Valutazione di Impatto

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

relativa al progetto di ricerca

Studio osservazionale ambispettivo ECHOS [Evaluation of clinical outcomes of Chemotherapy or androgen-receptor targeting agent (alone or combined) or radiotherapy on primary tumor in addition to androgen deprivation therapy in HOrmone-Sensitive metastatic prostate cancer patients]

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	Azienda Provinciale per i Servizi Sanitari (APSS) della Provincia Autonoma di Rento
Titolo dello studio	Valutazione degli outcomes clinici della chemioterapia o della terapia contro il Recettore degli androgeni (da sole o in Combinazione) o della radioterapia sul tumore primitivo in associazione a terapia ormonale nel carcinoma della prostata metastatico in fase ormonosensibile. Studio osservazionale multicentrico su pazienti sottoposti a trattamento nella pratica clinica negli ospedali italiani - ECHOS
Codice dello studio	Non applicabile
Redattori	Dott. Orazio Caffo (principal investigator), unità operativa oncologia medica, Ospedale Santa Chiara, Azienda Provinciale per i Servizi Sanitari, Provincia Autonoma di Trento
Verificatore interno	Dott. Emanuele Torri
DPO	Avv. Silvia Stefanelli
Versione	1
Data Revisione	13/08/2024

Indice del documento

Obiettivo e organizzazione del documento.

Questo documento, organizzato in sezioni, rappresenta la Valutazione di Impatto Privacy *(Data Protection Impact Assessment - DPIA)* di una attività di trattamento di dati personali ai sensi dell'art. 35 GDPR, finalizzata ad analizzare l'impatto sulla protezione dei dati personali di un trattamento.

Ai sensi dell'art. 35 del GDPR la Valutazione di Impatto deve essere effettuata quando un'attività di trattamento di dati personali è in grado di determinare un rischio elevato per i diritti e le libertà delle persone fisiche alle quali i dati si riferiscono (interessati).

La Valutazione di Impatto deve essere effettuata **prima** di mettere in atto il trattamento dei dati personali[1], coerentemente con il principio di Privacy by design e privacy by default[2] per individuare la necessità di implementare misure di sicurezza ulteriori rispetto a quelle già in atto e finalizzate a mitigare i rischi.

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

La presente Valutazione di Impatto è stata redatta secondo presenta i seguenti *step*:

1. Definizione del contesto in cui avviene l'attività di trattamento;
2. Descrizione sistematica dell'attività di trattamento con particolare attenzione al flusso dei dati;
3. Descrizione delle modalità di rispetto dei principi applicabili al trattamento dei dati personali[3];
4. Descrizione delle modalità di gestione dei diritti degli interessati[4];
5. Descrizione degli adempimenti relativi ai responsabili del trattamento[5] e degli autorizzati al trattamento[6];
6. Individuazione delle basi di legittimità dell'eventuale trasferimento dei dati in Paesi extra UE[7];
7. Individuazione delle minacce a cui è esposta l'attività di trattamento e delle vulnerabilità, calcolo del rischio inerente (probabilità e impatto), indicazione delle misure in atto, calcolo del rischio residuo, individuazione delle eventuali contromisure di mitigazione, valutazione dell'accettabilità del rischio residuo per verificare se mettere in atto il trattamento o ricorrere allo strumento della consultazione preventiva al Garante per la protezione dei dati personali[8].

La metodologia seguita per la redazione della DPIA soddisfa gli standard richiesti dal GDPR in quanto conforme ai criteri previsti dall' "Allegato 2 – Criteri per una DPIA ammissibile" alle Linee guida sulla Valutazione d'Impatto nella protezione dei dati (DPIA) e stabilire se il trattamento "può comportare un rischio elevato" ai sensi del regolamento 2016/679 (WP 248 rev.01).

[1] Considerando 90 e 93 e Artt. 35, par. 2 e 10, GDPR).
[2] Considerando 78 e Art. 25 GDPR.
[3] Art. 5 GDPR.
[4] Artt. 15-22 GDPR.
[5] Art. 28 GDPR
[6] Art. 29 GDPR e Art. 2-*quaterdecies* D. Lgs. 196/2003 (Codice Privacy);
[7] Capo V GDPR.
[8] Art. 36 GDPR.

1. Definizione del contesto.

Raccolta di dati da cartella clinica informatizzata nell'ambito di studio osservazionale multicentrico italiano coordinato dall'UO di Oncologia Medica su pazienti affetti da neoplasia della prostata metastatica sensibile alla castrazione. I dati vengono conservati su piattaforma informatizzata fornita da gestore esterno. Lo studio è stato approvato nel 2016 e sottoposto a successivi emendamenti: allo stato sono stati arruolati oltre 2000 pazienti in oltre 70 ospedali italiani. Quest'anno è stato presentato ulteriore emendamento per proseguire lo studio fino al 2026 ed estendere ad altri trattamenti l'arruolamento dei pazienti. Il Comitato Etico dell'APSS di Trento ha dato parere sospensivo anche in attesa di valutazione del DPIA.

