Valutazione di Impatto

(*Data Protection Impact Assessment* - DPIA) sulla protezione dei dati personali

relativa al progetto di ricerca TALOs "An Italian multicentric retrospective observational study to assess effectiveness and safety of the combination of tafasitamab and lenalidomide in diffuse large B-cell lymphoma patients treated under named patient program"

redatta ai sensi dell'art. 35 del Reg. UE 679/2016 (GDPR)

e sulla base delle Linee Guida del 4/10/2017 del Working Party Art. 29

TITOLARE DEL TRATTAMENTO / CONTITOLARI	AOU BOLOGNA AUSL ROMAGNA
TITOLO DELLO STUDIO	TALOs "AN ITALIAN MULTICENTRIC RETROSPECTIVE OBSERVATIONAL STUDY TO ASSESS EFFECTIVENESS AND SAFETY OF THE COMBINATION OF TAFASITAMAB AND LENALIDOMIDE IN DIFFUSE LARGE B-CELL LYMPHOMA PATIENTS TREATED UNDER NAMED PATIENT PROGRAM"
CODICE DELLO STUDIO	TALOs
DATA EMISSIONE	01/03/2023
REDATTORI	AUTHORS: PIER LUIGI ZINZANI SILVIA CORAZZA VIRGINIA BARONI LISA ARGNANI LOCAL PRINCIPAL INVESTIGATOR (DOTT. SSA) MONICA TANI
VERIFICATORE INTERNO	FUNZIONE PRIVACY U.O. GSI U.O. INNOVAZIONE E VALUTAZIONE DELLE TECNOLOGIE
VALIDATORE	DPO
VERSIONE	1
DATA REVISIONE	24/09/2024

Il presente modello è stato redatto con la collaborazione dello Studio Legale Stefanelli&Stefanelli

Indice del documento

OBIETTIVO E ORGANIZZAZIONE DEL DOCUMENTO ... **3**

1 DEFINIZIONE DEL CONTESTO. ... **3**

1.1 LA TITOLARITÀ DEL TRATTAMENTO ... 3
1.1.1 Titolare ... *3*
1.1.2 Contitolari ... *3*
1.2 INDIVIDUAZIONE GENERALE DELL'ATTIVITÀ DI TRATTAMENTO *(A CURA DEL P.I. E DEI RICERCATORI)* ... 5
1.2.a Breve descrizione del progetto di ricerca con particolare riferimento al flusso dei dati e dei campioni biologici e applicativi coinvolti ... *5*
1.2.b Tipo di ricerca ... *5*
1.2.c Consenso informato ... *5*
1.2.c Comitato Etico ... *5*
*1.2.1. Codici di condotta **(a cura della Funzione Privacy)*** ... *5*
*1.2.2 Rispetto del principio di finalità **(a cura del P.I., Ricercatori e della Funzione Privacy)*** ... *6*
*1.2.3 Rispetto del principio di liceità **(a cura della Funzione Privacy)*** ... *6*
*1.2.4 Rispetto del principio di liceità attraverso la raccolta del consenso **(a cura del P.I., Ricercatori e della Funzione Privacy)*** ... *7*
1.3 INTERESSATI AL TRATTAMENTO *(A CURA DEL P.I. E DEI RICERCATORI)* ... 8
1.3.a Numero (anche indicativo) dei partecipanti ... *1*
*1.3.1 Consultazione degli interessati **(a cura della Funzione Privacy)*** ... *8*
*1.3.2 Rispetto del principio di trasparenza **(a cura del P.I., Ricercatori e della Funzione Privacy)*** ... *9*
*1.3.3 Misure di protezione dei diritti degli interessati **(a cura del P.I., Ricercatori e della Funzione Privacy)*** ... *10*
1.4 Dati personali trattati (a cura del P.I. e dei Ricercatori) ... *11*
1.4.a Dati raccolti ... *11*
1.4.b Lo studio clinico prevede il trattamento di ... *11*
*1.4.1 Rispetto del principio di minimizzazione **(a cura del P.I., Ricercatori e della Funzione Privacy)*** ... *11*
*1.4.2 Rispetto del principio di proporzionalità **(a cura del P.I., Ricercatori e della Funzione Privacy)*** ... *12*
*1.4.3 Rispetto del principio di esattezza **(a cura del P.I., Ricercatori e della Funzione Privacy)*** ... *13*
*1.4.4 Rispetto del principio di limitazione della conservazione **(a cura del P.I., Ricercatori e della Funzione Privacy)*** ... *13*
1.5 SOGGETTI COINVOLTI *(A CURA DEL P.I., RICERCATORI E DELLA FUNZIONE PRIVACY)* ... 15
1.5.a Centri di sperimentazione ... *15*
1.5.b Comunicazione ... *17*
1.5.c Nomina a responsabile del trattamento ... *17*
1.5.d Diffusione ... *17*
1.5.e Chi tratta i dati personali dei partecipanti alla ricerca? ... *18*
1.5.1 CONTITOLARI DEL TRATTAMENTO ***(A CURA DELLA FUNZIONE PRIVACY)*** ... 18
1.6. TRASFERIMENTO DEI DATI EXTRA UE *(A CURA DEL P.I., RICERCATORI E DELLA FUNZIONE PRIVACY)* ... 18

2 TABELLE DI CALCOLO DEL RISCHIO E VALUTAZIONE DELL'IMPATTO SUGLI INTERESSATI. ... **20**

3.1 PERDITA DI RISERVATEZZA *(A CURA DEL P.I., RICERCATORI E DELLA U.O. GSI/U.O. INNOVAZIONE E VALUTAZIONE DELLE TECNOLOGIE E DELLA FUNZIONE PRIVACY LIMITATAMENTE AL PUNTO 3).*Ù ... 20
Divulgazione/ accesso non autorizzato o accidentale ... *21*
3.2 PERDITA DI INTEGRITÀ *(A CURA DEL P.I., RICERCATORI E DELLA U.O. GSI/U.O. INNOVAZIONE E VALUTAZIONE DELLE TECNOLOGIE E DELLA FUNZIONE PRIVACY LIMITATAMENTE AL PUNTO 3)* ... 23
Modifica non autorizzata o accidentale ... *23*
3.3 PERDITA DI DISPONIBILITÀ *(A CURA DEL P.I., RICERCATORI E DELLA U.O. GSI/ U.O. INNOVAZIONE E VALUTAZIONE DELLE TECNOLOGIE E DELLA FUNZIONE PRIVACY LIMITATAMENTE AL PUNTO 3)* ... 25
Impossibilità di accesso, perdita, distruzione non autorizzata o accidentale ... *25*

Obiettivo e organizzazione del documento.

Questo documento, organizzato in sezioni, rappresenta il modello da utilizzare per elaborare e redigere la Valutazione di Impatto *(Data Protection Impact Assessment - DPIA)* di una attività di trattamento.

La Valutazione di Impatto è finalizzata ad analizzare l'impatto sulla protezione dei dati personali di un trattamento che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

1. Definizione del contesto.

In questa sezione è analizzata nel dettaglio e sotto diversi punti di vista l'attività di trattamento da sottoporre a valutazione.

1.1 La titolarità del trattamento.

In questo paragrafo sono individuati i soggetti in capo ai quali sussiste la titolarità del trattamento dei dati personali oggetto della presente valutazione di impatto.

1.1.1 Titolare.

Il Titolare è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

	In caso di titolarità autonoma (un solo Titolare) inserire i dati del Titolare del trattamento.

