DPIA REPORT
STUDIO CLINICO

AYA

INFORMAZIONI DOCUMENTO:

Titolo	**DPIA REPORT- STUDIO CLINICO**		
Codice	AYA		
Data di emissione	28.11.2024	**Versione**	1.0

STESURA

Funzione	Nome	Data	Firma
Study Coordinator	Dott.ssa Alice Donnini	09.12. 2024	

REVISIONE

Funzione	Nome	Data	Firma
DPO	Dott.ssa Maria Rita Sechi	13.12.2024	

APPROVAZIONE

Funzione	Nome	Data	Firma
Presidente	Ing. Carlo Tosti		TOSTI CARLO 2024.12.19 11:59:48 CN=TOSTI CARLO C=IT 2.5.4.4=TOSTI 2.5.4.42=CARLO

Storia dei Cambiamenti

Versione	Data	Descrizione cambiamento

SOMMARIO

GLOSSARIO

GDPR: Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679 o solo "Regolamento";

DATO PERSONALE: qualsiasi informazione riguardante una persona fisica identificata o identificabile "interessato"; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

TRATTAMENTO: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

VIOLAZIONE DEI DATI PERSONALI: o "data breach", è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

LIMITAZIONE DI TRATTAMENTO: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

PROFILAZIONE: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

ARCHIVIO: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

PSEUDONIMIZZAZIONE: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

TITOLARE DEL TRATTAMENTO: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

DPO: il Data Protection Officer (D.P.O) è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 GDPR dal titolare del trattamento o dal responsabile del trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;

RESPONSABILE ESTERNO DEL TRATTAMENTO (O RESPONSABILE): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

DESTINATARIO: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

TERZO: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

CONSENSO DELL'INTERESSATO: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

DATI COMUNI: sono tutti i dati personali che non appartengono alle categorie dei dati particolari e giudiziari;

DATI PARTICOLARI: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

DATI GENETICI: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

DATI RELATIVI ALLA SALUTE: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

AUTORITÀ DI CONTROLLO: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR;

TRATTAMENTO TRANSFRONTALIERO o TRASFERIMENTO EXTRA UNIONE EUROPEA: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure, b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

DISPOSITIVO MEDICO: qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più delle seguenti destinazioni d'uso mediche specifiche:

- diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie;
- diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità;
- studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o

patologico;

- fornire informazioni attraverso l'esame *in vitro* di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati;

e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere coadiuvata da tali mezzi.

STUDIO CLINICO (o *Clinical Trial o Trial*): qualsiasi indagine sistematica cui partecipano uno o più soggetti umani, volta a valutare la sicurezza o le prestazioni di un dispositivo medico ovvero gli effetti e la sicurezza di nuovi farmaci o di nuovi trattamenti terapeutici. Lo studio clinico può essere effettuato in un unico centro o in più centri (c.d. studio multicentrico), in Italia o anche in altri Stati membri dell'Unione europea o in Paesi terzi. Lo studio clinico può altresì essere:

- **controllato:** in questo caso i partecipanti allo studio sono suddivisi in due gruppi, uno soltanto dei quali riceve il trattamento oggetto della sperimentazione, mentre l'altro, detto "gruppo di controllo", riceve il trattamento standard o il placebo;
- **randomizzato:** quando prevede che i partecipanti alla ricerca siano assegnati in maniera del tutto casuale al gruppo che riceverà il trattamento da sperimentare o al gruppo di controllo;
- **in doppio cieco:** si verifica tale condizione quando né i partecipanti né i ricercatori sono a conoscenza di chi sia sottoposto al trattamento sperimentale e chi, invece, sia assegnato a quello standard o assuma il placebo.
- **in cieco semplice:** è uno studio in cui solo i soggetti inclusi non sono a conoscenza dei trattamenti assegnati, mentre lo sperimentatore ne è a conoscenza.
- **multicentrico o policentrico:** studio che coinvolge più centri di sperimentazione.
- **prospettico:** valuta gli effetti di un intervento seguendo le persone coinvolte a partire dall'inizio dello studio e fino alla sua conclusione, al fine di osservare gli esiti dell'intervento stesso.
- **osservazionale:** tende a dimostrare i possibili effetti di vari fattori di rischio o protettivi, su un gruppo di persone, osservando gli eventi che si verificano senza alcun intervento da parte dello sperimentatore.
- **retrospettivo:** è uno studio che misura e analizza dati ed eventi accaduti in un periodo precedente rispetto al progetto dello studio.

