medio	SI	Misure di tracciabilità (log etc.)									4,5	
L.4	Sono previste eventuali procedure per l'integrità dei file di log	Medio	SI	Procedure per assicurare la riservatezza, l'integrità, la disponibilità dei dati (RID)									4,5	
L.5	Sono previsti eventuali alert per le manomissioni dei sistemi di registrazione degli accessi	Medio	SI										4,5	
M	**Sicurezza server / database**													
M.1	Sono previste modalità di configurazione dei server; privilegi di accesso	Basso	SI	Nomina amministratore sistema									4	4,250
M.2	Sono previsti criteri per la minimizzazione dei dati trattati nei server	Basso	PARZIALMENTE										3	
M.3	Sono previste eventuali soluzioni di crittografia su file o cartelle specifiche	Medio	SI	Pseudonimizzazione / Cifratura / Crittografia	Anonimizzazione								4,5	
M.4	È 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	È 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	

#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
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	
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	4,333
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	
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	2,944
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	
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	3,417
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	È indicato il luogo di distruzione di supporti o archivi cartacei (qualora si utilizzino 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 APPLICAZIONE PROTOCOLLI	**4,034**

Matrice Protocolli-Minacce

#ID	PROTOCOLLI \ 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
		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	Sono predisposte misure per la revoca dei diritti e delle responsabilità per l'accesso degli operatori al sistema informativo, con le rispettive procedure, per il caso di assenza temporanea o definitiva dell'operatore					4					4			4	4	4	4											4	4	4
B.3	Sono nominate le persone incaricate ai compiti di sicurezza specifici, compresa quella di un responsabile della sicurezza					4,5					4,5	4,5	4,5	4,5	4,5			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
C.2	Sono previste misure di sicurezza per la concessione dei diritti di accesso degli operatori al sistema informativo e restrizioni per ruoli utente specifici				4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5			4,5			4,5		4,5		4,5	4,5	4,5		4,5		4,5
C.3	Sono previste eventuali misure di sicurezza per la segregazione dei ruoli di controllo degli accessi (ad es. richiesta di accesso, autorizzazione all'accesso, amministrazione dell'accesso)				4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5			4,5			4,5		4,5		4,5	4,5	4,5		4,5		4,5
C.4	Sono definiti e assegnati a membri del personale specifici e limitati ruoli con diritti di accesso di sistema				5	5	5	5	5	5		5		5			5			5		5		5	5	5		5		5
D	**Gestione delle risorse**																													
D.1	Esiste un inventario dell'infrastruttura hardware (server, pc etc.), software (gestionali, applicativi, etc.) e di rete. L'inventario dovrebbe includere almeno le seguenti informazioni: risorsa informatica, tipo (es. server, postazione di lavoro), ubicazione (fisica o elettronica)	4	4	4							4						4	4	4	4	4	4	4	4	4	4		4		4
D.2	Le risorse IT sono oggetto di revisione e aggiornamento regolare	4	4	4							4						4	4	4	4	4	4	4	4	4	4		4		4
D.3	Sono previste eventuali misure di sicurezza e procedure per la definizione dei ruoli di accesso alle varie componenti dell'infrastruttura	4,5	4,5	4,5							4,5						4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5		4,5		4,5
D.4	Le risorse IT sono oggetto di revisione e aggiornamento su base annuale	5	5	5							5						5	5	5	5	5	5	5	5	5	5		5		5
E	**Cambio di gestione**																													
E.1	Sono previste procedure applicate per le modifiche al sistema IT: regole di registrazione e monitoraggio delle modifiche								4	4	4			4	4		4	4	4	4	4	4	4	4	4	4		4		4
E.2	Sono previste eventuali procedure per lo sviluppo di software, se applicabile																													
E.3	Sono previste eventuali regole per il cambio dell'operatore o per la sua definitiva cessazione: comunicazione ai mittenti della posta elettronica e simili					5	5				5	5		5			5											5	5	5