RAGIONE SOCIALE	
SEDE LEGALE	
INDIRIZZO MAIL	
INDIRIZZO PEC	
DPO	

1.1.2 Contitolari.

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.

	In caso di contitolarità (due o più Contitolari) inserire i dati dei Contitolari del trattamento.

RAGIONE SOCIALE	
SEDE LEGALE	

INDIRIZZO MAIL	
INDIRIZZO PEC	
DPO	

RAGIONE SOCIALE	
SEDE LEGALE	
INDIRIZZO MAIL	
INDIRIZZO PEC	
DPO	

RAGIONE SOCIALE	
SEDE LEGALE	
INDIRIZZO MAIL	
INDIRIZZO PEC	
DPO	

1.2 Individuazione generale dell'attività di trattamento *(a cura del P.I. e dei Ricercatori).*

In questo paragrafo sono individuate le caratteristiche generali dello studio clinico.

1.2.a Breve descrizione del progetto di ricerca con particolare riferimento al flusso dei dati e dei campioni biologici e applicativi coinvolti	Studio osservazionale retrospettivo che valuta l'efficacia, la sicurezza dell'associazione di tafasitamab e lenalidomide in pazienti con programma personalizzato in quanto affetti da malattia refrattaria e recidiva e con caratteristiche cliniche generali tali da non poter essere sottoposti a trapianto di midollo.	È possibile allegare il documento che riporta la sinossi o un diagramma di flusso che descrive l'attività di trattamento dei dati nell'ambito dello studio (All. n. 3 flusso, modulo di mancata acquisizione consenso, protocollo)
1.2.b Tipo di ricerca	☐ Studio unicentrico X Sudio multicentrico ☐ Studio osservazionale X Studio osservazionale di coorte retrospettivo ☐ Studio sperimentale con farmaco ☐ Indagine clinica con dispositivo medico ☐ Studio interventistico senza dispositivi e senza farmaci ☐ Studio esclusivamente su materiali biologici ☐ Altro _____	
1.2.c Consenso informato	Viene prevista l'acquisizione del consenso informato **allo studio**: X **SI (pazienti in vita contattabili)** ☐ **NO**	
1.2.c Comitato Etico	Il progetto di ricerca ha ottenuto **motivato parere favorevole** dal competente Comitato Etico a livello territoriale? X **SI** ☐ **NO** ☐ in corso di sottomissione	

1.2.1. Codici di condotta *(a cura della Funzione Privacy)*.

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'art. 40 del GDPR.

Codici di condotta	Il Titolare ha aderito a un **codice di condotta** per la corretta applicazione del Reg. UE 679/2016 alle attività di ricerca? ☐ **SI | Quale?** _____ ☒**NO**

1.2.2 Rispetto del principio di finalità *(a cura del P.I., Ricercatori e della Funzione Privacy)*.

In questo paragrafo è indicato il rispetto del principio di finalità del trattamento dei dati stabilito dall'art. 5.1-b del GDPR che prevede che i dati siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

FINALITÀ	
Il trattamento di dati verrà effettuato solo per le finalità indicate nell'informativa sul trattamento dei dati personali (cd. informativa privacy) eventualmente fornita agli interessati?	X SÌ ☐ NO ☐ L'informativa non può essere fornita ad alcun interessato
Se la risposta alla domanda precedente è NO indicare le finalità ulteriori:	
PARERE DEL **DPO**: X ACCETTABILE ☐ NON ACCETTABILE	
Indicazioni:	

1.2.3 Rispetto del principio di liceità *(a cura della Funzione Privacy)*.

In questo paragrafo è esplicitata la modalità di rispetto del principio di liceità di cui all'art. 5.1-a del GDPR nel trattamento di dati comuni e particolari tramute l'indicazione delle basi giuridiche previste all'art. 6 del GDPR per i dati comuni e all'art. 9 del GDPR per le particolari categorie di dati personali.
Per ogni finalità del trattamento deve essere individuata la relativa base giuridica.

	LICEITÀ	
	Basi giuridiche	**Finalità corrispondente**
Dati comuni	X L'interessato ha espresso il **consenso** (art. 6.1-a) * **pazienti contattabili**	Ricerca scientifica finalizzata a valutare valuta l'efficacia, la sicurezza dell'associazione di tafasitamab e lenalidomide in pazienti con programma personalizzato che non possono essere sottoposti a trapianto di midollo.
	☐ 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. 6.1-e)	

Dati particolari	X l'interessato ha prestato il proprio **consenso** esplicito al trattamento di tali dati personali per una o più finalità specifiche (art. 9.2-a) * **pazienti contattabili**	Ricerca scientifica finalizzata a valutare valuta l'efficacia, la sicurezza dell'associazione di tafasitamab e lenalidomide inpazienti con programma personalizzato che non possono essere sottoposti a trapianto di midollo.
	☐ 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, paragrafo 1, 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. 9.2-j). Ad. es. **La ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-*bis* del decreto legislativo 30 dicembre 1992, n. 502**. *	
Dati comuni e particolari	X Il consenso non è necessario poichè, 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. **Pazienti deceduti e non contattabili**	Ricerca scientifica finalizzata a valutare valuta l'efficacia, la sicurezza dell'associazione di tafasitamab e lenalidomide in pazienti con programma personalizzato che non possono essere sottoposti a trapianto di midollo. Si applica la non acquisizione del consenso per i pazienti non raggiungibili dopo ragionevole sforzo o deceduti. Questa pratica è necessaria alla popolazione al fine di non avere risultati non corrispondenti al vero, escludendo i pazienti con peggior outcome della ricerca.

1.2.4 Rispetto del principio di liceità attraverso la raccolta del consenso *(a cura del P.I., Ricercatori e della Funzione Privacy)*.

In questo paragrafo è esplicitata la modalità di rispetto del principio di liceità attraverso la raccolta del consenso.

	* **ATTENZIONE: compilare SOLO se la base giuridica del trattamento è il consenso (art. 6.1-a GDPR)**

CONSENSO	
Viene richiesto al partecipante il consenso **al trattamento dei dati personali**? (N.B.: è diverso dal consenso informato)	☒ SÌ (**pazienti contattabili**) ☐ NO

	☒**NO**, perché fornire l'informativa agli interessati **è impossibile (Pazienti deceduti)** ☒**NO**, perché fornire l'informativa agli interessati **richiede uno sforzo sproporzionato (pazienti non contattabili)** ☐ **NO**, perché fornire l'informativa agli interessati **rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca**

ATTENZIONE: Non compilare questa sezione se il consenso non viene raccolto	
Il modulo di consenso al trattamento dei dati personali è separato rispetto al modulo di consenso informato allo studio? (non necessario compilare se al punto 1.2.4.a. si è risposto NO) ☒ SI ☐ NO	
È stata prevista una procedura interna per gestire la revoca del consenso? (non necessario compilare se al punto 1.2.4.a. si è risposto NO)	Descrivere come viene tenuta traccia del consenso: L'acquisizione del consenso e l'eventuale revoca vengono tracciati in cartella clinica. Il consenso cartaceo viene conservato in istituto.
☒**SI** ☐ **NO**	(possono essere fornite più risposte) In caso di revoca del consenso: X il trattamento viene interrotto X i dati vengono cancellati ☐ altro. SPECIFICARE: _____

PARERE DEL **DPO**: X ACCETTABILE ☐ NON ACCETTABILE	
Indicazioni:	

1.3 Interessati al trattamento *(a cura del P.I. e dei Ricercatori).*

Indicare nella seguente tabella le informazioni relative ai soggetti a cui si riferiscono i dati trattati.