1.1 La titolarità del trattamento.

1.1.1 Titolare.

RAGIONE SOCIALE	AZIENDA PROVINCIALE PER I SERVIZI SANITARI DELLA PROVINCIA DI TRENTO
SEDE LEGALE	VIA DEGASPERI 79, 38123 TRENTO
INDIRIZZO MAIL	DIRGEN@APSS.TN.IT
INDIRIZZO PEC	APSS@PEC.APSS.TN.IT
DPO	RESPONSABILEPROTEZIONEDATI@APSS.TN.IT

1.1.2 Contitolari.

Non applicabile

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

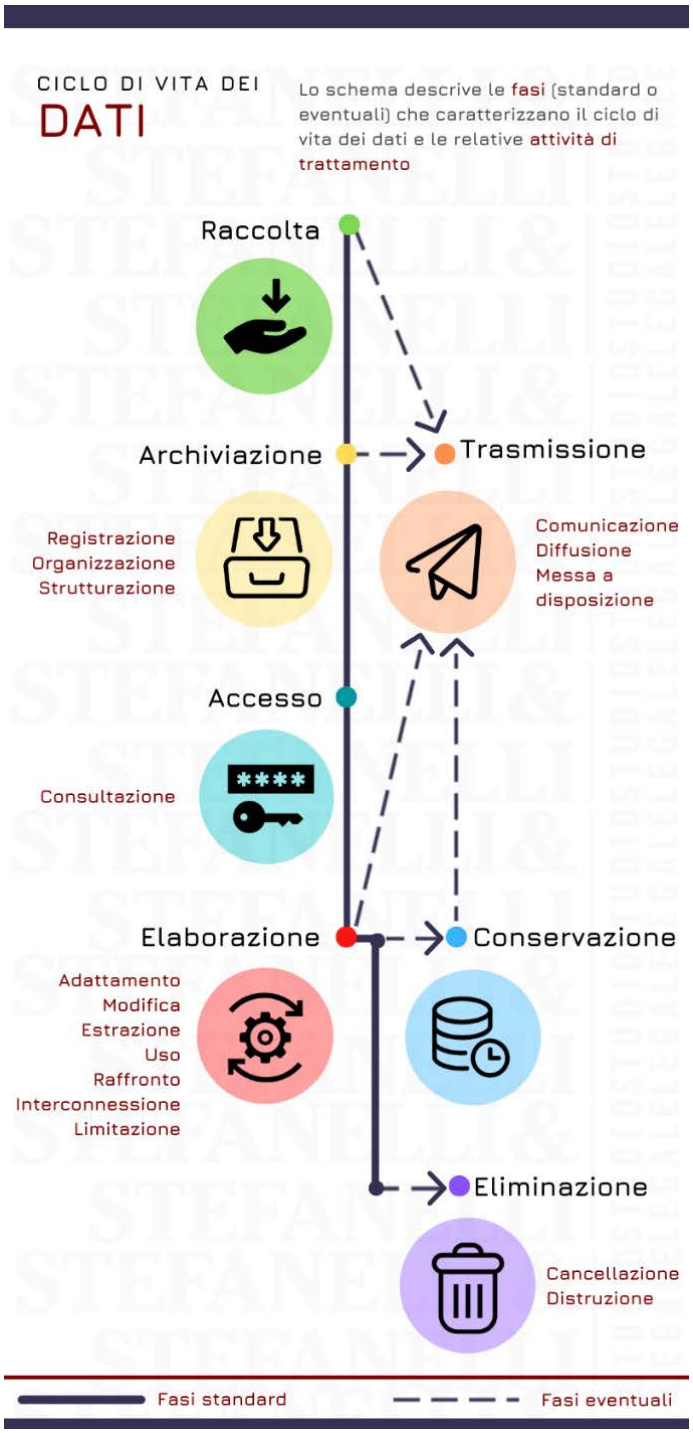
In questo paragrafo sono individuate le caratteristiche generali dello studio clinico.