F	**Responsabili del trattamento**																													
F.1	Sono definite e documentate linee guida e procedure formali, concordate tra il titolare e il responsabile del trattamento prima dell'inizio delle attività, che devono obbligatoriamente seguire lo stesso livello di sicurezza dei dati personali					4									4	4											4	4	4	4
F.2	Sono previste tempistiche di informazione al titolare da parte del responsabile del trattamento in merito a una violazione dei dati personali				4	4	4	4	4	4	4	4	4	4	4	4		4	4	4	4	4	4	4	4	4	4	4	4	4
F.3	Si provvede a formale accordo tra il titolare e il responsabile del trattamento su requisiti e obblighi formali, previa fornitura documentale sufficiente di conformità da parte del responsabile del trattamento					4									4	4											4	4	4	4
F.4	È prevista regolare verifica della conformità del responsabile del trattamento (audit del responsabile del trattamento)					3									3	3		3	3	3	3	3	3	3	3	3	3	3	3	3
F.5	Sono previsti specifici accordi di riservatezza/non divulgazione ai dipendenti del responsabile del trattamento incaricati di elaborare dati					5									5	5		5	5	5	5	5	5	5	5	5	5	5	5	5
G	**Gestione degli incidenti / violazione dei dati pesonali**																													
G.1	Esiste un piano tecnico di disaster recovery e di risposta agli incidenti di sicurezza / violazioni, con relative procedure	3	3	3	3	3	3	3	3	3	3	3	3	3	3			3	3	3	3	3	3	3	3	3				
G.2	Sono previste procedure tecniche di alert per gli incidenti, le violazioni, le quasi-violazioni (near miss)	4	4	4	4	4	4	4	4	4	4	4	4	4	4			4	4	4	4	4	4	4	4	4				4
G.3	Esiste ed è documentato un piano di risposta agli incidenti, comprese possibili azioni di mitigazione e una chiara assegnazione dei ruoli	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5			4	4	4	4	4	4	4	4	4				4
G.4	Esiste un sistema di registrazione degli incidenti e delle violazioni dei dati personali insieme ai dettagli relativi all'evento e alle azioni di mitigazione eseguite	5	5	5	5	5	5	5	5	5	5	5	5	5	5			5	5	5	5	5	5	5	5	5				5
H	**Business continuity**																													
H.1	Sono previste misure di sicurezza per garantire il livello richiesto di continuità e disponibilità del sistema IT in caso di incidente/violazione dei dati	4	4	4	4	4	4	4	4	4	4	4	4	4	4			4	4	4	4	4	4	4	4	4		4		4
H.2	È previsto un piano tecnico di business continuity, con evidenza delle azioni ed assegnazione dei ruoli nel caso di evento pregiudizievole	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
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	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
H.4	È prevista la nomina di personale specifico con responsabilità, autorità e competenze necessarie per gestire la coninuità operativa in caso di incidente/violazione dei dati personali	5	5	5	5	5	5	5	5	5	5	5	5	5	5			5	5	5	5	5	5	5	5	5	5	5	5	5
H.5	È presente una struttura alternativa a seconda dell'organizzazione e del tempo di inattività accettabile del sistema IT	5	5	5	5						5			5				5	5	5	5	5	5	5	5	5			5	
I	**Riservatezza del personale**																													
I.1	Sono previste misure di comunicazione dei ruoli, delle responsabilità e degli obblighi relativi al trattamento dei dati personali, durante il processo di preassunzione e/o inserimento lavorativo					4	4	4	4	4	4	4	4		4	4	4										4	4	4	4
I.2	Esiste un impegno dei dipendenti al rispetto della politica di sicurezza dell'organizzazione e firma dei rispettivi accordi di riservatezza e non divulgazione, prima di assumere le proprie funzioni					4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5		4,5	4,5	4,5										4,5	4,5	4,5	4,5
I.3	Esiste un vincolo a specifiche clausole di riservatezza di dipendenti coinvolti nel trattamento ad alto rischio dei dati personali					5		5				5			5	5								5			5	5	5	5
J	**Formazione**																													
J.1	Sono previste regole tecniche di informazione ai dipendenti dei controlli di sicurezza del sistema IT che riguardano il loro lavoro quotidiano, nel rispetto del divieto di controllo a distanza dei lavoratori laddove applicabile (art. 4 Statuto dei Lavoratori Legge 300/1970)											4	4				4										4	4	4	4
J.2	Sono previsti eventuali programmi di formazione del personale					4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5		4,5	4,5	4,5										4,5	4,5	4,5	4,5