DATI CLINICI: informazioni sulla sicurezza o sulle prestazioni ricavate dall'impiego di un dispositivo e che provengono:

- dalle indagini cliniche relative al dispositivo in questione;
- dalle indagini cliniche o da altri studi pubblicati nella letteratura scientifica relativi a un dispositivo di cui è dimostrabile l'equivalenza al dispositivo in questione;

- da relazioni pubblicate nella letteratura scientifica sottoposta a valutazione *inter pares* su altre esperienze cliniche relative al dispositivo in questione o a un dispositivo di cui è dimostrabile l'equivalenza al dispositivo in questione;
- da informazioni clinicamente rilevanti risultanti dalla sorveglianza post – commercializzazione, in particolare il *follow-up* clinico post-commercializzazione.

PROMOTORE DELLO STUDIO CLINICO O SPONSOR: qualsiasi persona, società, istituzione oppure organizzazione che si assume la responsabilità di avviare, gestire e curare il finanziamento dello studio o indagine clinica;

SPERIMENTATORE: una persona - medico o un odontoiatra qualificato ai fini delle sperimentazioni - responsabile dell'esecuzione della conduzione dello studio clinico presso il centro di sperimentazione. Se l'indagine clinica è svolta da un gruppo di persone nello stesso centro, è il responsabile del team di studio;

PROTOCOLLO: il documento in cui vengono descritti l'obiettivo o gli obiettivi, la progettazione, la metodologia, gli aspetti statistici e l'organizzazione della sperimentazione. Il termine protocollo comprende il protocollo, le versioni successive e le modifiche dello stesso;

SOGGETTO O PAZIENTE: la persona che partecipa a uno studio clinico;

COMITATO ETICO: un organismo indipendente, composto da personale sanitario e non, con poteri consultivi, che ha la responsabilità di garantire la tutela dei diritti, della sicurezza e del benessere dei soggetti che partecipano a uno studio clinico e di fornire pubblica garanzia di tale tutela, esprimendo, ad esempio, un parere sul protocollo di sperimentazione, sull'idoneità degli sperimentatori, sulla adeguatezza delle strutture e sui metodi e documenti che verranno impiegati per informare i soggetti e per ottenere il consenso informato;

CRO (Contract Research Organization): si tratta di una persona o un'organizzazione (commerciale, accademica o di altro tipo) con cui lo sponsor ha stipulato un contratto per assolvere ad una o più mansioni e funzioni relative allo studio;

CONSENSO INFORMATO o "IC": l'espressione libera e volontaria di un soggetto della propria disponibilità a partecipare a un determinato studio clinico, dopo essere stato informato di tutti gli aspetti dello studio clinico rilevanti per la sua decisione di partecipare oppure, nel caso di minori o di soggetti incapaci, l'autorizzazione o l'accordo dei rispettivi rappresentanti legalmente designati a

includerli nello studio clinico. Il consenso prestato è documentato mediante un modulo di consenso informato scritto (ICF), firmato e datato;

CODICE DI IDENTIFICAZIONE DEL SOGGETTO: un codice unico assegnato dallo sperimentatore a ciascun soggetto dello studio per tutelare l'identità dello stesso e utilizzato al posto del nome del soggetto quando lo sperimentatore segnala eventi avversi e/o altri dati collegati allo studio;

MONITORAGGIO: la supervisione dell'andamento di uno studio clinico per garantire che questo venga effettuato, registrato e relazionato in osservanza del protocollo, delle disposizioni normative applicabili e della GCP;

RAPPORTO DI MONITORAGGIO: un rapporto scritto inviato dal responsabile del monitoraggio allo sponsor al termine di ciascuna visita al centro di studio e/o ogni altra comunicazione collegata allo studio;

MONITOR/CRA (Clinical Research Associate): persona incaricata di valutare le prestazioni e il progresso dello studio al fine di garantire che siano condotte, registrate e segnalate in conformità al protocollo, al GCP e ai requisiti normativi applicabili. Può essere uno sponsor o un dipendente della CRO ed è il principale contatto con il sito clinico;

EVENTO AVVERSO: qualsiasi evento clinico dannoso, malattia o lesione involontaria o segno clinico sfavorevole, compreso un risultato di laboratorio anomalo, che si verifica in soggetti, utilizzatori o altre persone, nell'ambito di uno studio clinico, indipendentemente dal fatto che l'evento sia o meno collegato al dispositivo oggetto di indagine;

EVENTO AVVERSO GRAVE: qualsiasi evento avverso che ha avuto una delle seguenti conseguenze:

- un decesso;
- un grave peggioramento delle condizioni di salute del soggetto che ha comportato:

i) una malattia o una lesione potenzialmente letale;
ii) un danneggiamento permanente di una struttura o di una funzione corporea;
iii) la necessità di un ricovero ospedaliero del paziente o il suo prolungamento;
iv) un intervento medico o chirurgico inteso a prevenire una malattia o una lesione potenzialmente letale o un danneggiamento permanente di una struttura o di una funzione corporea;
v) una patologia cronica.

