Valutazione di Impatto

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

relativa al progetto di ricerca ROmagnaMulticenter ICU Study (ROMICUS)

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	AUSL DELLA ROMAGNA
TITOLO DELLO STUDIO	STUDIO OSSERVAZIONALE STORICO DEI RICOVERI IN TERAPIA INTENSIVA NELL'AUSL ROMAGNA: APPROFONDIMENTI CLINICI ED EPIDEMIOLOGICI
CODICE DELLO STUDIO	ROMAGNAMULTICENTER ICU STUDY (ROMICUS)
DATA EMISSIONE	
REDATTORI	PRINCIPAL INVESTIGATOR DOTT.JONATHANMONTOMOLI
VERIFICATORE INTERNO	U.O. AA.GG.LL. - FUNZIONE PRIVACY U.O. GSI
VALIDATORE	DPO
VERSIONE	1.0 DEL 30/10/2025
DATA REVISIONE	

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).* 4
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 *8*
*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)**.* *8*
*1.3.3 Misure di protezione dei diritti degli interessati **(a cura del P.I., Ricercatori e della Funzione Privacy)**.* *9*
1.4 Dati personali trattati (a cura del P.I. e dei Ricercatori). *10*
1.4.a Dati raccolti *10*
1.4.b Lo studio clinico prevede il trattamento di: *10*
*1.4.1 Rispetto del principio di minimizzazione **(a cura del P.I., Ricercatori e della Funzione Privacy)**.* *10*
*1.4.2 Rispetto del principio di proporzionalità **(a cura del P.I., Ricercatori e della Funzione Privacy)**.* *11*
*1.4.3 Rispetto del principio di esattezza **(a cura del P.I., Ricercatori e della Funzione Privacy)**.* *11*
*1.4.4 Rispetto del principio di limitazione della conservazione **(a cura del P.I., Ricercatori e della Funzione Privacy)**.* *12*
1.5 SOGGETTI COINVOLTI *(A CURA DEL P.I., RICERCATORI E DELLA FUNZIONE PRIVACY).* 13
1.5.a Centri di sperimentazione *13*
1.5.b Comunicazione *14*
1.5.c Nomina a responsabile del trattamento *14*
1.5.d Diffusione *14*
1.5.e Chi tratta i dati personali dei partecipanti alla ricerca? *14*
1.5.1 CONTITOLARI DEL TRATTAMENTO***(A CURA DELLA FUNZIONE PRIVACY).*** 15
1.6. TRASFERIMENTO DEI DATI EXTRA UE*(A CURA DEL P.I., RICERCATORI E DELLA FUNZIONE PRIVACY)*. 15

2. TABELLE DI CALCOLO DEL RISCHIO E VALUTAZIONE DELL'IMPATTO SUGLI INTERESSATI. **16**

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).* 16
Divulgazione/ accesso non autorizzato o accidentale *17*
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).* 19
Modifica non autorizzata o accidentale *19*
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).* 21
Impossibilità di accesso, perdita, distruzione non autorizzata o accidentale *21*

ALLEGATO 1 - INDICAZIONI PER IL CALCOLO DEL RISCHIO **24**

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	AZIENDA UNITÀ SANITARIA LOCALE DELLA ROMAGNA (AUSL ROMAGNA)
SEDE LEGALE	VIA DE GASPERI 8 - 48121 RAVENNA
INDIRIZZO MAIL	
INDIRIZZO PEC	AZIENDA@PEC.AUSLROMAGNA.IT
DPO	DOTT.SSA VALERIA MIGNATTI