J.3	È previsto un piano di formazione con scopi e obiettivi definiti su base annua					5	5	5	5	5	5	5	5		5	5	5										5	5	5	5
K	**Controllo accessi e autenticazione**																													
K.1	Esisten un sistema di controllo degli accessi, che preveda la creazione, l'approvazione, la revisione e l'eliminazione degli account utente, nel rispetto del divieto di controllo a distanza dei lavoratori laddove applicabile (art. 4 Statuto dei Lavoratori Legge 300/1970)					4					4					4	4			4						4	4	4	4	4
K.2	Sono previste misure di sicurezza per l'eventuale uso di account utente comuni; regole applicative per la gestione da parte degli operatori che vi accedono					4	4					4				4	4							4			4	4	4	4
K.3	Sono previste procedure di autenticazione per l'accesso al sistema IT: utente/password o altre forme di autenticazione				4	4								4				4	4	4	4	4	4	4	4	4	4	4	4	4
K.4	Sono previste misure di sicurezza per impedire l'uso di password non complesse				4	4								4				4	4	4	4	4	4	4	4	4	4	4	4	4
K.5	Sono previste eventuali regole di composizione della password: lunghezza della password, complessità, periodo di validità e numero di tentativi di accesso non riusciti accettabili				4,5	4,5								4,5						4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
K.6	Si provvede alla 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
K.7	È prevista l'autenticazione a due fattori				5	5								4				4	4	4	4	4	4	4	4	4	4	4	4	4
K.8	Sono previste forme di autenticazione del dispositivo in rete				5	5								5						5				5	5		5	5	5	5
L	**Registrazione e monitoraggio**																													
L.1	Si provvede all'eventuale registrazione dei file di log, nel rispetto del divieto di controllo a distanza dei lavoratori laddove applicabile (art. 4 Statuto dei Lavoratori Legge 300/1970)				4	4	4	4	4	4				4				4	4	4	4			4			4	4	4	4
L.2	Sono previste modalità di protezione dei file di registro, contrassegnati con data e ora, da manomissioni e accessi non autorizzati. Criteri di determinazione dell'ora (UTC)					4			4	4				4										4	4			4		4
L.3	Si provvede all'eventuale registrazione degli accessi e degli interventi degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta/cancellazione/modifica dei diritti utente					4,5			4,5	4,5				4,5				4,5	4,5	4,5	4,5			4,5	4,5			4,5		4,5
L.4	Sono previste eventuali procedure per l'integrità dei file di log					4,5			4,5	4,5				4,5				4,5	4,5	4,5	4,5			4,5	4,5			4,5		4,5
L.5	Sono previsti eventuali alert per le manomissioni dei sistemi di registrazione degli accessi					4,5			4,5	4,5		4,5		4,5				4,5	4,5	4,5	4,5			4,5	4,5			4,5		4,5
M	**Sicurezza server / database**																													
M.1	Sono previste modalità di configurazione dei server; privilegi di accesso					4			4	4				4						4	4			4	4	4		4		4
M.2	Sono previsti criteri per la minimizzazione dei dati trattati nei server															3				3				3			3	3		3
M.3	Sono previste eventuali soluzioni di crittografia su file o cartelle specifiche				4,5	4,5	4,5	4,5				4,5	4,5	4,5	4,5		4,5	4,5		4,5				4,5				4,5	4,5	4,5
M.4	È prevista l'eventuale crittografia delle unità di archiviazione				4,5	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
M.5	Sono previste eventuali tecniche di pseudonimizzazione, laddove applicate				4,5	4,5	4,5	4,5				4,5	4,5	4,5	4,5		4,5	4,5		4,5				4,5				4,5	4,5	4,5
M.6	Sono previste tecniche di database che supportano la privacy (es. query autorizzate, crittografia ricerca, ecc.)				5	5	5	5				5	5	5	5		5	5		5				5				5	5	5
N	**Sicurezza della postazione di lavoro**																													
N.1	Sono previste misure di sicurezza per impedire agli operatori di disattivare o ignorare le impostazioni di sicurezza				4	4	4	4	4	4				4	4				4			4	4	4	4	4	4	4		4
N.2	Esistono sistemi e strumenti antivirus, firewall ed altre misure di sicurezza analoghe				4	4							4	4					4	4	4	4		4	4	4				4
N.3	Sono previste regole per non permettere agli operatori di disporre di privilegi per installare o disattivare applicazioni software non autorizzate												3	3				3	3	3	3	3	3	3	3	3	3	3		3
N.4	Si provvede al timeout di sessione per l'assenza temporanea dell'operatore (screensaver)				3	3					3	3		3						3	3	3	3	3				3	3	3
N.5	Si provvede ad aggiornamenti di sicurezza critici				4	4								4				4	4	4	4	4	4	4	4	4	4	4	4	4