1.2.a Breve descrizione del progetto di ricerca 	ECHOS è uno studio osservazionale il cui obiettivo principale è quello di raccogliere dati real-world da vari centri italiani sulla gestione del trattamento medico o radiante in pazienti affetti da tumore della prostata metastatico in fase ormonosensibile, mettendone in luce gli outcomes clinici in relazione al tipo di terapia effettuata.	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. 1)
1.2.b Tipo di ricerca 	☐ Studio unicentrico x Sudio multicentrico x Studio osservazionale ☐ 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 Dati raccolti 	Nell'ambito della ricerca vengono raccolte informazioni riguardanti: x L'identità dei partecipanti x Lo stato di salute dei partecipanti ☐ Dati genetici SPECIFICARE: - Variabili anagrafiche: data di nascita. - Variabili relative alla storia clinica: comorbidità presenti, diagnosi di neoplasia prostatica (data della diagnosi, stadio iniziale, Gleason score), trattamenti radicali ricevuti per la malattia primaria (chirurgia e/o radioterapia), sede e numero di metastasi al momento di inizio trattamento. - Variabili relative al trattamento con docetaxel, farmaci antiandrogeni di nuova generazione (da soli o in combinazione) o con radioterapia sul tumore primitivo: stadi azione strumentale basale e finale, parametri ematochimici basali, in corso di trattamento e finali (antigene prostatico specifico, emocromo, lattico-deidrogenasi, fosfatasi alcalina), presenza di dolore al momento dell'inizio del trattamento, parametri clinici basali, in corso di trattamento e finali (performance status, presenza di dolore, uso di analgesici), timing della terapia di privazione degli androgeni (data inizio, tipo di terapia), data inizio e fine del trattamento, caratteristiche del trattamento radiante (dosi erogate e campi di trattamento (nel caso della radioterapia sul tumore primitivo, tossicità durante il trattamento (secondo criteri NCI CTCAE versione 5.0). - Variabili successive al trattamento con docatexal, farmaci antiandrogeni di nuova generazione (da soli o in combinazione) o con radioterapia sul tumore primitivo: data e tipologia della progressione dopo trattamento, terapie successive ricevute (tipologia, data di inizio e fine, risposta biochimica e obiettiva), dati relativi alla sopravvivenza ☐ Altro SPECIFICARE: Non applicabile	
1.2.d Consenso informato 	Viene prevista l'acquisizione del consenso informato allo studio: x SI (per i soggetti ancora in vita) ☐ NO	

1.2.e Comitato Etico 	Il progetto di ricerca ha ottenuto **motivato parere favorevole** dal competente Comitato Etico a livello territoriale? x **SI** (Prima approvazione: 10/03/16 , seguono emendamenti) ☐ **NO** ☐ in corso di sottomissione

2. Rappresentazione del ciclo di vita dei dati *(a cura del P.I., dei Ricercatori e del Responsabile IT).*

Segue l'immagine che graficizza il ciclo di vita dei dati suddiviso in quattro fasi che comprendono le operazioni elencate nell'art. 4.2 del GDPR.



2.1 Fase della raccolta dei dati.

In questo paragrafo sono indicate le modalità e i mezzi impiegati per effettuare l'attività di raccolta dei dati.

RACCOLTA

Come vengono raccolti i dati?	In che contesto vengono raccolti i dati?
☐ Sono forniti direttamente dall'interessato ☐ Sono forniti da un soggetto diverso dall'interessato ☐ Vengono raccolti da registri di patologia x sono raccolti dalle cartelle cliniche informatizzate dei pazienti	☐ Sono raccolti da partecipanti **appositamente arruolati** per lo studio x Sono raccolti da **pazienti** a cui viene proposta la partecipazione allo studio x Vengono raccolti da pazienti **precedentemente in cura** *[barrare questa opzione in caso di studi retrospettivi]* ☐ _____

Quali risorse vengono utilizzate per raccogliere i dati?
x Hardware (computer, router, supporti elettronici USB, etc.)
x Software (eCRF, sistemi di messaggistica, database, app, etc.)
x Reti di comunicazione (cavi, Wi-Fi, fibra ottica, etc.)
x Supporti cartacei (stampe, fotocopie, etc.)
☐ Canali di trasmissione cartacei (posta, consegna manuale, etc.)
☐ _____

2.2 Fase della archiviazione dei dati.

In questo paragrafo sono indicate le modalità e i mezzi impiegati per effettuare l'attività di archiviazione dei dati.

<table>
<tr><td colspan="4">ARCHIVIAZIONE
 
Si intende lo storage dei dati a breve e medio termine, ossia l'archiviazione dei dati finalizzata a una elaborazione degli stessi a breve e medio termine.</td></tr>
<tr><td>I dati vengono archiviati:</td><td>Dove vengono archiviati i dati?</td><td>Da chi vengono archiviati i dati?</td><td>Dove è ubicato l'archivio?</td></tr>
<tr><td rowspan="3">x Tramite intervento umano
☐ Tramite un processo automatizzato
☐ Entrambi
☐ _____</td><td rowspan="3">☐ Archivi cartacei
x Archivi informatici
☐ _____</td><td>x Dal Titolare
x Da soggetto esterno
☐ Dal contitolare
☐ _____</td><td>☐ In azienda (sede principale o distaccata)
☐ In una filiale dell'azienda
☐ Presso un soggetto terzo
x In cloud
☐ _____</td></tr>
<tr><td>Indicare chi archivia i dati e chi può accedere ai dati archiviati:</td><td>Indicare l'ubicazione specifica dell'archivio:</td></tr>
<tr><td>- Titolare dei Dati
- Personale di CVM-Stat S.r.l individuato nell'allegato 4</td><td>Archiviazione effettuata tramite servizio Object Storage di proprietà di CVM-Stat S.r.l</td></tr>
</table>

2.3 Fase dell'accesso ai dati.

In questo paragrafo sono indicate le modalità e i mezzi impiegati per effettuare l'attività di accesso ai dati.