1.3.a Numero (anche indicativo) dei partecipanti **n. complessivo 96**	Gli interessati sono: ☐ partecipanti **appositamente arruolati** per lo studio [numero:__] ☐ **pazienti** a cui viene proposta la partecipazione allo studio [numero:____] ☒ OMISSIS ☐ _____

1.3.1 Consultazione degli interessati *(a cura della Funzione Privacy).*

Se del caso, il Titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

È stato richiesto il parere agli interessati?	Motivare l'eventuale assenza del parere degli interessati:
☐ SÌ ☒NO	Non viene chiesta l'opinione degli interessati perché la finalità di ricerca è connessa a interessi della collettività.

1.3.2 Rispetto del principio di trasparenza *(a cura del P.I., Ricercatori e della Funzione Privacy)*.

In questo paragrafo è esplicitata la modalità di rispetto del principio di trasparenza nel trattamento di dati (art. 5.1-a del GDPR).

TRASPARENZA	
Viene fornita agli interessati una specifica informativa **sul trattamento dei dati personali** (N.B.: è diversa dall'informativa sullo studio)	☒ SÌ (solo per i pazienti contattabili) ☐ **NO** ☐ SÌ per la parte prospettica dello studio; NO per la parte retrospettiva
ATTENZIONE: rispondere a questa domanda solo se l'informativa sul trattamento dei dati personali viene fornita agli interessati o anche solo a una parte di essi:	
L'informativa al trattamento dei dati personali è contenuta in un documento separato rispetto a quello che contiene le informazioni sulla ricerca	☒ SÌ ☐ **NO**
Fornire l'informativa agli interessati [è possibile fornire più risposte in caso di studio sia prospettico sia retrospettivo]:	☒ è **possibile** (solo per i pazienti contattabili) ☐ è **possibile solo per la parte prospettica dello studio** ☒ è **impossibile (Pazienti deceduti)** ☒ richiede uno **sforzo sproporzionato (pazienti non contattabili)** ☐ rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle **finalità della ricerca**
ATTENZIONE: NON compilare questa sezione se fornire l'informativa sul trattamento dei dati personali ai pazienti <u>è possibile</u>:	
Per quale motivo fornire l'informativa ai pazienti risulta impossibile, richiede uno sforzo sproporzionato o rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca?	☐ motivi **etici** (il partecipante ignora la propria condizione[1]) ☒ motivi di **impossibilità organizzativa** (partecipanti deceduti o non contattabili[2])

[1] Rientrano in questa categoria le ricerche per le quali l'informativa sul trattamento dei dati da rendere agli interessati comporterebbe la rivelazione di notizie concernenti la conduzione dello studio la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi (possono rientrare in questa ipotesi, ad esempio, gli studi epidemiologici sulla distribuzione di un fattore che predica o possa predire lo sviluppo di uno stato morboso per il quale non esista un trattamento).

[2] Nel caso in cui la mancata considerazione dei dati riferiti al numero stimato di interessati che non è possibile contattare per informarli, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati; ciò avuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti (ad esempio, nei casi in cui lo studio riguarda interessati con patologie ad elevata incidenza di mortalità o in fase terminale della malattia o in età avanzata e in gravi condizioni di salute)

	☐ motivi di **salute** (gravità dello stato clinico del partecipante impossibilitato a comprendere il contenuto dell'informativa e a prestare validamente il consenso)

ATTENZIONE: compilare questa sezione se si è barrato "motivi di **impossibilità organizzativa"**

Gli interessati risultano essere al momento dell'arruolamento dello studio: ☒ **deceduti** ☒ **non contattabili**	…in esito a: ☒ verifica dello **stato in vita** ☒consultazione dei dati riportati nella **documentazione clinica** ☒ impiego dei **recapiti telefonici** eventualmente forniti ☒ acquisizione dei dati di contatto presso l'**anagrafe** degli assistiti o della popolazione residente

Descrivere nel dettaglio ogni ragionevole sforzo compiuto per contattare gli interessati:

Si prevede che i pazienti non contattabili siano assenti o pochi. Verranno effettuati almeno 3 tentativi di contatto di cui verrà data traccia in un file cartaceo apposito conservato nell'Investigator site file.

ATTENZIONE: compilare questa sezione se si è barrato "motivi **di salute"**

☐ Lo studio è volto al **miglioramento dello stato clinico** in cui versa l'interessato

☐ È **comprovato** che le finalità dello studio non possano essere conseguite mediante il trattamento di dati riferiti a persone in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso o con altre metodologie di ricerca[3]

☐ Viene acquisito il consenso del soggetto che **rappresenta** l'interessato/ del **responsabile della struttura**

☐ Viene resa all'interessato l'informativa sul trattamento dei dati non appena le **condizioni di salute glielo consentono**

	PARERE DEL **DPO**: X ACCETTABILE ☐ NON ACCETTABILE
	Indicazioni:

1.3.3 Misure di protezione dei diritti degli interessati *(a cura del P.I., Ricercatori e della Funzione Privacy)*.

In questa sezione sono esplicitate le modalità utilizzate per la soddisfazione dei diritti degli interessati di cui agli artt. 15-22 del GDPR.

GESTIONE DEI DIRITTI DEGLI INTERESSATI	
È stata adottata una procedura di **gestione delle richieste di esercizio dei diritti degli interessati**?	
☒ SÌ	**PA 262** https://rr.auslromagna.it/index.php?option=com_fabrik&view=details&formid=159&rowid=1330&Itemid=1803
☐ NO	Indicare come vengono **raccolte le richieste** degli interessati: Ai contatti dell'Azienda
	Indicare la U.O. o il soggetto che **prende in carico** le richieste degli interessati: PI presso U.O. Ematologia di Ravenna
	PARERE DEL **DPO**: X ACCETTABILE ☐ NON ACCETTABILE
	Indicazioni: La PA 262 non riguarda la gestione delle richieste di esercizio dei diritti degli interessati. Si suggerisce l'adozione di una procedura per la gestione delle richieste di esercizio dei diritti degli interessati

[3] 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.

1.4 Dati personali trattati *(a cura del P.I. e dei Ricercatori)*.

Indicare nella seguente tabella le informazioni relative ai dati personali trattati.

<table>
<tr><td rowspan="2">1.4.a Dati raccolti</td><td colspan="2">Nell’ambito della ricerca vengono raccolte informazioni riguardanti:
☒ Dati anagrafici dei partecipanti
☒ Lo stato di salute dei partecipanti
☐ Dati genetici
SPECIFICARE:</td></tr>
<tr><td colspan="2">Dati clinico-demografici, di pazienti affetti da linfoma a cellule B recidivo refrattario ai trattamenti e non eleggibile per il trapianto autologo. Tali pazienti sono stati trattati con anticorpo monoclonale umanizzato è diretto contro gli antigeni presenti sulle B cellule e con immunoterapia. L’attività di tafasitamab e lenalidomide in associazione si è dimostrata un’arma vincente e dal 2022 e’ stata approvata anche da AIFA nei pazienti non eleggibili per il trapianto autologo.