- sofferenza fetale, morte fetale o una malformazione o disabilità fisica o intellettiva congenita;

INCIDENTE: qualsiasi malfunzionamento o alterazione delle caratteristiche o delle prestazioni di un dispositivo messo a disposizione sul mercato, compreso l'errore d'uso determinato dalle caratteristiche ergonomiche, come pure qualsiasi inadeguatezza nelle informazioni fornite dal fabbricante e qualsiasi effetto collaterale indesiderato;

INCIDENTE GRAVE: qualsiasi incidente che, direttamente o indirettamente, ha causato, può aver causato o può causare una delle seguenti conseguenze:

a) il decesso di un paziente, di un utilizzatore o di un'altra persona;
b) il grave deterioramento, temporaneo o permanente, delle condizioni di salute del paziente, dell'utilizzatore o di un'altra persona;
c) una grave minaccia per la salute pubblica;

SCHEDA RACCOLTA DATI (CRF): un documento su supporto cartaceo, ottico, oppure elettronico progettato per registrare tutte le informazioni richieste dal protocollo, che devono essere riferite allo sponsor relativamente a ciascun partecipante allo studio;

DOCUMENTAZIONE: tutti i documenti, in qualsiasi forma (compresi, tra gli altri, registrazioni scritte, elettroniche, magnetiche e ottiche, scansioni, radiografie ed elettrocardiogrammi), che descrivono o registrano metodi, conduzione, e/o risultati di uno studio, fattori che incidono su di uno studio e le azioni intraprese;

DOCUMENTI ESSENZIALI: documenti che, singolarmente o nel loro insieme, consentono di valutare la conduzione di uno studio e la qualità dei dati prodotti. Questi documenti servono a dimostrare la conformità dello sperimentatore, dello sponsor e del monitor agli standard di Good Clinical Practice e a tutte le disposizioni normative applicabili. L'archiviazione dei documenti essenziali è opportunamente effettuata presso lo sperimentatore/istituzione e presso lo sponsor;

DATI ORIGINALI: tutte le informazioni contenute nelle registrazioni originali e nelle copie certificate delle registrazioni originali di referti clinici, osservazioni, o altre attività in uno studio clinico necessarie per la ricostruzione e la valutazione dello studio stesso. I dati originali sono contenuti nei documenti originali (registrazioni originali o copie certificate);

DOCUMENTI ORIGINALI: documenti, dati e registrazioni originali (ad esempio, cartelle ospedaliere, registri clinici ed amministrativi, note di laboratorio, memoranda, diari dei soggetti o schede di valutazione, registrazioni della distribuzione del farmaco, dati registrati mediante strumentazione automatizzata, copie o trascrizioni certificate dopo verifica della loro aderenza all'originale,

microfiches, negativi di fotografie, microfilm o supporti magnetici, radiografie, fascicoli dei soggetti e registrazioni conservate nella farmacia, nei laboratori e nei dipartimenti medico-tecnici coinvolti nello studio clinico);

ACCESSO: autorizzazione ad esaminare, analizzare, verificare e riprodurre qualsiasi registrazione e relazione rilevanti per la valutazione di uno studio clinico. Coloro che hanno accesso diretto a tale documentazione (per esempio autorità regolatorie nazionali ed estere, responsabili del monitoraggio e della verifica) devono adottare ogni adeguata precauzione per mantenere riservata l'identità dei soggetti e le informazioni di proprietà dello sponsor, nel rispetto delle disposizioni normative applicabili;

ISPEZIONE: l'effettuazione, da parte di una o più autorità regolatorie, di una revisione ufficiale di documenti, strutture, registrazioni e ogni altra risorsa considerata dall'autorità stessa collegata allo studio clinico; la revisione potrà aver luogo nel centro della sperimentazione, presso le strutture dello sponsor e/o della CRO, oppure in qualsiasi altra sede giudicata appropriata dalle autorità regolatorie;

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA): è una metodologia per valutare l'impatto sui diritti e le libertà delle persone fisiche di un progetto, servizio, applicazione, programma, prodotto o qualsiasi altra iniziativa che implichi il trattamento di dati personali che presenta alti rischi per i suddetti diritti e libertà delle persone fisiche e, dopo aver consultato tutti i terzi coinvolti nel trattamento dei dati e il DPO, prendere le misure necessarie per evitare o minimizzare l'impatto negativo. Si tratta di un processo continuo che deve iniziare nella fase più preliminare possibile del progetto, servizio, applicazione, programma, prodotto o iniziativa, quando, sia ancora possibile influenzarne il risultato, in modo tale da garantire la privacy by design;