ACCESSO	
L'accesso ai dati è:	Ai dati è possibile accedere tramite accesso a:
x Fisico	x edificio/sede x ufficio ☐ sala server ☐ archivi cartacei
x Logico	Ai dati è possibile accedere tramite accesso a: x server ☐ cartelle di rete x computer desktop x notebook ☐ tablet ☐ smartphone

Categorie di soggetti appartenenti al personale aziendale autorizzati ad **accedere** ai dati:	MOTIVAZIONE DELL'ACCESSO	I SOGGETTI ACCEDONO AI DATI:		
x Principal Investigator	Verifica della sussistenza di criteri di inclusione/esclusione, raccolta dati, registrazione dei dati nella eCRF, elaborazione dei dati e verifica di eventuale cancellazione	x in chiaro ☐ in modalità pseudonimizzata ☐ _____		
☐ Ricercatori		☐ in chiaro ☐ in modalità pseudonimizzata ☐ _____		
x Amministratori di Sistema	Risoluzioni eventuali problemi informatici o manutenzione del sistema(vedere allegato 3 o 4)	☐ in chiaro x in modalità pseudonimizzata ☐ _____		
☐ Personale IT		☐ in chiaro ☐ in modalità pseudonimizzata ☐ _____		
☐ Personale sanitario		☐ in chiaro ☐ in modalità pseudonimizzata ☐ _____		
☐ Medici specialisti		☐ in chiaro ☐ in modalità pseudonimizzata ☐ _____		
☐ Data scientists		☐ in chiaro ☐ in modalità pseudonimizzata ☐ _____		

2.4 Fase dell'elaborazione dei dati.

In questo paragrafo sono indicate le modalità e i mezzi impiegati per effettuare l'attività di elaborazione dei dati.

ELABORAZIONE
Indicare la tipologia di trattamento [*possono essere fornite più risposte*]:
☐ Analisi dei dati tramite modalità cartacea ☐ Analisi dei dati tramite software di intelligenza artificiale ☐ Analisi dei dati tramite software di sanità digitale ☐ Monitoraggio tramite dispositivi wearable ☐ Trattamento su larga scala di dati genetici x Analisi dei dati tramite software statistico

Soggetti appartenenti al personale aziendale che elaborano i dati:	**Software con cui vengono elaborati i dati:**
x Principal Investigator	IBM SPSS Statistics
☐ Ricercatori	MedCalc statistical software
☐ _____	
☐ _____	

2.5 Fase della trasmissione dei dati.

In questo paragrafo sono indicate le modalità e i mezzi impiegati per effettuare l'attività di trasmissione dei dati.

TRASMISSIONE			
Indicare le <u>categorie</u> di soggetti esterni a cui vengono trasmessi i dati o che hanno accesso agli stessi:	Inserire le <u>ragioni sociali</u> dei singoli soggetti esterni destinatari dei dati, il relativo ruolo privacy e le modalità di trasmissione		
☐ Promotore (Azienda farmaceutica) ☐ Promotore (Azienda fabbricante di dispositivi medici) ☐ Clinical Research Organization (CRO) ☐ Centro coordinatore ☐ Centri partecipanti x Cloud provider x Azienda di sviluppo software ☐ Azienda di manutenzione hardware ☐ Consulenti esterni ☐ Strutture sanitarie x Società di servizi ☐ Istituzioni	RAGIONE SOCIALE DEI DESTINATARI	RUOLO PRIVACY	MODALITÀ DI TRASMISSIONE/ ACCESSO AI DATI
	CVM-Stat S.r.l	☐ Responsabile ☐ Titolare autonomo ☐ Contitolare	☐ in chiaro x in modalità pseudonimizzata ☐ _____
		☐ Responsabile ☐ Titolare autonomo ☐ Contitolare	☐ in chiaro ☐ in modalità pseudonimizzata ☐ _____
		☐ Responsabile ☐ Titolare autonomo ☐ Contitolare	☐ in chiaro ☐ in modalità pseudonimizzata ☐ _____

_____	
I dati della ricerca vengono **diffusi?**	☐ SI ☐ NO x Solo in forma aggregata per fini di pubblicazione scientifica

2.6 Fase della conservazione dei dati.

In questo paragrafo sono indicate le modalità e i mezzi impiegati per effettuare l'attività di conservazione dei dati.