☐ Altro
SPECIFICARE:</td></tr>
<tr><td rowspan="3">1.4.b Lo studio clinico prevede il trattamento di:</td><td>☐ dati personali di partecipanti identificati</td><td>es. nome e cognome</td></tr>
<tr><td>X dati personali pseudonimizzati</td><td>es. i partecipanti sono indicati da un codice univoco</td></tr>
<tr><td>☐ dati anonimi</td><td>i dati trattati <u>non consentono</u> di risalire all’identità dei partecipanti</td></tr>
</table>

1.4.1 Rispetto del principio di minimizzazione *(a cura del P.I., Ricercatori e della Funzione Privacy)*.

In questo paragrafo è esplicitata la modalità di rispetto del principio di minimizzazione dei dati trattati stabilito dall’art. 5.1-c del GDPR, che stabilisce che i dati debbano essere adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati.

MINIMIZZAZIONE
Spiegare perché i dati indicati al paragrafo 1.4.a devono essere trattati <u>necessariamente tutti</u> per conseguire le finalità del trattamento. Motivare per ognuna delle tipologie di dato selezionate al paragrafo 1.4.a:

Tipologia di dato	**Motivazione**
Dati anagrafici dei partecipanti	Per il raggiungimento degli obiettivi dello studio
Lo stato di salute dei partecipanti	Per il raggiungimento degli obiettivi dello studio
Dati clinico-demografici	Per il raggiungimento degli obiettivi dello studio

PARERE DEL **DPO**: X ACCETTABILE ☐ NON ACCETTABILE	
Indicazioni:	Inserire le motivazioni specifiche per ciascuna tipologia di dati trattati

1.4.2 Rispetto del principio di proporzionalità *(a cura del P.I., Ricercatori e della Funzione Privacy)*.

In questo paragrafo è esplicitata la modalità di rispetto del principio di proporzionalità dei dati trattati di cui all'art. 5.1-c del GDPR in base al quale i dati devono essere adeguati, pertinenti e limitati rispetto alle finalità per le quali sono trattati.

PROPORZIONALITÀ	
Il Titolare può raggiungere gli obiettivi della ricerca utilizzando dati anonimi?	
Sì, i dati verranno resi anonimi [4] X NO	I dati non verranno resi anonimi perché: Per la raccolta dati occorre l'accesso alla cartella clinica del paziente e successivamente per verificare l'esattezza del database
PARERE DEL **DPO**: X ACCETTABILE ☐ NON ACCETTABILE	
Indicazioni:	**SI SUGGERISCE DI MOTIVARE IN MANIERA PIÙ PUNTUALE.**

[4] Verificare l'effettività dell'anonimizzazione tramite l'analisi delle tecniche utilizzate. ATTENZIONE: i dati anonimi non devono essere considerati dati personali, di conseguenza ai dati anonimi non si applica il GDPR.

1.4.3 Rispetto del principio di esattezza *(a cura del P.I., Ricercatori e della Funzione Privacy)*.

In questo paragrafo è esplicitata la modalità di rispetto del principio di esattezza dei dati trattati previsto dall'art. 5.1-d del GDPR che stabilisce che i dati devono essere esatti e, se necessario, aggiornati, e che devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

ESATTEZZA	
In che modo viene verificata l'esattezza (correttezza) dei dati?	La qualità e la completezza dei dati raccolti viene verificata periodicamente dallo Sponsor. Attenzione nella compilazione della CRF. Monitoraggio via mail e telefonico.
Chi verifica l'esattezza (correttezza) dei dati?	PI, lo sponsor e, se richiesto, l'ente regolatorio
PARERE DEL **DPO**: X ACCETTABILE ☐ NON ACCETTABILE	
Indicazioni:	

1.4.4 Rispetto del principio di limitazione della conservazione *(a cura del P.I., Ricercatori e della Funzione Privacy)*.

In questo paragrafo è esplicitata la modalità di rispetto del principio di limitazione della conservazione dei dati previsto dall'art. 5.1-e del GDPR, che stabilisce che i dati vengono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

LIMITAZIONE DELLA CONSERVAZIONE

Indicare per ognuna delle tipologie di dati trattati il tempo massimo di conservazione per il raggiungimento delle relative finalità.

Tipologia di dato	**Tempo di conservazione**	**Motivazione della conservazione**
Dati dello studio pseudonimizzati	10 anni	Analisi dei dati ed eventuali successivi verifiche
conservazione prolungata dei dati in forma non anonima	10 anni previo consenso dell'interessato	conservazione dei dati per future attività di ricerca

PARERE DEL **DPO**: X ACCETTABILE ☐NON ACCETTABILE

Indicazioni: Si fa presente che l'indicazione della conservazione dei dati per "Future attività di ricerca" è eccessivamente generica ai sensi di quanto prevedono le Linee Guida del Working Party Articolo 29 sulla Limitazione delle finalità. Pertanto **si ricorda che all'interno dell'informativa privacy che verrà sottoposta per la raccolta dell'ulteriore consenso dovrà essere indicata la finalità specifica.** Si riporta quanto previsto dalle citate Linee Guida "La finalità della raccolta deve essere identificata in modo chiaro e specifico: deve essere abbastanza dettagliata da determinare quale tipo di trattamento sia, deve consentire di valutare la conformità con la legge e di applicare le dovute garanzie.

Per queste ragioni, una finalità che sia vaga o generica, come ad esempio per 'migliorare l'esperienza utente' o per 'finalità di marketing', 'sicurezza internet' o '**ricerca futura**' e che non fornisca ulteriori dettagli, probabilmente non soddisferà il criterio di 'specifico'. Detto questo, il grado di dettaglio in cui dovrebbe essere esplicitata una finalità dipende dal particolare contesto in cui i dati sono raccolti e dal contesto in cui saranno usati."

1.5 Soggetti coinvolti *(a cura del P.I., Ricercatori e della Funzione Privacy).*

In questa sezione sono esplicitate le modalità con le quali il titolare rispetta gli adempimenti previsti:

- dall'art. 26 del GDPR con riferimento ai Contitolari del trattamento;
- 28 del GDPR con riferimento ai Responsabili del trattamento
- dall'art. 29 del GDPR con riferimento a chi svolge trattamenti sotto l'autorità del Titolare
- dall'art. 2 *quaterdecies* del Codice Privacy, che prevede l'obbligo di attribuzione di funzioni e compiti a soggetti designati.

	Centri di sperimentazione coinvolti nello studio	**Localizzazione dei centri di sperimentazione** (indicare la località geografica):	**Numero indicativo di pazienti afferenti ai centri sul territorio**
1.5.a Centri di sperimentazione	1.Azienda Universitaria Ospedaliera Consorziale - Policlinico di Bari - Ospedale "Giovanni XIII"	1. Bari	
	2.Ospedale San Bassiano –Azienda ULSS 7 - Pedemontana	2. Bassano del Grappa	
	3. AORN Sant'Anna e San Sebastiano	3. Caserta	
	4. ARNAS Garibaldi – PO Garibaldi- Nesima	4. Catania	
	5. Azienda Ospedaliero-Universitaria di Ferrara – Arcispedale Sant'Anna	5. Ferrara	
	6. AOU Careggi	6. Firenze	
	7. Ospedale Policlinico San Martino IRCCS	7. Genova	
	8.ASL Lecce - Polo Oncologico "Giovanni Paolo II" Presidio Ospedaliero "Vito Fazzi"	8. Lecce	
	9. IRST Dino Amadori IRCCS	9. Meldola	
	10. Ospedale dell'Angelo Azienda ULSS 3 Serenissima	10. Mestre	
	11. IEO IRCCS	11. Milano	
	12. IRCCS Ospedale San Raffaele	12. Milano	
	13. AOU Federico II	13. Napoli	
	14. AOU Maggiore della Carità	14. Novara	
	15. AOU San Luigi Gonzaga	15. Obassano	
	16. Azienda Ospedale Università di Padova	16. Padova	
	17. Istituto Oncologico Veneto IOV IRCCS	17. Padova	
	18. Azienda Ospedaliera Ospedali Riuniti Villa Sofia Cervello	18. Palermo	
	19. AOU di Parma	19. Parma	
	20. Ospedale "Guglielmo da Saliceto"	20. Piacenza	
	21. AUSL Toscana Centro –Ospedale di Prato Santo Stefano	21. Prato	
	22. Ospedale Santa Maria delle Croci	22. Ravenna	Circa 96
	23. AUSL IRCCS Reggio Emilia	23. Reggio Emilia	