N.6	È prevista una frequenza nella configurazione di antivirus				4,5													4,5	4,5	4,5	4,5	4,5		4,5	4,5	4,5				
N.7	Sono previste eventuali misure tecniche per impedire l'archiviazione di informazioni su dispositivi esterni (es. USB, DVD, dischi rigidi esterni)				3	3	3	3						3			3										3	3	3	3
N.8	Sono previste eventuali misure per la restrizione dell'accesso ad internet												5	5	5												5	5	5	5
N.9	Si provvede alla crittografia completa sulle unità centrali del sistema operativo				5	5	5	5			5	5	5	5	5			5	5	5				5				5	5	5
O	**Sicurezza di rete / comunicazione**																													
O.1	Sono previste misure di crittografia tramite protocolli TLS/SSL per l'accesso ad Internet												4	4	4			4		4				4				4	4	4
O.2	Sono previste eventuali regole per l'attivazione dell'accesso wireless al sistema IT				4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5		4,5	4,5					4,5				4,5			4,5	4,5	4,5	4,5
O.3	Sono previste eventuali misure per l'accesso remoto al sistema informatico (ad es. VPN per smart working o simili)				4,5	4,5	4,5	4,5						4,5	4,5		4,5			4,5				4,5			4,5	4,5	4,5	4,5
O.4	Sono previsti strumenti firewall e sistemi di rilevamento delle intrusioni				4,5	4,5	4,5	4,5						4,5	4,5		4,5			4,5				4,5			4,5	4,5	4,5	4,5
O.5	Sono previste modalità di blocco della connessione ad internet alle postazioni utilizzate per il trattamento dei dati personali				1	1	1	1			1	1	1	1	1			1	1	1	1	1	1	1	1	1	1	1		1
O.6	Sono previste misure di segregazione della rete informatica				5	5	5	5			5	5	5	5	5			5	5	5	5	5	5	5	5	5	5			5
O.7	Si abilita l'accesso al sistema IT mediante tecniche di pre-autorizzazione quali il filtraggio MAC o il Network Access Control (NAC)				1	1								1						1				1			1			
P	**Backup**																													
P.1	Sono previste procedure 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
P.2	Sono previste regole di custodia e di protezione fisica ed ambientale delle strutture e dei supporti di backup	4	4	4	4					4	4		4	4	4	4	4	4	4	4	4	4	4		4	4	4	4	4	4
P.3	Sono previste regole di monitoraggio per la corretta esecuzione dei backup	4	4	4	4					4	4		4	4	4	4	4	4	4	4	4	4	4		4	4	4	4	4	4
P.4	Esiste una frequenza nell'esecuzione dei backup	4	4	4	4					4	4		4	4	4	4	4	4	4	4	4	4	4		4	4	4	4	4	4
P.5	Sono previsti eventuali test dei supporti di backup per l'utilizzo in caso di emergenza	4,5	4,5	4,5	4,5					4,5	4,5		4,5	4,5	4,5	4,5	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
P.6	Esiste una frequenza dei backup incrementali	4,5	4,5	4,5	4,5					4,5	4,5		4,5	4,5	4,5	4,5	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
P.7	Sono previste modalità di archiviazione delle copie del backup	4,5	4,5	4,5	4,5					4,5	4,5		4,5	4,5	4,5	4,5	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
P.8	Sono previsti eventuali servizi di terze parti per attività di backup	4,5	4,5	4,5	4,5					4,5	4,5		5	5	5	5	5	5	5	5	5	5	5		4,5	4,5	4,5	4,5	4,5	4,5
P.9	Sono previste eventuali procedure di crittografia ed archiviazione offline dei backup	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**																													
Q.1	Sono previste misure di sicurezza per l'accesso dei dispositivi mobili e portatili al sistema IT				4	4	4	4	4	4	4	4		4	4		4	4	4	4	4	4	4	4			4	4	4	4
Q.2	Si provvede all'eventuale pre-registrazione dei dispositivi mobili per l'accesso al sistema IT				1	1	1	1	1	1	1	1		1	1		1	1	1	1	1	1	1	1			1	1	1	1
Q.3	Sono previste regole per i livelli di protezione dei dispositivi mobili utilizzati in ambito aziendale					1	1	1				1	1	1	1												1	1	1	1
Q.4	Sono previste modalità di definizione di ruoli e responsabilità specifici per la gestione dei dispositivi mobili e portatili					4,5	4,5	4,5				4,5	4,5	4,5	4,5												4,5	4,5	4,5	4,5
Q.5	Sono previste eventuali misure per la cancellazione da remoto dei dati aziendali su dispositivi mobili												1				1										1	1	1	1
Q.6	Sono previste eventuali misure per la separazione dell'uso privato da quello aziendale nei dispositivi personali mobili												4,5				4,5										4,5	4,5	4,5	4,5
Q.7	Sono previste eventuali misure per il caso di smarrimento/furto dei dispositivi mobili				4,5	4,5					4,5	4,5		4,5													4,5	4,5	4,5	4,5