CONSERVAZIONE  *Si intende la conservazione dei dati in archivi a lungo termine finalizzata a tenere a disposizione i dati per obblighi di legge e/o per effettuare trattamenti sporadici e/o eventuali.*			
I dati:	**Dove vengono conservati i dati a lungo termine?**	**Da chi vengono archiviati i dati nell'archivio a lungo termine?**	**Dove è ubicato l'archivio a lungo termine?**
x Vengono conservati ☐ Non vengono conservati ☐ _____	☐ Archivio cartaceo x Archivio informatico ☐ _____	x Dal Titolare x Da soggetto esterno ☐ Dal contitolare ☐ _____	☐ In azienda (sede principale o distaccata) ☐ In una filiale dell'azienda ☐ Presso un soggetto terzo x In cloud ☐ _____
		Indicare chi è addetto alla conservazione dei dati e chi può accedere all'archivio a lungo termine:	**Indicare l'ubicazione specifica dell'archivio:**
		- Titolare di dati - **Personale di CVM-Stat S.r.l individuato nell'allegato 3**	Conservazione effettuata tramite servizio Object Storage di proprietà di CVM-Stat S.r.l

2.7 Fase della eliminazione dei dati.

In questo paragrafo sono indicate le modalità e i mezzi impiegati per effettuare l'attività di eliminazione dei dati.

ELIMINAZIONE

Si intende la cancellazione temporanea dei dati o la loro eliminazione definitiva secondo quanto previsto dal Doc-Web:1574080 del Garante per la protezione dei dati personali "Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori" del 12/12/08

I dati:	Indicare il metodo di eliminazione dei documenti <u>cartacei</u> contenenti dati:
☐ Non vengono eliminati ☐ Vengono cancellati x Vengono eliminati con sistemi di cancellazione sicura ☐ _____	☐ Inserimento nel cestino dei rifiuti ☐ Trita carte ☐ Società certificata per lo smaltimento sicuro dei documenti sensibili ☐ Nessuno ☐ _____
	Indicare il metodo di eliminazione dei documenti <u>elettronici</u> contenenti dati:
	☐ Cancellazione del file (spostamento nel cestino) x Formattazione ☐ Demagnetizzazione ☐ Distruzione fisica ☐ Società certificata per lo smaltimento sicuro dei documenti sensibili ☐ Nessuno ☐ _____

3. Conformità alla normativa in materia di protezione dei dati *(a cura del P.I., dei Ricercatori e del Referente Privacy).*

3.1. Criteri indicativi di rischio elevato *(a cura del Referente 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? _____ x NO

3.2. Rispetto del principio di finalità *(a cura del P.I., Ricercatori e del Referente).*

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 	
Le finalità del trattamento sono indicate nell'informativa privacy dello studio in maniera specifica?	x SÌ ☐ NO
Il trattamento di dati verrà effettuato solo per le finalità indicate nell'informativa?	x SÌ ☐ NO
Se la risposta alla domanda precedente è NO indicare le finalità ulteriori:	

L'informativa verrà fornita a tutti i soggetti in vita. Per i soggetti deceduti (i cui dati verranno raccolti retrospettivamente) non sarà possibile invece fornire un'informativa privacy.

3.3. Rispetto del principio di liceità *(a cura del Referente 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) *	Il trattamento è necessario ai fini di ricerca scientifica
	☐ 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) *	Il trattamento è necessario ai fini di ricerca scientifica
	x 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.** *	Il trattamento è necessario ai fini di ricerca scientifica
	☐ _____	
Dati comuni e particolari	x Il consenso non è necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.	Il trattamento è necessario ai fini di ricerca scientifica. Si ritiene necessario raccogliere anche i dati di pazienti deceduti in quanto risultano necessari per garantire la validità dello studio

3.4. Rispetto del principio di liceità attraverso la raccolta del consenso *(a cura del P.I., Ricercatori e del Referente 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 e/o art. 9.2-a GDPR)

CONSENSO	
Viene richiesto al partecipante il consenso **al trattamento dei dati personali**? (N.B.: è diverso dal consenso informato)	x SÌ, qualora possibile ☐ NO
Il modulo di consenso al trattamento dei dati personali è separato rispetto al modulo di consenso informato allo studio?	
x SI ☐ NO	
È stata prevista una procedura interna per gestire la revoca del consenso?	**Descrivere come viene tenuta traccia del consenso:** x tramite copia firmata del modulo di consenso cartaceo ☐ _____
x **SI** ☐ **NO**	(possono essere fornite più risposte) In caso di revoca del consenso: ☐ il trattamento viene interrotto

	x i dati vengono cancellati ☐ altro. SPECIFICARE: i soggetti vivi che hanno fornito il consenso al trattamento dei dati personali possono revocare il consenso in qualsiasi momento comunicandolo al ricercatore. Per tutelare i soggetti deceduti che, per palesi ragioni, non possono revocare un consenso al trattamento dei dati personali, è stata predisposto un aggiornamento della valutazione di impatto a cadenza regolare.