RISCHIO: si riferisce al rischio derivante dal trattamento di dati personali; il rischio può essere tanto patologico **(RISCHIO PATOLOGICO)**, quale rischio di violazione dei dati che deriva da una determinata fonte o patologia (per es. l'accidentale o illecita distruzione, perdita, modifica, divulgazione di dati personali, l'accesso non autorizzato ai dati personali, ecc.); quanto fisiologico **(RISCHIO IMPLICITO O FISIOLOGICO)**, ossia insito nel trattamento stesso;

RICHIESTE DELL'INTERESSATO: si classificano come segue:

- "**Istanze di revoca del consenso**" ex art. 7 GDPR. In ogni momento l'interessato può revocare il consenso precedentemente espresso in relazione a uno o più trattamenti, senza necessità di fornire motivazioni. In tali casi i campioni biologici a lui correlati dovranno essere distrutti e non saranno

raccolti ulteriori dati che lo riguardano, pur restando possibile l'utilizzazione di quelli eventualmente già raccolti per determinare, senza alterarli, i risultati della ricerca;

- "**Richieste di accesso**" ex art. 15 GDPR. Con l'esercizio del diritto di accesso ex art. 15 GDPR, l'interessato ha il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguarda e di avere accesso ai propri dati personali e relativa copia;

- "**Richieste di rettifica**" ex art. 16 GDPR. L'interessato ha diritto di ottenere la correzione/rettifica/integrazione di dati inesatti che lo riguardano; nel caso in cui il paziente di uno studio clinico intenda esercitare il diritto di rettifica ex art 16 GDPR, le modifiche richieste devono essere annotate e registrate, a cura dello Sponsor, a margine dei dati originari della ricerca senza modificare questi ultimi, in quanto la modifica dei dati originari può avere effetti significativi sui risultati dello Studio;

- "**Richieste di cancellazione**" ex art. 17 GDPR (Diritto all'oblio). L'interessato ha il diritto di richiedere e ottenere la cancellazione dei dati personali o la loro trasformazione in forma anonima. Se il paziente di uno studio intende esercitare il diritto di cancellazione ex art 17 GDPR, le modifiche richieste devono essere annotate e registrate, a cura dello Sponsor, a margine dei dati originari della ricerca senza modificare questi ultimi, in quanto la modifica dei dati originari può avere effetti significativi sui risultati dello Studio;

- "**Richieste di limitazione di trattamento**" ex art. 18 GDPR. L'interessato ha diritto di far interrompere qualsiasi forma di utilizzo dei propri dati personali, ad eccezione della loro conservazione;
- "**Richieste di portabilità dei dati**" ex art. 20 GDPR. L'interessato ha il diritto di ricevere in formato strutturato, di uso comune e leggibile da dispositivi informatici i dati personali che lo riguardano forniti al Titolare;

- "**Richieste di opposizione al trattamento**" ex art. 21 GDPR. L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano per motivi connessi alla sua situazione particolare, qualora i dati siano trattati ai fini di ricerca scientifica o storica o ai fini statistici; in tali casi, i campioni biologici a lui correlati dovranno essere distrutti e non saranno raccolti ulteriori dati che lo riguardano, ferma restando l'utilizzazione di quelli eventualmente già raccolti per determinare, senza alterarli, i risultati della ricerca;

- "**Istanze di opposizione alla profilazione (processi decisionali automatizzati)**" ex art. 22 GDPR. L'interessato può chiedere di non essere sottoposto a decisioni aziendali basate unicamente

su trattamenti automatizzati, compresa la profilazione dei dati, quando tali decisioni producano effetti giuridici sull'interessato o comunque incidano in modo significativo sulla sua persona.