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	Lo studio si propone di descrivere le caratteristiche della popolazione ricoverata nelle Terapie Intensive (TI) dell'AUSL Romagna durante un periodo di 24 anni (2000-2023), analizzando variabili demografiche, diagnosi principali, comorbidità, durata della degenza e variazioni tra le diverse TI del sistema sanitario regionale, con particolare attenzione ai trend temporali dei ricoveri e agli esiti ospedalieri nel periodo osservato ed in sottoperiodi. Lo studio valuterà inoltre la prognosi a medio e lungo termine e i bisogni sanitari dei sopravvissuti alla TI. Saranno inoltre analizzati i pattern di utilizzo dei servizi sanitari post-dimissione, come successive ospedalizzazioni, accessi al Pronto Soccorso e necessità di servizi di assistenza cronica. Lo studio utilizzerà esclusivamente i flussi informativi correnti regionali dell'Emilia-Romagna, che raccolgono dati standardizzati su tutti i contatti dei pazienti con il sistema sanitario regionale. I pazienti saranno selezionati attraverso codici di reparto specifici per Terapia Intensiva nelle strutture dell'AUSL Romagna. Le fonti dati comprendono il flusso SDO, Scheda di Dimissione Ospedaliera, quale database primario per l'identificazione della coorte di studio, contenente informazioni su ricoveri ospedalieri, dati demografici, date di ammissione e dimissione, diagnosi, procedure eseguite e codici DRG. Il flusso ASA, Assistenza Specialistica Ambulatoriale, permetterà di tracciare i servizi specialistici ambulatoriali ricevuti dai pazienti prima e dopo l'ammissione in TI. Il flusso PS, Pronto Soccorso, sarà utilizzato per analizzare gli accessi d'emergenza con relativi servizi forniti. Il flusso informativo del ReM, Registro di Mortalità regionale, sarà impiegato per rilevare gli eventi di decesso e determinare la mortalità a lungo termine. Tutti i pazienti che rispetteranno i criteri d'inclusione verranno estratti in forma pseudonimizzata su una eCRF in formato elettronico. Sarà mantenuto un file di trascodifica, in cui saranno registrate le corrispondenze fra dati anagrafici e ID univoco associato al paziente	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. dichiarazione mancata acquisizione del consenso e sinossi)

1.2.b Tipo di ricerca	X Studio unicentrico ☐ 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**: ☐**SI** X**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**: XACCETTABILE☐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	☐ L'interessato ha espresso il **consenso** (art. 6.1-a) ✱	
	☐ 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	☐ l'interessato ha prestato il proprio **consenso** esplicito al trattamento di tali dati personali per una o più finalità specifiche (art. 9.2-a) ✱	
	☐ 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.	Finalità di ricerca scientifica in campo medico finalizzata alla valutazione epidemiologica dell'impatto del ricovero in terapia intensiva

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 X NO X**NO**, perchéfornire l'informativa agli interessati **è impossibile** x **NO**, perchéfornire l'informativa agli interessati **richiede uno sforzo sproporzionato** x**NO**, perchéfornire 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 :
☐ **SI** ☐ **NO**	(possono essere fornite più risposte) In caso di revoca del consenso: ☐ il trattamento viene interrotto ☐ i dati vengono cancellati ☐ altro. SPECIFICARE:

	PARERE DEL **DPO**: XACCETTABILE☐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 stimato circa 70.000**	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)	xSÌ mediante pubblicazione dell'informativa dello studio sul sito internet istituzionale dell'Azienda ☐**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 **X NO**

Fornire l'informativa agli interessati [è possibile fornire più risposte in caso di studio sia prospettico sia retrospettivo]:	☐ è **possibile** ☐ è **possibile solo per la parte prospettica dello studio** X è **impossibile** x richiede uno **sforzo sproporzionato** x 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]) X motivi di **impossibilità organizzativa** (partecipanti deceduti o non contattabili[2]) ☐ 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: X**deceduti** X**non contattabili**	…in esito a: X 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:

I flussi informativi correnti utilizzati per il presente studio non contengono recapiti diretti dei pazienti né dati identificativi quali nome e cognome, bensì esclusivamente identificativi pseudonimizzati. Lo studio abbraccia un arco temporale di 24 anni e coinvolge tutte le TI dell'AUSL Romagna, includendo pertanto una coorte altamente numerosa, stimata in circfa 70.000 pazienti, non necessariamente residenti nei comuni afferenti al territorio dell'Azienda Sanitaria.