3.5. Consultazione degli interessati *(a cura del Referente 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.

3.6. Rispetto del principio di trasparenza *(a cura del P.I., Ricercatori e del Referente 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 al partecipante una specifica informativa **sul trattamento dei dati personali** (N.B.: è diversa dall'informativa sullo studio)	L'informativa al trattamento dei dati personali è contenuta in un documento separato rispetto a quello che contiene le informazioni sulla ricerca	Fornire l'informativa agli interessati:
x SÌ ☐ NO	x SÌ ☐ NO	x è possibile (pazienti in vita) x è impossibile ☐ richiede uno sforzo sproporzionato x rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca (pazienti deceduti)

3.7. Misure di protezione dei diritti degli interessati *(a cura del P.I., Ricercatori e del Referente 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**?	
x SÌ	Allegare la **procedura** (All. n.)
☐ NO	Indicare come vengono **raccolte le richieste** degli interessati:
	Richiesta all'Ufficio Rapporti con il Pubblico (URP)
	Indicare la funzione aziendale/U.O. o il soggetto che **prende in carico** le richieste degli interessati:
	Ufficio Rapporti con il Pubblico (URP)

3.8. Rispetto del principio di minimizzazione *(a cura del P.I., Ricercatori del Referente 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 1.2.c. devono essere trattati necessariamente tutti per conseguire le finalità del trattamento. Motivare per ognuna delle tipologie di dato selezionate al paragrafo 1.2.c:

Tipologia di dato	**Motivazione**
Variabili anagrafiche	Definire l'età del paziente
Variabili relative alla storia clinica	Definire le caratteristiche anamnestiche in grado di influenzare la risposta al trattamento
Variabili relative al trattamento con docetaxel, farmaci antiandrogeni di nuova generazione (da soli o in combinazione) o con radioterapia sul tumore primitivo	Definire le caratteristiche di somministrazione delle terapie, gli effetti collaterali e la risposta ad esse
Variabili successive al trattamento con docatexal, farmaci antiandrogeni di nuova generazione (da soli o in combinazione) o con radioterapia sul tumore primitivo	Definire la progressione di malattia, le eventuali terapie successive ad essa, sopravvivenza

3.9. 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 x NO

☐ SÌ, i dati verranno resi anonimi [9] ⚠ x NO	I dati non verranno resi anonimi perché: Necessità di riaccesso ai dati clinici originali per aggiornamento del follow-up o per risoluzione delle query. La piattaforma genera un codice identificativo univoco associato ad ogni soggetto coinvolto nello studio.

3.10. Rispetto del principio di esattezza *(a cura del P.I., Ricercatori e del Referente 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 dei dati?	Confronto fra dati inseriti in eCRF e quelli presenti nella cartella clinica
Chi verifica l'esattezza dei dati?	Principal Investigator

3.11. Rispetto del principio di limitazione della conservazione *(a cura del P.I., Ricercatori e del Referente 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**
Variabili anagrafiche	Cinque anni dopo la conclusione dello studio	Consentire eventuali analisi aggiuntive sulla scorta di eventuali nuove esigenze di studio in riferimento all'evoluzione delle conoscenze scientifiche.
Variabili relative alla storia clinica	Cinque anni dopo la conclusione dello studio	Consentire eventuali analisi aggiuntive sulla scorta di eventuali nuove esigenze di studio in riferimento all'evoluzione delle conoscenze scientifiche.
Variabili relative al trattamento	Cinque anni dopo la	Consentire eventuali analisi

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

con docetaxel, farmaci antiandrogeni di nuova generazione (da soli o in combinazione) o con radioterapia sul tumore primitivo	conclusione dello studio	aggiuntive sulla scorta di eventuali nuove esigenze di studio in riferimento all'evoluzione delle conoscenze scientifiche.
Variabili successive al trattamento con docatexal, farmaci antiandrogeni di nuova generazione (da soli o in combinazione) o con radioterapia sul tumore primitivo	Cinque anni dopo la conclusione dello studio	Consentire eventuali analisi aggiuntive sulla scorta di eventuali nuove esigenze di studio in riferimento all'evoluzione delle conoscenze scientifiche.