DOCUMENTI DI RIFERIMENTO

- Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679 o solo "Regolamento";
- D.Lgs. 30 giugno 2003, n. 196 ("Codice Privacy");
- Regolamento (UE) 2017/745 del Parlamento Europeo e del Consiglio del 5 aprile 2017 relativo ai dispositivi medici;
- D.lgs. 24 giugno 2003 n. 211 ("Decreto") in attuazione della direttiva 2001/20/CE sull'applicazione della buona pratica clinica nell'esecuzione delle sperimentazioni cliniche di medicinali per uso clinico;
- *"Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali"* adottate dal Garante per la Protezione dei Dati Personali con Deliberazione n. 52 del 24 luglio 2008;
- *"Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101"* adottate dal Garante per la Protezione dei Dati Personali con il provvedimento n. 515 del 19 dicembre 2018;
- *"Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101"* adottate dal Garante per la Protezione dei Dati Personali con il provvedimento n. 146 del 5 giugno 2019;
- *"Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice"* (provv. del Garante per la Protezione dei Dati Personali n. 298 del 9 maggio 2024);
- *"Parere 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati"*, adottato dall'EDPB il 23 gennaio 2019;
- Good Clinical Practice (GCP), recepite in Italia con il D.M. 15 luglio 1997;
- D.M. 8 febbraio 2013 ("DM CE/13") - Criteri per la composizione ed il funzionamento dei Comitati etici;
- *"Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato"* ai sensi del regolamento 2016/679" adottate il 4 aprile 2017 dal Gruppo di Lavoro ex art. 29 (WP29);
- Procedura di valutazione di impatto sulla protezione dei dati personali Regolamento (UE) 2016/679;

- Procedura sull'esercizio dei diritti dell'interessato ai sensi del Regolamento (UE) 2016/679;
- ISO/IEC 29134:2020 *"Information technology – Security techniques – Guidelines for privacy impact assessment"*.

1 LO STUDIO CLINICO E LE SUE PRINCIPALI CARATTERISTICHE

La **FONDAZIONE POLICLINICO UNIVERSITARIO CAMPUS BIO – MEDICO** (di seguito, anche solo la "**Fondazione**") è un ente che persegue finalità di tutela e promozione della persona umana nell'ambito dell'assistenza sanitaria, della formazione, della ricerca scientifica e dell'innovazione in campo biomedico e sanitario.
In qualità di soggetto promotore (o sponsor) nell'ambito degli studi clinici, la Fondazione ha predisposto un protocollo relativo a uno studio clinico sulla valutazione retrospettiva dell'impatto di diversi approcci terapeutici in un gruppo di pazienti adolescenti/giovani adulti, con diagnosi di Linfoma di Hodgkin.
I dati afferenti allo studio clinico saranno raccolti in qualità di documenti ufficiali nell'apposito *Case Report Form* (CRF), e sarà predisposto un singolo CRF per ogni paziente partecipante allo studio.

Descritte sinteticamente le principali caratteristiche dello studio clinico, prima di procedere all'analisi, anche sotto il profilo giuridico, dei flussi di informazioni e dei trattamenti di dati personali, è opportuno svolgere alcune considerazioni preliminari di carattere generale in merito agli studi clinici, mettendo in luce gli aspetti maggiormente rilevanti rispetto all'applicazione della normativa in materia di protezione dei dati personali.
In linea generale, gli studi clinici sono promossi da una società, istituzione od organizzazione (committente o sponsor o, anche, promotore), che, dopo aver predisposto un protocollo che descrive la progettazione, gli obiettivi e la metodologia dello studio clinico, cura la presentazione della documentazione necessaria all'attivazione della sperimentazione alle autorità competenti (Ministero della Salute nel caso dei dispositivi medici e AIFA nel caso di farmaci) e ai comitati etici interessati. Al comitato è demandata l'approvazione dei protocolli sperimentali e dei documenti connessi (cd. SOP "Procedure Operative Standard"), i quali sono predisposti dallo sponsor conformemente ai princìpi etici (che traggono origine dalla Dichiarazione di Helsinki del giugno 1964) ed ai requisiti previsti dalle Linee Guida per la Buona Pratica Clinica - "GCP"[1] (adottati anche dall'Unione Europea e recepiti nell'ordinamento italiano con il D.lgs. 6 novembre 2007, n. 200; D.lgs. 24 giugno 2003, n. 211; D.M. 15 luglio 1997 e, da ultimo, D.M. 21 dicembre 2007).
Le attività collegate allo studio clinico vengono eseguite presso una o più strutture ospedaliere o universitarie o istituti di ricerca pubblici o privati autorizzati in base alla legge e individuati

[1] le **Linee Guida Per La Buona Pratica Clinica Cpmp/Ich/ 135/95 - GCP (DM 15 luglio 1997)**, ossia lo standard internazionale di etica e qualità scientifica per progettare, condurre, registrare e relazionare gli studi clinici che coinvolgano soggetti umani.

appositamente dallo sponsor (c.d. “centri di sperimentazione”). Le attività sono condotte da un team di studio composto da medici sperimentatori, infermieri, ecc., guidato dal *principal investigator* (sperimentatore principale). Quest’ultimo è responsabile di tutte le decisioni mediche di competenza del centro di sperimentazione e della conformità dello studio al protocollo GCP e alle SOP.