	24. Fondazione Policlinico Universitario Campus Bio-Medico	24. Roma	
	25. Fondazione Policlinico Universitario A. Gemelli IRCCS	25. Roma	
	26. AOU Policlinico Umberto I	26. Roma	
	27. IRCCS Istituto Nazionale Tumori Regina Elena	27. Roma	
	28. ASL Salerno - PO “Andrea Tortora” di Pagani	28. Salerno	
	29. AOU Città della Salute e della Scienza di Torino – PO Molinette	29. Torino	
	30. AO Ordine Mauriziano di Torino	30. Torino	
	32. Ospedale Ca’ Foncello Azienda ULSS 2 Marca Trevigiana	31. Treviso	
	32. Pia Fondazione di Culto e religione Cardinale Giovanni Panico – Azienda Ospedaliera	32. Lecce	
	33. Azienda Sanitaria Universitaria Giuliano Isontina (ASU GI)	33. Trieste	
	34. AOUI Verona - Ospedale Borgo Roma	34. Verona	
	35. ULSS 8 Berica - Ospedale San Bortolo	35. Vicenza	
	36. PROMOTORE: IRCCS AOU di Bologna	36. Bologna	

1.5.b Comunicazione	I dati vengono comunicati alle seguenti categorie di soggetti esterni:	☒ Promotore (IRCCS AOU di Bologna) titolare autonomo ☐ Promotore (Azienda fabbricante di dispositivi medici) ☐ Clinical Research Organization (CRO) ☐ Centro coordinatore ☐ Centri partecipanti ☐ Cloud provider ☐ Azienda di sviluppo software ☐ Azienda di manutenzione hardware ☐ Consulenti esterni ☐ Strutture sanitarie ☐ Società di servizi ☐ Istituzioni: SPECIFICARE: ☐ Altro: SPECIFICARE:
1.5.c Nomina a responsabile del trattamento	Indicare soggetti esterni a cui vengono comunicati i dati o che possono accedere ai dati che sono stati nominati responsabili del trattamento ai sensi dell'art. 28 GDPR:	
	1.	
	2.	
	3.	
	4.	
	5.	
	6.	
	7.	
	8.	
	9.	
1.5.d Diffusione	I dati della ricerca vengono **diffusi**?	☐ SI ☐ NO ☒ Solo in forma aggregata per fini di pubblicazione scientifica

1.5.e Chi tratta i dati personali dei partecipanti alla ricerca?	☒ Personale sanitario ☐ Personale tecnico ☒ Ricercatori ☐ Personale di laboratorio ☐ Altro:	Sono stati autorizzati con specifica nomina? ☒ SI ☐ NO ☐ Solo alcuni Hanno ricevuto la formazione privacy? ☒ SI ☐ NO ☐ Solo alcuni

Soggetti	Motivazione dell'accesso
Dott.ssa Tani Monica	PI

	PARERE DEL **DPO**: X ACCETTABILE ☐ NON ACCETTABILE
	Indicazioni:

1.5.1 Contitolari del trattamento *(a cura della Funzione Privacy).*

	ATTENZIONE: compilare solo se il trattamento è svolto da due o più Titolari in regime di contitolarità (v. par. 1.32.).

GESTIONE DEL RAPPORTO DI CONTITOLARITÀ			
I Contitolari hanno stipulato un accordo di contitolarità?	☐ SÌ ☐ NO		
L'accordo di contitolarità contiene le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR con riguardo a: ☐ esercizio dei diritti degli interessati ☐ rispettive funzioni di comunicazione delle informative sul trattamento dei dati personali ☐ quale dei Contitolari è il punto di contatto con gli interessati e i rispettivi ruoli e rapporti dei contitolari con gli interessati			
Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato?	☐ SÌ ☐ NO	In che modo?	☐ inserimento nell'informativa privacy ☐ rinvio nell'informativa a pubblicazione su sito web ☐ pubblicazione su sito web

	PARERE DEL **DPO**: ☐ ACCETTABILE ☐ NON ACCETTABILE
	Indicazioni:

1.6. Trasferimento dei dati extra UE *(a cura del P.I., Ricercatori e della Funzione Privacy).*

In questa sezione vengono riportate le basi di legittimità del trasferimento dei dati a soggetti che sono stabiliti in Paesi esterni allo Spazio Economico Europeo (Capo V del GDPR).

TRASFERIMENTO EXTRA-UE	
I dati vengono trasferiti al di fuori dell'Unione Europea?	☐ SÌ ☒ **NO**

	ATTENZIONE: compilare i seguenti riquadri solo in caso di trasferimenti di dati personali extra UE		
Indicare i Paesi terzi in cui i dati vengono trasferiti		Indicare il contesto e la finalità del trasferimento	Indicare le basi di legittimità del trasferimento:
	PARERE DEL **DPO**: X ACCETTABILE ☐ NON ACCETTABILE		
	Indicazioni:		

2. Tabelle di calcolo del rischio e valutazione dell'impatto sugli interessati.

In questa sezione del documento è dettagliata l'analisi del rischio del trattamento oggetto della valutazione d'impatto.

La definizione di rischio è la seguente:

> *il rischio è l'eventualità di subire un danno in conseguenza di un'azione compiuta o subita, e si calcola ricorrendo alla formula R=P*I, in cui P è la probabilità di accadimento delle minacce, e I è l'impatto o danno conseguente.*[5]

Alla luce della definizione di cui sopra, l'analisi del rischio viene svolta nel seguente modo:

- prima vengono analizzate le minacce e la probabilità di accadimento;
- poi viene analizzato l'impatto o danno conseguente;
- e, infine, tenuto conto delle minacce e del possibile impatto, viene valutato il rischio.

Il rischio di cui sopra è denominato rischio inerente, ossia connaturato nell'attività svolta dall'organizzazione prima dell'adozione di misure volte a contenerlo o controllarlo. In sostanza, si opera una valutazione dei rischi intrinseci cui è esposta l'organizzazione senza che si operi un controllo sugli stessi[6].

Valutato il rischio inerente si andranno ad analizzare le misure di sicurezza implementate o che si reputa opportuno implementare per valutare il rischio residuo.

Il rischio residuo è il rischio che permane dopo aver trattato il rischio inerente[7].

Se il rischio residuo viene valutato come accettabile, potrà procedersi con l'attività di trattamento dei dati. Laddove, invece, il rischio residuo continui ad essere elevato nonostante le misure di sicurezza adottate, sarà necessario svolgere la Consultazione preventiva dinanzi l'Autorità Garante ai sensi dell'art. 36 GDPR.

NB: La compilazione delle tabelle riportate ai successivi paragrafi 3.1., 3.2. e 3.3. deve seguire le istruzioni riportate nell'Allegato 1.