La popolazione in studio presenta caratteristiche peculiari che rendono oggettivamente impossibile il contatto sistematico con gli interessati. In primo luogo, i pazienti ricoverati in TI rappresentano una popolazione caratterizzata da elevata mortalità sia durante il ricovero sia nei periodi successivi alla dimissione, come documentato dalla letteratura scientifica internazionale. Considerando l'ampio arco temporale dello studio, si stima che una percentuale consistente dei pazienti inclusi nella coorte sia ad oggi deceduta, rendendo de facto impossibile l'acquisizione del consenso informato.

Qualsiasi tentativo di recuperare i nominativi e i recapiti dei pazienti attraverso il collegamento tra il codice nosologico pseudonimizzato e altri database contenenti dati identificativi richiederebbe un dispendio considerevole di risorse umane, economiche e temporali. Tale procedura, oltre a comportare rischi aggiuntivi per la privacy attraverso la re-identificazione dei dati pseudonimizzati, permetterebbe comunque di rintracciare soltanto una

[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)

frazione dei pazienti inclusi nello studio. I pazienti non contattabili comprenderebbero i soggetti deceduti, coloro che hanno modificato la residenza al di fuori del territorio regionale, i pazienti con recapiti non aggiornati nei registri sanitari e coloro che, per varie ragioni, risultano irraggiungibili nonostante la disponibilità di dati anagrafici.
La mancata considerazione dei dati riferiti al numero stimato di interessati non contattabili rispetto al numero complessivo dei soggetti coinvolti nella ricerca produrrebbe conseguenze significative per lo studio in termini di alterazione dei risultati. L'esclusione di questa popolazione comporterebbe un bias di selezione sostanziale che comprometterebbe la validità scientifica della ricerca, poiché i pazienti non contattabili, in particolare i deceduti, rappresentano proprio quella categoria di soggetti con outcome sfavorevoli che costituisce uno degli obiettivi primari di indagine dello studio.
In considerazione di tali elementi oggettivi, si configura una situazione di impossibilità organizzativa documentata che giustifica il ricorso al trattamento dei dati personali senza preventiva acquisizione del consenso informato individuale, in conformità con quanto previsto dal Provvedimento del Garante per la protezione dei dati personali.

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**: XACCETTABILE☐NON ACCETTABILE	
	Indicazioni:	Si raccomanda di fornire l'informativa al trattamento dei dati personali tramite pubblicazione su sito web aziendale in un documento separato rispetto a quello che contiene le informazioni sulla ricerca

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 **gestionedelle richieste di esercizio dei diritti degli interessati**?	
☒SÌ (Istruzione operativa collegata alla PA 262)	Allegare la **procedura** (All. n.)
☐ NO	Indicare come vengono **raccoltele richieste** degli interessati:
	mediante contatto telefonico o email presente sulla informativa privacy pubblicata sul sito aziendale
	Indicare la U.O. o il soggetto che **prende in carico** le richieste degli interessati:
	U.O.AFFARIGENERALI E LAGALI E PI
	PARERE DEL **DPO**: XACCETTABILE☐NON ACCETTABILE
	Indicazioni:

[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.