Nel corso dello studio clinico vengono raccolti, in conformità al protocollo, varie informazioni di carattere medico/clinico e campioni biologici delle persone che accettano di far parte dello studio tramite visite mediche e accertamenti diagnostici effettuati da medici sperimentatori.

Alle predette informazioni non ha accesso soltanto il personale sanitario operante presso i centri di sperimentazione. Il promotore supervisiona, infatti, l’andamento dello studio, per garantire che esso venga effettuato in osservanza del protocollo. Ciò, avvalendosi di propri collaboratori (c.d. *Clinical Study Monitor*) i quali, nell’ambito delle loro attività di monitoraggio, visitano i centri di sperimentazione e, se necessario, esaminano la documentazione medica originale degli individui partecipanti allo studio messa a loro disposizione dai medici (es. cartelle ospedaliere, referti, note di laboratorio ecc.).

I pazienti che vogliono iscriversi ad uno studio clinico devono volontariamente confermare la loro disponibilità a partecipare, solo dopo essere stati debitamente informati dal principal investigator. Quest’ultimo, infatti, assicura che ogni paziente riceva e comprenda a pieno le informazioni pertinenti relative allo studio clinico al fine di prestare liberamente il consenso, mettendolo al corrente dei rischi e dei benefici della sua partecipazione, e illustrando, in ogni suo punto, il modulo di consenso informato ICF (cfr. all.1). La documentazione relativa agli studi clinici comprende anche una sezione relativa al trattamento dei dati personali. Rispetto agli obblighi informativi in materia di protezione dei dati personali e all’eventuale esonero dalla raccolta del consenso del paziente/interessato al trattamento dei propri dati personali trovano applicazione anche le disposizioni di cui all’art. 110 del Codice Privacy (v. *infra*).

Il modulo di ICF deve essere datato e firmato dal paziente e dal principal investigator (o un altro medico sperimentatore appositamente delegato).

Nel corso dello studio, i medici sperimentatori che prestano servizio presso i centri di sperimentazione raccolgono, tramite visite mediche e accertamenti diagnostici, varie informazioni di carattere medico-clinico, compresi i campioni biologici dei pazienti che partecipano allo studio. A tali informazioni hanno accesso solo i medici sperimentatori e i “monitor” dello sponsor, i quali controllano l’andamento dello studio per garantirne la conformità al protocollo avvalendosi di propri collaboratori (interni o esterni) che visitano i centri di sperimentazione accedendo alla documentazione clinica originale dei pazienti se necessario ai fini della verifica.

Conclusa la fase della sperimentazione presso il centro, le medesime informazioni sono normalmente inserite dal promotore, direttamente o tramite soggetti esterni di cui si avvale, su un *data-base* unico attraverso il quale vengono effettuati il controllo e la validazione dei dati e,

successivamente, l'elaborazione statistica, con l'obiettivo di conseguire i risultati dello studio da documentare poi in un rapporto.

2 LA VALUTAZIONE D'IMPATTO SUI DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE "DPIA"

La *Data Protection Impact Assessment* "DPIA" è un processo introdotto dall'art. 35 del nuovo Regolamento Generale sulla Protezione dei Dati, Reg. (UE) 2016/679, volto a descrivere il trattamento, valutare la necessità e la proporzionalità dello stesso, per gestire i rischi per i diritti e le libertà delle persone fisiche che ne derivano e, attraverso la loro analisi, determinare le misure per farvi fronte. La DPIA è un importante strumento di *accountability* per la gestione dei rischi, in *primis* quelli relativi al diritto alla privacy, ma può riguardare anche altri diritti fondamentali delle persone fisiche, quali la libertà di espressione e di pensiero, la libertà di movimento, il diritto alla libertà di coscienza e di religione, ecc.

La DPIA aiuta i titolari, non solo a soddisfare i requisiti del GDPR, ma anche a documentare e dimostrare che sono state adottate misure adeguate per garantirne il rispetto. Coerentemente con l'approccio basato sulla prevenzione del rischio, che caratterizza nella sua interezza il GDPR, lo svolgimento di una DPIA non è obbligatorio per ogni singolo trattamento, ma è necessario solo se il trattamento ***"può comportare un rischio elevato per i diritti e le libertà delle persone fisiche"***, come previsto dall'art. 35.1 GDPR. L'obbligo di condurre una DPIA, in determinate circostanze, deve essere collocato nel contesto del più generale obbligo imposto ai titolari di gestire correttamente i rischi connessi al trattamento di dati personali, in un'ottica di responsabilizzazione a cui titolare è soggetto; sul punto, difatti, il WP29 raccomanda ai titolari del trattamento di farvi comunque ricorso in quanto la DPIA contribuisce all'osservanza delle norme in materia di protezione dati. Una DPIA può riguardare un singolo trattamento o un insieme di trattamenti simili che presentano rischi elevati analoghi o un oggetto più ampio di un unico progetto, ex c. 92. GDPR. Il processo si articola nelle seguenti fasi:

1) Valutazione della necessità di procedere alla DPIA:

La prima fase riguarda l'esame della necessità di condurre o meno la valutazione d'impatto; a tale scopo il GDPR contempla tre ipotesi di trattamento in cui la DPIA è obbligatoria, meglio specificate e integrate dal WP29 nelle *"Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679*".