Q.8	Si provvede all'eventuale autenticazione a due fattori nei dispositivi mobili				3	3	3	3	3	3	3	3		3						3				3	3		3	3	3	3
Q.9	Sono previste forme di crittografia dei dati aziendali nei dispositivi mobili				3	3	3	3	3	3	3	3		3						3				3			3	3	3	3
R	**Sicurezza del ciclo di vita delle applicazioni**																													
R.1	Sono previste misure di aggiornamento delle applicazioni e dei software in generale				4							4	4	4				4	4	4	4	4		4	4	4				4
R.2	Sono previsti requisiti di sicurezza specifici per le applicazioni ed i software in generale				4							4	4	4				4	4	4	4	4		4	4	4				4
R.3	Sono adottate tecnologie e tecniche specifiche per supportare la privacy e la protezione dei dati in analogia ai requisiti di sicurezza				4	4	4	4	4	4	4	4	4	4	4	4	4										4	4	4	4
R.4	Sono previsti standard e pratiche di codifica sicura				3			3			3	3	3	3				3	3	3	3	3		3			3	3	3	3
R.5	Si provvede a test e strumenti di convalida sull'implementazione dei requisiti di sicurezza iniziali				3						3	3		3				3	3	3	3	3		3	3	3				
R.6	Sono previsti test di vulnerabilità e di penetrazione delle applicazioni, dei software e dell'infrastruttura IT in generale					4,5	4,5	4,5	4,5	4,5				4,5				4,5	4,5	4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
R.7	Si provvede con una certa frequenza ai test di penetrazione					3	3	3	3	3				3				3	3	3				3	3	3	3	3	3	3
R.8	Sono previste modalità di ottenimento delle informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati					3	3	3	3	3				3				3	3	3				3	3	3	3	3	3	3
R.9	Si provvede a test e valutazioni delle patch software prima dell'installazione					4,5	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**																													
S.1	Sono previste misure per la distruzione dei dati contenuti nei dispositivi e supporti IT destinati allo smaltimento					4	4	4		4						4								4		4	4	4	4	4
S.2	Sono previste modalità di distruzione dei documenti cartacei e dei supporti portatili utilizzati per la memorizzazione dei dati personali					1	1	1		1						1											1	1	1	1
S.3	Si provvede alla sovrascrittura dei software su tutti i supporti prima di essere eliminati					1				1	1	1				1											1	1	1	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)					4,5				4,5	4,5	4,5				4,5											4,5	4,5	4,5	4,5
S.5	Si provvede alla smagnetizzazione dell'hardware dopo la cancellazione del software (se necessario anche distruzione fisica)					5				5	5	5				5											5	5	5	5
S.6	È indicato il luogo di distruzione di supporti o archivi cartacei (qualora si utilizzino fornitore esterni del servizio quali responsabile del trattamento)					5				5	5	5				5											5	5	5	5
T	**Sicurezza fisica**																													
T.1	Sono previste misure di protezione del perimetro fisico dell'infrastruttura (locali server, regole di accesso, serrature e chiavi etc.)				4	4								4							4		4				4	4	4	4
T.2	Sono previste misure di identificazione del personale che accede ai locali				4,5	4,5								4,5						4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
T.3	Si provvede al controllo e monitoraggio degli accessi alle zone sicure				4,5	4,5								4,5						4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
T.4	Sono installati sistemi di 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
T.5	Ove applicabile, esistono barriere fisiche per impedire l'accesso non autorizzato				4,5	4,5								4,5			4,5			4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
T.6	Si provvede a revisione periodica delle aree interessate da trattamenti																													
T.7	Sono previste misure di protezione contro incendi (estintori etc.), allagamenti (server ed armadi sopraelevati), disfunzioni elettriche (gruppo di continuità UPS), crolli (per terremoto etc.) e simili	4,5	4,5	4,5										4,5	4,5						4,5	4,5	4,5			4,5				
T.8	Le aree protette sono limitate rispetto al personale di servizi esterni				4,5	4,5								4,5							4,5	4,5	4,5	4,5			4,5	4,5	4,5	4,5
T.9	Sono previste misure di protezione degli archivi fisici (armadi, schedari, contenitori, cartelline)				4,5	4,5								4,5			4,5							4,5			4,5	4,5	4,5	4,5
	MEDIA FINALE MITIGAZIONE PER MINACCIA	4,239	4,239	4,239	4,055	4,024	3,927	3,894	4,014	4,000	4,038	4,010	4,065	4,042	4,144	4,094	4,214	4,054	4,009	4,045	4,010	3,990	3,975	4,027	4,131	4,121	3,936	4,044	4,065	4,063