3.12. Soggetti esterni *(a cura del P.I., Ricercatori e del Referente 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

3.12.a Centri di sperimentazione[1] 	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.	1.	
	2.	2.	
	3.	3.	
	4.	4.	
	5.	5.	
	6.	6.	
	7.	7.	
	8.	8.	
	9.	9.	
3.12.c Nomina a responsabile del trattamento 	Indicare soggetti esterni a cui vengono comunicati i dati o che possono accedere ai dati		
	1. CVM-Stat S.r.l		
	2.		
	3.		
	4.		
	5.		
	6.		
	7.		
	8.		
	9.		

[1]Considerazioni del PI rispetto ai centri di sperimentazione:

- I centri coinvolti nella sperimentazione sono elencati nell'allegato 2; il numero dei pazienti per singolo centri non è prevedibile.
- I ricercatori sono individuati come Principal Investigator dai rispettivi Comitati Etici.
- Ii ricercatori dei singoli centri possono accedere eslusivamente ai dati dei pazienti del proprio centro.

3.13. Contitolari del trattamento *(a cura del Referente Privacy).*

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

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

3.14 Trasferimento dei dati extra UE *(a cura del P.I., Ricercatori e del Referente 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:

4. 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.*[10]

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 delle minacce**;
- poi viene analizzato **l'impatto** o danno conseguente in caso di accadimento;
- tenuto conto poi delle minacce e del possibile impatto, viene valutato il **rischio**.

Tale rischio è denominato **rischio inerente:** vale a dire il rischio 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[11].

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 implementato le misure di sicurezza sul rischio inerente[12].

Infine:

- Se il rischio residuo viene valutato come **accettabile**, potrà procedersi con l'attività di trattamento dei dati.
- Se il rischio residuo viene invece valutato come **non accettabile** (in quanto 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 4.1., 4.2. e 4.3. deve seguire le istruzioni riportate nell'Allegato 1.

10 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;
11 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.
12 Guida ISO/IEC 73/2009: 3.8.1.6 rischio residuo: rischio (1.1) rimanente dopo il trattamento del rischio (3.8.1)

4.1. Perdita di riservatezza *(a cura del P.I., Ricercatori, del Personale Tecnico e del Referente Privacy limitatamente al punto 3 della tabella sottostante).*

☐ **La perdita di riservatezza dei dati non ha impatto sui diritti e le libertà degli interessati**	**Se è stata spuntata questa casella, la tabella sotto riportata NON deve essere compilata**

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?	☐ 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) x Infezione del sistema tramite software nocivi diffusi via mail o attraverso internet (es. trojan horse, malware, spyware, cryptolocker, ransmoware, etc.) ☐ Intercettazione del traffico Ethernet; acquisizione dei dati inviati su una rete Wi-Fi, ☐ Condivisione dei dati con soggetti non autorizzati ☐ _____	
2. Quali sono le principali **vulnerabilità** rilevate?	☐ Salvataggio dei dati su chiavette USB o dischi esterni personali ☐ Inefficacia delle tecniche di pseudonimizzazione o crittografia x Mancata formazione del personale o formazione risalente ☐ Locali non protetti da accessi esterni ☐ Strumenti non protetti da attacchi informatici ☐ Mancata adozione di una policy per il corretto utilizzo degli strumenti informatici ☐ _____	
3.**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
☐ 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	
x Perdita di riservatezza dei dati personali protetti da segreto professionale	Rivelazione del segreto professionale (art. 622 c.p.)	
☐ Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
☐ altro_____	_____	
4. Stima della **probabilità** di accadimento delle minacce	x Improbabile 1 ☐ Poco probabile 2	

(fattore **P** della formula di calcolo del Rischio)	☐ Probabile 3 ☐ Molto probabile 4
5. Stima dell'**impatto** (fattore **I** della formula di calcolo del Rischio)	x 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	x 1	☐ 2	☐ 3	☐ 4

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?	☐ crittografia [*descrizione delle tecniche di crittografia*:_____] x pseudonimizzazione [*descrizione delle tecniche di pseudonimizzazione*: descrizione disponibile nell'allegato 3 x limitazione degli accessi [*descrizione delle modalità*: descrizione disponibile nell'allegato 3] x Misure di protezione dagli attacchi informatici [*descrizione delle misure*: descrizione disponibile nell'allegato 3] ☐ Adozione di una policy per il corretto utilizzo degli strumenti informatici ☐ Formazione del personale ☐ _____			
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	x 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**	x accettabile (1-6)	☐ non accettabile (8-16)
	attuazione del trattamento	consultazione preventiva

4.2. Perdita di integrità *(a cura del P.I., Ricercatori, del Personale Tecnico e del Referente Privacy limitatamente al punto 3 della tabella sottostante).*

☐ **La perdita di integrità dei dati non ha impatto sui diritti e le libertà degli interessati**	**Se è stata spuntata questa casella, la tabella sotto riportata NON deve essere compilata**