1.4.a Dati raccolti	Nell'ambito della ricerca vengono raccolte informazioni riguardanti: X Dati anagrafici dei partecipanti X Lo stato di salute dei partecipanti ☐ Dati genetici SPECIFICARE: Lo studio raccoglie dati anagrafici in forma pseudonimizzata attraverso l'identificativo univoco regionale di paziente. Le informazioni anagrafiche comprendono l'età o la data di nascita, il genere al momento del ricovero in Terapia Intensiva. Questi dati permettono di caratterizzare la popolazione in studio da un punto di vista demografico e di stratificare le analisi per fasce d'età, sesso e distribuzione geografica sul territorio dell'AUSL Romagna. Lo studio raccoglie informazioni cliniche dettagliate relative allo stato di salute dei partecipanti attraverso i flussi informativi correnti regionali. Le informazioni includono le diagnosi primarie e secondarie codificate secondo la classificazione ICD-9-CM, che identificano le patologie acute che hanno motivato il ricovero in Terapia Intensiva nonché le condizioni cliniche concomitanti. Vengono raccolte informazioni sulle comorbidità preesistenti, identificate attraverso l'indice di Charlson. Le procedure terapeutiche e diagnostiche eseguite durante il ricovero sono documentate attraverso i codici procedurali ICD-9-CM, includendo interventi quali ventilazione meccanica, ossigenazione extracorporea a membrana, emodialisi, monitoraggio emodinamico invasivo, tracheostomia, angioplastica coronarica e altri trattamenti intensivi. Vengono inoltre raccolti dati relativi alla durata della degenza in Terapia Intensiva e alla durata complessiva del ricovero ospedaliero, all'origine del paziente al momento dell'ammissione in Terapia Intensiva, se proveniente dal Pronto Soccorso, da altro reparto ospedaliero o trasferito da altro presidio ospedaliero, e alla destinazione alla dimissione dalla struttura ospedaliera. Per quanto riguarda gli esiti clinici, lo studio raccoglie informazioni sulla mortalità in Terapia Intensiva, sulla mortalità ospedaliera successiva alla dimissione dalla Terapia Intensiva e sulla mortalità a lungo termine, valutata a trenta giorni, novanta giorni, centottanta giorni, un anno e fino a cinque anni dopo la dimissione ospedaliera attraverso il Registro di Mortalità regionale. Vengono inoltre documentati i ricoveri ospedalieri successivi, includendo le riammissioni in Terapia Intensiva e le ospedalizzazioni ordinarie con relative diagnosi, gli accessi al Pronto Soccorso nel periodo post-dimissione con i relativi codici di triage e prestazioni erogate, e l'utilizzo di servizi specialistici ambulatoriali post-dimissione attraverso il flusso dell'Assistenza Specialistica Ambulatoriale. Infine, attraverso il flusso Laboratori vengono raccolte informazioni relative agli esami di laboratorio e alle analisi microbiologiche eseguite sui pazienti durante il percorso di cura. ☐ Altro SPECIFICARE:	
1.4.b Lo studio clinico prevede il trattamento di:	☐ dati personali di **partecipanti identificati**	es. nome e cognome
	X dati personali **pseudonimizzati**	es. i partecipanti sono indicati da un codice univoco

	☐ dati **anonimi**	i dati trattati non consentono di risalire all'identità dei partecipanti

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 necessariamente tutti 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	Il trattamento dei dati anagrafici risulta imprescindibile per il conseguimento delle finalità dello studio. L'età o la data di nascita costituisce una variabile fondamentale nell'analisi della popolazione in Terapia Intensiva, poiché l'età rappresenta uno dei principali fattori prognostici per la sopravvivenza e per gli esiti a lungo termine dei pazienti critici. La stratificazione per fasce d'età permette di identificare popolazioni particolarmente vulnerabili, quali i pazienti anziani o quelli in età pediatrica, e di valutare l'appropriatezza dei ricoveri in Terapia Intensiva in relazione all'età del paziente. Inoltre, l'analisi dei trend temporali nell'arco dei ventiquattro anni di studio richiede necessariamente la disponibilità del dato età per identificare eventuali modifiche nel profilo demografico dei pazienti ammessi in Terapia Intensiva nel corso del tempo. Il dato relativo al genere è parimenti necessario in quanto la letteratura scientifica documenta differenze significative tra uomini e donne nella risposta alle patologie acute, nell'accesso alle cure intensive e negli esiti clinici. L'analisi stratificata per genere permette di identificare eventuali disparità nell'assistenza e di caratterizzare in modo appropriato la popolazione in studio, garantendo che i risultati siano applicabili a entrambi i sessi
dati relativi allo stato di salute	Il trattamento dei dati relativi allo stato di salute costituisce il nucleo centrale dello studio e rappresenta la categoria di dati assolutamente necessaria per conseguire gli obiettivi della ricerca. Le diagnosi primarie e secondarie codificate secondo la classificazione internazionale delle malattie rappresentano l'elemento fondamentale per caratterizzare la casistica dei pazienti ricoverati in Terapia Intensiva. Senza la disponibilità di questi dati sarebbe impossibile descrivere le principali categorie diagnostiche che motivano il ricovero in ambito intensivo, identificare i trend temporali nelle tipologie di pazienti ammessi, confrontare il case mix tra le diverse Terapie Intensive dell'AUSL Romagna e stratificare le analisi di mortalità e di utilizzo dei servizi sanitari in base alla patologia di base. La diagnosi primaria costituisce inoltre un elemento essenziale per l'aggiustamento del rischio nelle analisi di mortalità, permettendo di confrontare pazienti con profili clinici comparabili.