3.1 Perdita di riservatezza *(a cura del P.I., Ricercatori e della U.O. GSI/U.O. Innovazione e valutazione delle tecnologie e della Funzione Privacy limitatamente al punto 3)*.ù

[5] Guida ISO/IEC 73/2009, 3.6.1.8: il rischio può esser definito come la combinazione delle probabilità di un evento e delle sue conseguenze;

[6] Guida ISO/IEC 73/2009, 3.6.1.8: L'identificazione del rischio comporta l'individuazione delle fonti di rischio (3.5.1.2), degli eventi (3.5.1.3), delle loro cause e delle loro potenziali conseguenze (3.6.1.3). L'identificazione del rischio può coinvolgere dati storici, analisi teoriche, opinioni informate ed esperte e le esigenze delle parti interessate.

7 Guida ISO/IEC 73/2009: 3.8.1.6 rischio residuo: rischio (1.1) rimanente dopo il trattamento del rischio (3.8.1)

☐ **La perdita di riservatezza dei dati non è configurabile**	**Se una o entrambe le caselle vengono spuntate, la tabella sotto riportata NON deve essere compilata**
☐ **La perdita di riservatezza dei dati non ha impatto sui diritti e le libertà degli interessati**	

Divulgazione/ accesso non autorizzato o accidentale		
1. Quali sono le **potenziali minacce** alle quali sono esposte le aree ad accesso ristretto in cui si svolge il trattamento dei dati?	**Azioni intenzionali esterne o interne** ☒ Accesso abusivo da parte di persone non autorizzate ai luoghi in cui si svolge il trattamento (es. sala CED, archivio dei documenti, uffici con computer, laboratori ecc.) ☒ Sottrazione da parte di soggetti interni o esterni alla struttura di documenti cartacei o di strumenti elettronici (pc) ☒ Infezione del sistema tramite software nocivi diffusi via mail o attraverso internet (es. trojan horse, malware, spyware, cryptolocker, ransmoware, etc.) ☐ Condivisione dei dati con soggetti non autorizzati ☐ _____	
2. Quali sono le principali **vulnerabilità** rilevate?	OMISSIS	
3. **Conseguenze per gli interessati della perdita di riservatezza dei dati:** OMISSIS	Impatto sui **diritti e le libertà** degli interessati: OMISSIS	**Livello di impatto** della perdita di riservatezza dei dati: OMISSIS
4. Stima della **probabilità** di accadimento delle minacce (fattore **P** della formula di calcolo del Rischio)	OMISSIS	
4a. Motivazione sull'indicazione del livello di probabilità		
5. Stima dell'**impatto** (fattore **I** della formula di calcolo del Rischio)	OMISSIS	

6. Rischio inerente (R = P x I) OMISSIS

		P			
	I	Improbabile	Poco probabile	Probabile	Molto probabile
	Gravissimo				
	Grave				
	Medio				
	Lieve				

Rischio inerente:	X basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

7. Quali misure di sicurezza già in atto contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	OMISSIS

8. Misure di sicurezza:	X adeguate	☐ minime	☐ insufficienti	☐ inesistenti

9. Stima del rischio residuo

		Misure di sicurezza			
	R_i	Adeguate	Minime	Insufficienti	Inesistenti
	Molto alto	☐ 4	☐ 8	☐ 12	☐ 16
	Alto	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Basso	X 1	☐ 2	☐ 3	☐ 4

Rischio residuo:	X basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

10. Modalità di mitigazione del rischio per gestire il rischio residuo	OMISSIS

11. Quali **misure ulteriori di sicurezza** contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	OMISSIS
12. Priorità degli **interventi** di attuazione delle ulteriori misure di sicurezza	OMISSIS
13. **Responsabile/i** dell'attuazione delle ulteriori misure di sicurezza	OMISSIS

14. **Rischio residuo**	X accettabile (1-6)	☐ non accettabile (8-16)
	attuazione del trattamento	consultazione preventiva

	PARERE DEL **DPO**: X ACCETTABILE ☐NON ACCETTABILE
	Indicazioni:

3.2 Perdita di integrità *(a cura del P.I., Ricercatori e della U.O. GSI/U.O. Innovazione e valutazione delle tecnologie e della Funzione Privacy limitatamente al punto 3).*

☐ **La perdita di integrità dei dati non è configurabile**	**Se una o entrambe le caselle vengono spuntate, la tabella sotto riportata NON deve essere compilata**
X **La perdita di integrità dei dati non ha impatto sui diritti e le libertà degli interessati**	

Modifica non autorizzata o accidentale	
Esempi di **minacce**	☐ Malfunzionamento dell'hardware ☐ Malfunzionamento del software ☐ Deterioramento degli strumenti informatici ☐ Errore umano nell'inserimento dei dati ☐ Infezione del sistema tramite software nocivi diffusi via mail o attraverso internet (es. trojan horse, malware, spyware, cryptolocker, ransmoware, etc.)
2. Quali sono le principali **vulnerabilità** rilevate?	☐ Mancanza di regolarità nella manutenzione dell'hardware ☐ Mancanza di regolarità nell'aggiornamento del software ☐ Strumenti non protetti da attacchi informatici ☐ Mancata adozione di una policy per il corretto utilizzo degli strumenti informatici ☐ Mancata formazione del personale ☐ _____

3.**Conseguenze per gli interessati della perdita di integrità dei dati:**	Impatto sui **diritti e le libertà** degli interessati:	**Livello di impatto** della perdita di integrità dei dati:

☐ Morte	Diritto alla vita (art. 2 Cost.)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	
☐ Furto o usurpazione d'identità	Diritto all'identità personale (art. 2 Cost.)	
☐ Discriminazioni	Diritto all'uguaglianza (art. 3 Cost.)	
☐ Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	
☐ Perdite finanziarie	Diritti patrimoniali	
☐ altro_____	_____	
4. Stima della probabilità di accadimento delle minacce (fattore P della formula di calcolo del Rischio)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4	
4a. Motivazione sull'indicazione del livello di probabilità		
5. Stima dell'impatto (fattore I della formula di calcolo del Rischio)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4	

6. Rischio inerente (R = P x I)

		P			
		Improbabile	Poco probabile	Probabile	Molto probabile
I	Gravissimo	☐ 4	☐ 8	☐ 12	☐ 16
	Grave	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Lieve	☐ 1	☐ 2	☐ 3	☐ 4

Rischio inerente:	☐ basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

7. Quali misure di sicurezza già in atto contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	☐ Regolare manutenzione dell'hardware ☐ Software aggiornato regolarmente ☐ Adozione di una policy per il corretto utilizzo degli strumenti informatici ☐ Formazione del personale ☐ _____

8. Misure di sicurezza:	☐ adeguate	☐ minime	☐ insufficienti	☐ inesistenti

9. Stima del rischio residuo

		Misure di sicurezza			
		Adeguate	Minime	Insufficienti	Inesistenti
R_i	Molto alto	☐ 4	☐ 8	☐ 12	☐ 16
	Alto	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Basso	☐ 1	☐ 2	☐ 3	☐ 4

Rischio residuo:	☐ basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

10. Modalità di mitigazione del rischio per gestire il rischio residuo	☐ nessuna: accettazione del rischio (1-6) ☐ trasferimento del rischio (outsourcing)

	☐ trasferimento del rischio (polizza assicurativa) ☐ adozione di ulteriori misure di sicurezza ☐ altro _____
11. Quali **misure ulteriori di sicurezza** contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	• _____
12. Priorità degli **interventi** di attuazione delle ulteriori misure di sicurezza	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
13. **Responsabile/i** dell'attuazione delle ulteriori misure di sicurezza	1. 2.