Modifica non autorizzata 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?	☐ Malfunzionamento dell'hardware ☐ Malfunzionamento del software ☐ Deterioramento degli strumenti informatici x 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 x 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	
x Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
☐ altro_____	_____	

4. Stima della **probabilità** di accadimento delle minacce (fattore **P** della formula di calcolo del Rischio)	x Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
5. Stima dell'**impatto** (fattore **I** della formula di calcolo del Rischio)	x 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	X 1	☐ 2	☐ 3	☐ 4

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?	x Regolare manutenzione dell'hardware x Software aggiornato regolarmente x Adozione di una policy per il corretto utilizzo degli strumenti informatici ☐ Formazione del personale x Doppio controllo nell'inserire i dati nella eCFR			
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	x 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**	x accettabile (1-6)	☐ non accettabile (8-16)
	attuazione del trattamento	consultazione preventiva

4.3. Perdita di disponibilità *(a cura del P.I., Ricercatori, del Personale Tecnico e del Referente Privacy limitatamente al punto 3 della tabella sottostante).*

x La perdita di disponibilità dei dati non ha impatto sui diritti e le libertà degli interessati	**Se è stata spuntata questa casella, la tabella sotto riportata NON deve essere compilata**

Impossibilità di accesso, perdita, distruzione non autorizzata 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?	☐ 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 ☐ 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	
☐ Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
☐ altro_____	_____	
4. Stima della **probabilità** di accadimento delle	☐ Improbabile 1	

minacce (fattore **P** della formula di calcolo del Rischio)	☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
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*:_____] ☐ 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 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	1.

misure di sicurezza	2.	
14. **Rischio residuo**	☐ accettabile (1-6)	☐ non accettabile (8-16)
	 attuazione del trattamento	 consultazione preventiva

5. CONCLUSIONI *(a cura del Referente Privacy in base anche a quanto rilevato dal DPO).*

5.1 Valutazione finale.

Il Titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché delle diverse probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento. Dette misure saranno riesaminate e aggiornate qualora necessario.
Nelle precedenti sezioni di questa DPIA:

- è stato presentato definito il contesto e presentato il processo di trattamento dei dati personali;
- sono state descritte le caratteristiche del trattamento dei dati;
- sono state individuate e analizzati – in rapporto alle differenti minacce – i rischi per l'interessato conseguenti alla perdita di riservatezza, integrità e disponibilità dei dati e le misure di sicurezza in atto per la mitigazione di tali rischi;
- sono state identificate le vulnerabilità nell'adozione delle misure di sicurezza in atto e indicate contromisure alla mitigazione del rischio.

Nella Sezione successiva si andrà a riportare se permane un rischio residuo elevato e se risulti pertanto necessaria una consultazione preventiva con l'Autorità Garante per la protezione dei dati personali.

5.2 Rischio residuo.

Ai sensi del GDPR, se il rischio residuo a fronte dell'adozione delle contromisure rimane elevato, deve essere consultata l'Autorità Garante per la protezione dei dati personali.
Il Gruppo di Lavoro Articolo 29 (WP29) nelle Linee Guida sulla DPIA definisce come rischio residuo elevato inaccettabile quello che caratterizza i "*casi in cui le persone gli interessati possano subire conseguenze significative, o addirittura irreversibili, che non possono superare (ad es. accesso illegittimo a dati che comportano una minaccia per la vita degli interessati, un loro licenziamento, un rischio finanziario) e/o quando appare evidente che il rischio si verificherà (ad es. poiché non si è in grado di ridurre il numero di persone che accedono ai dati a causa delle loro modalità di condivisione, utilizzo o distribuzione o quando non si può porre rimedio a una vulnerabilità ben nota*)".

Il Titolare ha concluso che, considerate le misure di sicurezza in atto e pianificate e le contromisure che verranno attuate nei tempi indicati dalla presente DPIA, nel trattamento di dati oggetto della presente DPIA, non si rilevano condizioni di rischio residuo elevato e che pertanto non è necessario consultare l'Autorità garante ai sensi dell'art. 36 del GDPR.

Il Titolare del trattamento

_____

Allegato 1

Indicazioni per il calcolo del rischio

[Istruzioni per la compilazione delle Tabelle riportate al Paragrafo 4]

[NON COMPILARE questo allegato]

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). [13]

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*	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

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

accidentale)	☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
	☐ 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	
	☐ Perdita di riservatezza dei dati personali protetti da segreto professionale	Rivelazione del segreto professionale (art. 622 c.p.)	
	☐ Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
	☐ altro_____	_____	
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
	☐ 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	
	☐ Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
	☐ 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
	☐ 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	
	☐ Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
	☐ 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).

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	MOLTO PROBABILE	4

• 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		

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

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 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