2) Descrizione del progetto e del flusso di informazioni:

Una volta stabilito se procedere alla DPIA rappresenta una scelta obbligatoria o facoltativa, si procede alla descrizione dettagliata dei trattamenti di dati personali che il progetto implica dando evidenza a tutti gli aspetti del trattamento rilevanti per i diritti fondamentali delle persone (interessati e terzi) che siano suscettibili di generare un rischio più elevato indicando altresì:

- le modalità (cartacee o automatizzate) e gli strumenti per mezzo dei quali sono trattati i dati personali (hardware, software, reti, persone, mezzi cartacei o di trasmissione cartacei);
- le misure di sicurezza tecniche e organizzative poste a protezione dei dati e delle nuove tecnologie utilizzate per elaborarli, per scongiurare violazioni dei dati;
- la categoria di dati personali trattati, le finalità e le basi di legittimità e le categorie di interessati,
- la valutazione sulla necessità e sulla proporzionalità dei trattamenti in relazione alle finalità;
- le categorie ed i soggetti che accederanno ai dati, le ragioni e le finalità per le quali vi accederanno, nonché i controlli relativi all'accesso;
- il flusso delle informazioni, raccolta (origine dei dati), circolazione all'interno dell'azienda e comunicazione all'esterno, l'eventuale trasferimento extra UE;
- gli aspetti relativi alla conservazione dei dati.

3) Analisi della conformità normativa:

Una volta operata la ricognizione dei trattamenti e di tutti gli aspetti più rilevanti, si passa alla verifica della loro conformità normativa, ossia alla rispondenza ai principi generali di necessità, proporzionalità e trasparenza dei trattamenti in relazione alle finalità, da effettuarsi tramite compilazione del questionario allegato al presente report, che include una serie di domande (cd. *screening questions*) cui è necessario rispondere per iscritto per comprovare se i trattamenti dei dati personali analizzati rispettino i suddetti principi del GDPR e comprenda, come chiarito dai Garanti Europei, misure che:

- contribuiscano alla proporzionalità e necessità del trattamento sulla base di:
  - finalità specifiche, esplicite e legittime ex art. 5.1.b;
  - liceità del trattamento ex art. 6;
  - adeguatezza, pertinenza e limitazione dei dati a quanto necessario ex art. 5.1.c;
  - limitazione della durata di conservazione ex art. 5.1;
- contribuiscano ai diritti delle persone interessate:
  - informazioni fornite alla persona interessata ex artt. 12,13 e 14;
  - diritto di accesso e alla portabilità ex artt. 15 e 20;
  - diritto di revocare il consenso, rettificare, cancellare, opporsi, limitazione del trattamento ex artt. 16, 17, 18, 19 e 21;
  - destinatari dei dati;
  - responsabili del trattamento ex art. 28;
  - garanzie sul trasferimento artt. 45 e ss.;

4) Consultazioni:

Il processo di valutazione d'impatto segue una fase di consultazione con le parti interessate, al fine di garantire la trasparenza sullo svolgimento di tale attività. Le opinioni degli interessati possono essere ricercate attraverso un'ampia varietà di mezzi, a seconda del contesto, (es. conducendo uno

studio interno o esterno legato alla finalità e alla modalità del trattamento, operando interrogazioni formali ai rappresentanti sindacali dei lavoratori, o alle associazioni di categoria o ai sindacati o facendo con loro delle riunioni, o attraverso dei sondaggi o questionari inviati ai futuri clienti/pazienti ecc..). La consultazione delle opinioni degli interessati è fondamentale per individuare i rischi potenziali del trattamento.

Qualora la decisione finale del titolare del trattamento si discosti dalle opinioni degli interessati, le sue motivazioni devono essere documentate.

Il titolare del trattamento deve altresì documentare la sua giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che tale operazione non sia appropriata, ad esempio nei casi in cui possa compromettere la riservatezza dei piani economici dell'impresa o sarebbe sproporzionata o impraticabile.