14. **Rischio residuo**	☐ accettabile (1-6)	☐ non accettabile (8-16)
	attuazione del trattamento	consultazione preventiva

	PARERE DEL **DPO**: X ACCETTABILE ☐ NON ACCETTABILE
	Indicazioni:

3.3 Perdita di disponibilità *(a cura del P.I., Ricercatori e della U.O. GSI/ U.O. Innovazione e valutazione delle tecnologie e della Funzione Privacy limitatamente al punto 3).*

☐ **La perdita di disponibilità dei dati non è configurabile**	**Se una o entrambe le caselle vengono spuntate, la tabella sotto riportata NON deve essere compilata**
X **La perdita di disponibilità dei dati non ha impatto sui diritti e le libertà degli interessati**	

Impossibilità di accesso, perdita, distruzione non autorizzata o accidentale	
Esempi di **minacce**	☐ Infezione del sistema tramite software nocivi diffusi via mail o attraverso internet (es. trojan horse, malware, spyware, cryptolocker, ransmoware, etc.) ☐ Catastrofi naturali (incendi, allagamenti, terremoti) ☐ Eliminazione accidentale dei dati ☐ _____
2. Quali sono le principali **vulnerabilità** rilevate?	☐ Assenza di impianto antincendio ☐ Conservazione dei dati in locali seminterrati o vicino a tubature ☐ Zona sismica ☐ Strumenti non protetti da attacchi informatici ☐ Mancata formazione del personale ☐ _____

3.Conseguenze per gli interessati della perdita di disponibilità dei dati:	Impatto sui diritti e le libertà degli interessati:	Livello di impatto della perdita di disponibilità dei dati:
☐ Morte	Diritto alla vita (art. 2 Cost.)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	
☐ Furto o usurpazione d'identità	Diritto all'identità personale (art. 2 Cost.)	
☐ Discriminazioni	Diritto all'uguaglianza (art. 3 Cost.)	
☐ Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	
☐ Perdite finanziarie	Diritti patrimoniali	
☐ altro_____	_____	
4. Stima della probabilità di accadimento delle minacce (fattore P della formula di calcolo del Rischio)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4	
4a. Motivazione sull'indicazione del livello di probabilità		
5. Stima dell'impatto (fattore I della formula di calcolo del Rischio)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4	

6. Rischio inerente (R = P x I)

		P			
	I	Improbabile	Poco probabile	Probabile	Molto probabile
	Gravissimo	☐ 4	☐ 8	☐ 12	☐ 16
	Grave	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Lieve	☐ 1	☐ 2	☐ 3	☐ 4

Rischio inerente:	☐ basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

7. Quali misure di sicurezza già in atto contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	☐ Misure di protezione dagli attacchi informatici [*descrizione delle misure*:_____] ☐ Backup [*descrizione delle modalità di backup*:_____] ☐ Cloud [*descrizione del cloud*:_____] ☐ Formazione del personale ☐ _____

8. Misure di sicurezza:	☐ adeguate	☐ minime	☐ insufficienti	☐ inesistenti

9. Stima del rischio residuo

		Misure di sicurezza			
	R_i	Adeguate	Minime	Insufficienti	Inesistenti
	Molto alto	☐ 4	☐ 8	☐ 12	☐ 16
	Alto	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Basso	☐ 1	☐ 2	☐ 3	☐ 4

Rischio residuo:	☐ basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

10. **Modalità di mitigazione del rischio** per gestire il rischio residuo	☐ nessuna: accettazione del rischio (1-6) ☐ trasferimento del rischio (outsourcing) ☐ trasferimento del rischio (polizza assicurativa) ☐ adozione di ulteriori misure di sicurezza ☐ altro _____
11. Quali **misure ulteriori di sicurezza** contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	• _____
12. Priorità degli **interventi** di attuazione delle ulteriori misure di sicurezza	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
13. **Responsabile/i** dell'attuazione delle ulteriori misure di sicurezza	1. 2.

14. **Rischio residuo**	☐ accettabile (1-6)	☐ non accettabile (8-16)
	attuazione del trattamento	consultazione preventiva

	PARERE DEL **DPO**: X ACCETTABILE ☐ NON ACCETTABILE
	Indicazioni:

Lo Sperimentatore principale

Il referente dell'UO Governo Sistemi Informativi

Il Direttore dell'UO Affari Generali e Legali

Il Data Protection Officer (DPO)

Allegato 1 - Indicazioni per il calcolo del rischio

In questa sezione sono riportate le indicazioni per la compilazione delle tabelle di calcolo del rischio presenti nel paragrafo 8, ove sono presentati gli elementi – a livello macro – esposti alle minacce di:

Perdita della RISERVATEZZA dei dati	Perdita della INTEGRITÀ dei dati	Perdita della DISPONIBILITÀ dei dati

Per ogni elemento:

1. indicare le principali **minacce** suddivisibili in azioni esterne o interne *(si possono aggiungere quelle non previste)*

1. Quali sono le potenziali minacce alle quali sono esposte le aree ad accesso ristretto in cui si svolge il trattamento dei dati?	Azioni intenzionali esterne o interne ☐ Accesso abusivo da parte di persone non autorizzate ai luoghi in cui si svolge il trattamento (es. sala CED, archivio dei documenti, uffici con computer, ecc.)

2. indicare le principali **vulnerabilità** - intese come scarsa qualità dei mezzi impiegati che genera punti di debolezza

2. Quali sono le principali vulnerabilità rilevate?	Indicare le vulnerabilità rilevate

3. indicare le conseguenze per gli interessati e il livello di **impatto sui diritti e le libertà degli interessati** per ognuno dei tre requisiti di sicurezza (riservatezza, integrità, disponibilità) in base alla scala riportata di seguito. Si tratta di una scala di tipo "semi quantitativo", ovvero, la valutazione è guidata dal criterio (espresso in termini qualitativi) che corrisponde al livello (espresso in termini qualitativi) e al valore (espresso in termini numerici). [8]

CRITERIO	LIVELLO	VALORE
Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).	LIEVE	1
Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).	MEDIO	2
Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).	GRAVE	3
Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).	GRAVISSIMO	4

3a. Perdita di riservatezza *(Divulgazione/ accesso non autorizzato o accidentale)*	Conseguenze per gli interessati della perdita di riservatezza dei dati:	Impatto sui diritti e le libertà degli interessati:	Livello di impatto della perdita di riservatezza dei dati:
	☐ Morte	Diritto alla vita (art. 2 Cost.)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4 ☐ La perdita di riservatezza non è configurabile
	☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	
	☐ Furto o usurpazione d'identità	Diritto all'identità personale (art. 2 Cost.)	
	☐ Discriminazioni	Diritto all'uguaglianza (art. 3 Cost.)	
	☐ Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	
	☐ Perdite finanziarie	Diritti patrimoniali	
	☐ altro_____	_____	

[8] La natura della violazione è ripresa dal Modello di notifica al Garante in caso di data breach, sezione C note al punto 6.