comorbidità	Le informazioni sulle comorbidità preesistenti, quantificate attraverso l'indice di Charlson, sono necessarie per valutare il burden di malattia della popolazione in studio e per identificare i fattori di rischio associati a esiti sfavorevoli. La presenza di patologie croniche multiple rappresenta infatti uno dei principali determinanti della prognosi a lungo termine dei pazienti critici. L'analisi delle comorbidità permette inoltre di identificare popolazioni particolarmente fragili e di valutare l'appropriatezza del ricovero in Terapia Intensiva in relazione al carico di malattia del paziente. Senza la disponibilità di queste informazioni, qualsiasi analisi degli esiti sarebbe gravemente confusa dalla mancata considerazione delle condizioni cliniche preesistenti dei pazienti.
procedure terapeutiche e diagnostiche	I dati relativi alle procedure terapeutiche e diagnostiche eseguite durante il ricovero in Terapia Intensiva sono indispensabili per caratterizzare l'intensità delle cure ricevute dai pazienti e per identificare specifiche popolazioni sottoposte a trattamenti intensivi quali la ventilazione meccanica, l'ossigenazione extracorporea, la dialisi o il monitoraggio emodinamico invasivo. Queste informazioni permettono di valutare la complessità assistenziale dei pazienti, di confrontare l'utilizzo di diverse tecnologie tra i vari presidi ospedalieri dell'AUSL Romagna e di analizzare l'appropriatezza di specifici interventi, quali ad esempio la tracheostomia, in relazione agli esiti dei pazienti. Inoltre, l'identificazione dei pazienti sottoposti a procedure specifiche consente analisi di sottogruppo mirate, quali la valutazione della prognosi dei pazienti tracheostomizzati o di quelli sottoposti a terapia sostitutiva renale.
durata della degenza	La durata della degenza in Terapia Intensiva e la durata complessiva del ricovero ospedaliero costituiscono indicatori essenziali della gravità della malattia e dell'intensità delle cure ricevute. Questi dati permettono di identificare i pazienti con degenze prolungate, popolazione particolarmente vulnerabile e ad alto rischio di complicanze, di valutare l'utilizzo delle risorse intensive nel corso del tempo e di confrontare l'efficienza operativa tra le diverse Terapie Intensive dell'AUSL Romagna. La durata della degenza rappresenta inoltre un importante confondente nelle analisi di mortalità e di utilizzo dei servizi post-dimissione, la cui mancata considerazione comprometterebbe la validità delle analisi.
origine del paziente al momento dell'ammissione	L'informazione relativa all'origine del paziente al momento dell'ammissione in Terapia Intensiva e alla destinazione alla dimissione dalla struttura ospedaliera è necessaria per comprendere i percorsi assistenziali dei pazienti critici. La provenienza dal Pronto Soccorso, da altro reparto ospedaliero o da altro presidio ospedaliero caratterizza diverse tipologie di pazienti con differenti profili di urgenza e gravità. La destinazione alla dimissione, che può includere il domicilio, strutture di riabilitazione, lungodegenze o il decesso, rappresenta un importante outcome intermedio che riflette il grado di recupero funzionale del paziente e predice l'utilizzo successivo dei servizi sanitari.
dati relativi alla mortalità	I dati relativi alla mortalità in Terapia Intensiva, alla mortalità ospedaliera successiva e alla mortalità a lungo termine costituiscono gli outcome primari dello studio. Senza la disponibilità di queste informazioni sarebbe impossibile conseguire gli obiettivi secondari della ricerca, che prevedono la valutazione della prognosi a lungo termine dei pazienti critici, il confronto della mortalità con quella di pazienti ospedalizzati mai ammessi in Terapia Intensiva e con la popolazione generale, e l'identificazione dei fattori prognostici associati alla sopravvivenza. La disponibilità di dati di mortalità a diversi intervalli