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

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

#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	2	2,000	
6	Comunicazione non autorizzata	Umana	R	PARZIALMENTE	2	3	6,000	
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	2	2,000	
12	Vittima di phishing o altra manipolazione	Umana	RID	SI	2	3	6,000	
13	Altro trattamento illecito doloso	Umana	RID	SI	1	1	1,000	
14	Altro trattamento illecito colposo	Umana	RID	SI	1	1	1,000	
15	Mancata soddisfazione dei diritti	Umana	RID	SI	1	3	3,000	3,069
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	2	2,000	
24	Altri fattori di corruzione dati	Tecnica	I	SI	1	2	2,000	
25	Altri fattori di indisponibilità dei dati	Tecnica	D	SI	1	2	2,000	
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

Natura minaccia
Ambientale
Umana
Tecnica
Organizzativa

Comparazione Rischio Inerente / Rischio Residuo

#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			SI	1	2	2,000	
2	Allagamento	Ambientale	ID		2	3	6,000			SI	1	1	1,000	
3	Crollo o altro fattore naturale/fisico	Ambientale	ID		2	3	6,000			SI	1	1	1,000	
4	Furto di archivi o di singoli dati	Umana	RID		3	5	15,000			SI	1	3	3,000	
5	Accesso non autorizzato	Umana	RI		3	4	12,000			SI	1	2	2,000	
6	Comunicazione non autorizzata	Umana	R		3	4	12,000			PARZIALMENTE	2	3	6,000	
7	Diffusione non autorizzata	Umana	R		3	5	15,000			PARZIALMENTE	2	4	8,000	
8	Modifica dati non autorizzata	Umana	RID		3	5	15,000			SI	1	3	3,000	
9	Distruzione dati non autorizzata	Umana	ID		3	5	15,000			SI	1	3	3,000	
10	Perdita dati o dispositivo contenente dati	Umana	RID		3	4	12,000			SI	1	2	2,000	
11	Diffusione credenziali accesso	Umana	R		3	4	12,000			SI	1	2	2,000	
12	Vittima di phishing o altra manipolazione	Umana	RID		4	5	20,000			SI	2	3	6,000	
13	Altro trattamento illecito doloso	Umana	RID		3	3	9,000			SI	1	1	1,000	
14	Altro trattamento illecito colposo	Umana	RID		3	3	9,000			SI	1	1	1,000	
15	Mancata soddisfazione dei diritti	Umana	RID		2	5	10,000	11,897		SI	1	3	3,000	3,069
16	Cessazione rapporto / turnover	Umana	RID		2	3	6,000			SI	1	1	1,000	
17	Attacco informatico	Tecnica	RID		4	5	20,000			SI	2	3	6,000	
18	Virus informatico	Tecnica	RID		4	5	20,000			SI	2	3	6,000	
19	Intromissione nel sistema	Tecnica	RID		4	5	20,000			SI	2	3	6,000	
20	Danno tecnico informatico	Tecnica	RID		2	5	10,000			SI	1	3	3,000	
21	Malfunzionamento informatico	Tecnica	RID		2	5	10,000			PARZIALMENTE	1	4	4,000	
22	Malfunzionamento tecnico	Tecnica	RID		2	4	8,000			PARZIALMENTE	1	3	3,000	
23	Altri fattori di divulgazione dati	Tecnica	R		3	4	12,000			SI	1	2	2,000	
24	Altri fattori di corruzione dati	Tecnica	I		3	4	12,000			SI	1	2	2,000	
25	Altri fattori di indisponibilità dei dati	Tecnica	D		3	4	12,000			SI	1	2	2,000	
26	Mancata consapevolezza privacy	Organizzativa	RID		3	4	12,000			PARZIALMENTE	2	3	6,000	
27	Inosservanza principi/adempimenti privacy	Organizzativa	RID		3	4	12,000			SI	1	2	2,000	
28	Carenza di personale/Turnover elevato	Organizzativa	RID		2	3	6,000			SI	1	1	1,000	
29	Altre inefficienze organizzative	Organizzativa	RID		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)	MEDIO

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

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	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