3b. Perdita di integrità dei dati *(Modifica non autorizzata o accidentale)*	Conseguenze per gli interessati della perdita di integrità dei dati:	Impatto sui diritti e le libertà degli interessati:	Livello di impatto della perdita di integrità dei dati:
	☐ Morte	Diritto alla vita (art. 2 Cost.)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4 ☐ La perdita di integrità non è configurabile
	☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	
	☐ Furto o usurpazione d'identità	Diritto all'identità personale (art. 2 Cost.)	
	☐ Discriminazioni	Diritto all'uguaglianza (art. 3 Cost.)	
	☐ Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	
	☐ Perdite finanziarie	Diritti patrimoniali	
	☐ altro_____	_____	
3c. Perdita di disponibilità dei dati *(Impossibilità di accesso, perdita, distruzione non autorizzata o accidentale)*	Conseguenze per gli interessati della perdita di disponibilità dei dati:	Impatto sui diritti e le libertà degli interessati:	Livello di impatto della perdita di disponibilità dei dati
	☐ Morte	Diritto alla vita (art. 2 Cost.)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4 ☐ La perdita di disponibilità non è configurabile
	☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	
	☐ Furto o usurpazione d'identità	Diritto all'identità personale (art. 2 Cost.)	
	☐ Discriminazioni	Diritto all'uguaglianza (art. 3 Cost.)	
	☐ Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	
	☐ Perdite finanziarie	Diritti patrimoniali	
	☐ altro_____	_____	

4. indicare la **stima della probabilità** di accadimento delle minacce in base alla scala riportata di seguito. Si tratta di una scala di tipo "semi quantitativo", ovvero, la valutazione è guidata dal criterio (espresso in termini qualitativi) che corrisponde al livello (espresso in termini qualitativi) e al valore (espresso in termini numerici). Motivare nella sezione 4a il grado di probabilità indicato con riferimento alla realtà organizzativa del Titolare.

CRITERIO	LIVELLO	VALORE
• La mancanza rilevata può provocare un danno per la concomitanza di più eventi poco probabili indipendenti • L'evento non si è mai verificato negli ultimi 5 anni • Il verificarsi del danno conseguente la mancanza rilevata susciterebbe incredulità in azienda	IMPROBABILE	1
• La mancanza rilevata può provocare un danno solo in circostanze sfortunate di eventi • L'evento si è verificato negli ultimi 5 anni e/o ci si aspetta una frequenza fra 1 e 3 anni • Il verificarsi del danno conseguente la mancanza rilevata susciterebbe una grande sorpresa in azienda	POCO PROBABILE	2
• La mancanza rilevata può provocare un danno, anche se non in modo automatico o diretto • L'evento si è verificato negli ultimi 3 anni e/o ci si aspetta una frequenza fra 1 mese ed 1 anno • Il verificarsi del danno conseguente la mancanza rilevata susciterebbe una moderata sorpresa in azienda	PROBABILE	3
• Esiste una correlazione diretta tra la mancanza rilevata e il verificarsi del danno ipotizzato • L'evento si è verificato nell'ultimo mese e/o ci si aspetta una frequenza inferiore a 1 mese • Il verificarsi del danno conseguente la mancanza rilevata susciterebbe alcuno stupore in azienda	MOLTO PROBABILE	4

4. Stima della probabilità di accadimento delle minacce (fattore P della formula di calcolo del Rischio)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
4a. Motivazione sull'indicazione del livello di probabilità	

5. individuare la **stima dell'impatto** provocato dall'accadimento delle minacce che corrisponde al valore più elevato tra i tre livelli di impatto su ognuno dei tre requisiti di sicurezza calcolati al punto 3

5. Stima dell'impatto (fattore I della formula di calcolo del Rischio)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4

6. calcolare la gravità del **rischio inerente** incrociando i valori qualitativi che risultano dalla stima della probabilità e dalla stima dell'impatto (R_i=PxI), che possono generare risultati da 1 (impatto lieve e improbabile) a massimo 16 (impatto gravissimo e molto probabile)

6. Rischio inerente (R = P x I)					
		P			
	I		Improbabile	Poco probabile	Probabile	Molto probabile
		Gravissimo	☐ 4	☐ 8	☐ 12	☐ 16
		Grave	☐ 3	☐ 6	☐ 9	☐ 12
		Medio	☐ 2	☐ 4	☐ 6	☐ 8
		Lieve	☐ 1	☐ 2	☐ 3	☐ 4

Rischio inerente:	☐ basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

7. indicare le **misure di sicurezza tecniche e organizzative** già in atto che contribuiscono a ridurre la probabilità e l'impatto di un evento negativo**.**

7. Quali misure di sicurezza già in atto contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	inserire le misure di sicurezza già implementate

8. indicare il **livello di adeguatezza delle misure di sicurezza** in base alla scala riportata di seguito.

CRITERIO	LIVELLO
Misure di mitigazione adeguate ai requisiti di legge e capaci di fungere da contromisure rispetto alle tipologie di rischio individuate.	ADEGUATE
Modalità organizzative e gestionali di sola sufficienza rispetto alle tipologie di rischio individuate e alla conformità legislativa.	MINIME
Modalità organizzative e gestionali insufficienti rispetto alle tipologie di rischio individuate e alla conformità legislativa.	INSUFFICIENTI
Nessuna previsione di misure di mitigazione nonostante un rischio inerente MEDIO / ALTO / MOLTO ALTO.	INESISTENTI

8. Misure di sicurezza:	☐ adeguate	☐ minime	☐ insufficienti	☐ inesistenti

9. calcolare la gravità del **rischio residuo** alla luce delle misure in atto, incrociando il livello di adeguatezza delle misure con il livello di gravità del rischio inerente;

9. Stima del rischio residuo						
		Misure di sicurezza				
	R_i		Adeguate	Minime	Insufficienti	Inesistenti
		Molto alto	☐ 4	☐ 8	☐ 12	☐ 16
		Alto	☐ 3	☐ 6	☐ 9	☐ 12

	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Basso	☐ 1	☐ 2	☐ 3	☐ 4

Rischio residuo:	☐ basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

10. indicare le **modalità di mitigazione del rischio** per gestire il rischio residuo: solo in caso di rischio basso (1-3) o medio (4-6) è possibile optare per l'accettazione del rischio;

10. **Modalità di mitigazione del rischio** per gestire il rischio residuo	☐ nessuna: accettazione del rischio (1-3) ☐ trasferimento del rischio (outsourcing) ☐ trasferimento del rischio (polizza assicurativa) ☐ adozione di ulteriori misure di sicurezza ☐ altro _____

11. nel caso in cui come modalità di mitigazione del rischio sia stata indicata l'"adozione di ulteriori misure di sicurezza" indicare quali **misure ulteriori di sicurezza** contribuiscono a ridurre la probabilità e l'impatto di un evento negativo.

11. Quali **misure ulteriori di sicurezza** contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	inserire le misure di sicurezza che si intende implementare per mitigare il rischio

12. indicare **entro quanto tempo** dovranno essere attuate le ulteriori misure di sicurezza sulla base dei valori ottenuti nella tabella di calcolo del rischio residuo

12. Priorità degli **interventi** di attuazione delle ulteriori misure di sicurezza	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)

13. indicare la/e **funzione/i aziendale/i** o il/i **responsabile/i di funzione** deputato/i ad attuare le ulteriori misure di sicurezza. È possibile fare riferimento ai soggetti indicati nel paragrafo inziale "Organizzazione e obiettivo del documento" (CPO, DPO, PM, Legale/CM, CISO, RTD).

13. **Responsabile/i** dell'attuazione delle ulteriori misure di sicurezza	1. 2.

14. indicare l'**accettabilità del rischio residuo** in base al valore ottenuto nella tabella al punto 9 e alla valutazione qualitativa delle risposte fornite ai punti 10 e 11.

14. **Rischio residuo**	☐ **accettabile (1-6)**	☐ **non accettabile (8-16)**
	attuazione del trattamento	consultazione preventiva