	temporali, da trenta giorni fino a cinque anni, permette di caratterizzare la traiettoria di sopravvivenza dei pazienti e di identificare i periodi di maggiore vulnerabilità dopo la dimissione ospedaliera.
ricoveri ospedalieri successivi	Le informazioni relative ai ricoveri ospedalieri successivi, alle riammissioni in Terapia Intensiva e alle diagnosi associate costituiscono elementi essenziali per valutare il burden assistenziale dei pazienti critici dopo la dimissione e per identificare le principali cause di nuove ospedalizzazioni. Questi dati permettono di quantificare il fenomeno delle riammissioni, di identificare popolazioni ad alto rischio di riospedalizzazione e di valutare l'impatto del ricovero in Terapia Intensiva sull'utilizzo successivo delle risorse ospedaliere. La conoscenza delle diagnosi associate alle riammissioni consente inoltre di identificare le principali complicanze a medio e lungo termine dei pazienti critici.
accessi al Pronto Soccorso nel periodo post-dimissione	Gli accessi al Pronto Soccorso nel periodo post-dimissione rappresentano un importante indicatore dell'instabilità clinica dei pazienti e del loro bisogno di assistenza urgente. Questi dati permettono di quantificare l'utilizzo dei servizi di emergenza da parte dei pazienti dimessi dalla Terapia Intensiva, di identificare popolazioni con accessi frequenti che potrebbero beneficiare di percorsi assistenziali dedicati e di valutare la qualità della transizione dall'ospedale al territorio. I codici di triage e le prestazioni erogate consentono inoltre di caratterizzare la gravità degli accessi e le motivazioni che li hanno determinati.
utilizzo di servizi specialistici ambulatoriali	L'utilizzo di servizi specialistici ambulatoriali post-dimissione fornisce informazioni sul bisogno assistenziale dei pazienti critici dopo il ritorno al domicilio e permette di identificare le principali specialità mediche coinvolte nel follow-up. Questi dati sono necessari per quantificare il carico assistenziale complessivo dei pazienti dimessi dalla Terapia Intensiva e per valutare l'adeguatezza del percorso di continuità assistenziale dopo la dimissione ospedaliera.

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

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: NECESSITà DI RISALIRE A DATI MANCANTI ERRATI O INCOMPLETI, RISCONTRATA DURANTE LA FASI SUCCESSIVE RISPETTO ALL'ESTRAZIONE DATI
PARERE DEL **DPO**: XACCETTABILE☐NON ACCETTABILE	
Indicazioni:	

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 verifica dell'esattezza dei dati raccolti viene condotta mediante un approccio sistematico articolato su diversi livelli di controllo qualità. I flussi informativi correnti regionali dell'Emilia-Romagna sono sottoposti a procedure standardizzate di validazione alla fonte da parte delle strutture sanitarie e del sistema informativo sanitario regionale. La natura istituzionale di questi flussi e il loro utilizzo consolidato per finalità amministrative e di programmazione sanitaria garantiscono un elevato livello di completezza e accuratezza. La verifica viene ulteriormente assicurata mediante controlli di coerenza interna ed esterna. I controlli interni identificano incongruenze logiche quali date incompatibili, codici non validi o valori anomali. I controlli esterni prevedono verifiche incrociate tra diversi flussi informativi, confrontando ad esempio la data di decesso registrata nel Registro di Mortalità regionale con eventuali ricoveri o accessi al Pronto Soccorso successivi.

[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.

	L'esattezza viene inoltre valutata mediante analisi di plausibilità clinica ed epidemiologica, verificando che la distribuzione delle variabili e la sequenza temporale degli eventi siano coerenti con la letteratura scientifica e l'esperienza clinica consolidata. Vengono implementate procedure di identificazione e gestione dei valori mancanti e degli outlier, documentando eventuali pattern sistematici e valutandone l'impatto mediante analisi di sensibilità.
Chi verifica l'esattezza (correttezza) dei dati?	Personale addetto all'estrazione dei dati e PI

	PARERE DEL **DPO**: XACCETTABILE☐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
tutti i dati	3 anni	Tempo necessario per conseguire gli obiettivi dello studio

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

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. AUSL ROMAGNA**	**1. Province di Forli-Cesena, Ravenna, Rimini**	**70000**
	2.	**2.**	
	3.	**3.**	
	4.	**4.**	
	5.	**5.**	
	6.	**6.**	
	7.	**7.**	
	8.	**8.**	
	9.	**9.**	

1.5.b Comunicazione	I dati vengono comunicati alle seguenti categorie di soggetti <u>esterni</u>:	☐ Promotore (Azienda farmaceutica) ☐ Promotore (Azienda fabbricante di dispositivi medici) ☐ClinicalResearch 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 X Solo in forma aggregata per fini di pubblicazione scientifica
1.5.e Chi tratta i dati personali dei partecipanti alla ricerca?	X Personale sanitario X Personale tecnico X Ricercatori ☐ Personale di laboratorio ☐ Altro:	Sono stati autorizzati con specifica nomina? XSI (il PI verrà nominato responsabile interno del trattamento dei dati al momento della determinazione di nulla osta allo studio e, a sua volta, nominerà i collaboratori autorizzati al trattamento)☐NO ☐ Solo alcuni Hanno ricevuto la formazione privacy? X SI ☐ NO ☐ Solo alcuni

Soggetti	**Motivazione dell'accesso**
Personale sanitario	PI dello studio
personale tecnico/ricercatori	estrazione dati e analisi

	PARERE DEL **DPO**: XACCETTABILE☐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 X**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**: XACCETTABILE☐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.

Ilrischio 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).*

☐ **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**	

[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)

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** XAccesso 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.) XSottrazione da parte di soggetti interni o esterni alla struttura di documenti cartacei o di strumenti elettronici (pc) XInfezione del sistema tramite software nocivi diffusi via mail o attraverso internet (es. trojanhorse, malware, spyware, cryptolocker, ransomware, 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:**	Impatto sui **dirittie le libertà** degli interessati:	**Livello di impatto** della perdita di riservatezza dei dati:
omissis	omissis	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			
		Improbabile	Poco probabile	Probabile	Molto probabile
I	Gravissimo				
	Grave				
	Medio				
	Lieve				

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?	omissis

8. Misure di sicurezza:	X 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	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**: XACCETTABILE☐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. trojanhorse, malware, spyware, cryptolocker, ransomware, 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 **dirittie 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 mitigazionedel 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**: XACCETTABILE☐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**
XLa 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. trojanhorse, malware, spyware, cryptolocker, ransomware, 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 **dirittie 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			
		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?	☐ Misure di protezione dagli attacchi informatici [*descrizione delle misure*:_____] ☐ Backup [*descrizione delle modalità di backup*:back up su server aziendal] ☐ Cloud [*descrizione del cloud*:_____] ☐ 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 mitigazionedel 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**: XACCETTABILE☐NON ACCETTABILE
	Indicazioni:

Lo Sperimentatore principale _____

Per l'UO Governo Sistemi Informativi _____

Per l'UO Affari Generali e Legali: Il Direttore _____

Il 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** dirittie 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_____	_____	
3b. **Perdita di integrità** dei dati *(Modifica non autorizzata o accidentale)*	**Conseguenze** per gli interessati della perdita di integrità dei dati:	Impatto sui **dirittie 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.)	

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

	☐ Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	☐ La perdita di integrità non è configurabile
	☐ 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 **dirittie 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			
		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. 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			
		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. 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 mitigazionedel 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