5) Parere del DPO[2]

Il D.P.O. della Fondazione, nell'esercizio delle proprie funzioni attribuitegli dall'art. 35 del Regolamento, ha esaminato le attività di trattamento oggetto della presente valutazione d'impatto nonché l'esito delle analisi condotte dal Titolare del trattamento.

Il D.P.O., preliminarmente, ritiene di condividere le conclusioni cui è pervenuta la Fondazione Promotore dello Studio circa l'obbligatorietà di condurre una valutazione d'impatto per la protezione dei dati rispetto al trattamento effettuato nell'ambito dell'attività di ricerca qui esaminato, tenuto conto del numero di interessati coinvolti e delle tipologie di trattamento che si possono utilizzare per pazienti con diagnosi di Linfoma di Hodgkin.

La metodologia seguita dalla Fondazione nel condurre la valutazione d'impatto appare conforme alle disposizioni contenute nel Regolamento e negli specifici provvedimenti adottati in materia dai Garanti Europei. La valutazione comprende altresì una serie di domande puntuali (c.d. *screening questions*) volte a verificare che i trattamenti svolti nel caso di specie rispettino i principi sanciti dalla normativa in materia di protezione dei dati personali e che siano state adottate dal titolare del trattamento le necessarie misure di sicurezza tecniche e organizzative.

La Fondazione ha inoltre fornito una descrizione sufficientemente dettagliata e completa delle operazioni di trattamento e del flusso di informazioni che lo Studio "AYA" implica, evidenziando nel contempo tutti gli aspetti rilevanti del trattamento che possono essere suscettibili di generare un rischio più elevato per i diritti e le libertà delle persone fisiche (interessati e terzi).

La fase di analisi della conformità normativa del trattamento è stata effettuata tenendo conto della rispondenza del trattamento alla normativa vigente in materia di protezione dei dati personali - in particolare ai principi generali espressi dall'art. 5 del Regolamento – ed ai provvedimenti prescrittivi emessi dall'Autorità di Controllo competente (Garante per la Protezione dei Dati Personali). Il Promotore dello Studio ha altresì dimostrato di aver predisposto un sistema idoneo a permettere agli interessati di esercitare facilmente i diritti previsti dagli artt. da 15 a 22 del Regolamento.

Le conclusioni cui è giunta la Fondazione all'esito della propria disamina sono condivisibili in quanto, oltre ad apparire coerenti sotto il profilo logico – giuridico, illustrano in modo sufficientemente dettagliato ed esente da critiche le motivazioni poste alla base del giudizio di conformità delle attività di trattamento rispetto alle disposizioni normative sulla protezione dei dati personali.

All'interno della valutazione d'impatto la Fondazione ha inoltre dato conto in maniera esaustiva dei ruoli dei soggetti coinvolti nelle operazioni di trattamento e delle responsabilità gravanti su ciascuno.

La Fondazione ha, infine, analizzato e individuato gli specifici rischi – patologici e fisiologici – per i diritti e le libertà degli interessati e di terzi che il trattamento in oggetto potrebbe comportare nonché le conseguenti misure di sicurezza adottate, che sono risultate adeguate a garantire la tutela dei diritti e delle libertà degli interessati.

Per quanto concerne l'analisi dei rischi derivanti dal trattamento in oggetto, la valutazione ha evidenziato un livello di rischio attuale e futuro di livello Basso, escludendo pertanto la necessità di procedere alla consultazione preventiva all'Autorità di Controllo ex art. 36 del Regolamento. Inoltre, lo Studio non ha evidenziato specificità né tecnologiche né sostanziali così che si è potuto ricorrere al modello di DPIA predisposto per la tipologia di Studio cui l'AYA rientra. Alla luce delle considerazioni sopra riportate, il D.P.O. ritiene che la valutazione d'impatto condotta dalla Fondazione in relazione allo Studio AYA sopra descritto sia completa di tutti gli elementi indispensabili previsti dall'art. 35, par. 7 del Regolamento e, pertanto, ne ratifica il contenuto e le conclusioni.

6) Identificazione, analisi e gestione dei rischi:

A questo punto, attraverso l'analisi della documentazione generata, si procede alla individuazione e la valutazione scritta dei rischi potenziali per i diritti e le libertà degli interessati e dei terzi derivanti dal trattamento/i in oggetto: in una prima fase si cercano i possibili rischi "patologici" incombenti sui dati personali oggetto di trattamento, ovverosia i gradi di severità e di probabilità che si verifichino "violazioni dei dati" come definite all'art. 4 GDPR ("la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"); mentre, in una seconda fase, si valutano i rischi per i diritti e le libertà delle persone fisiche causati:

2.a) dal trattamento in sé, implicitamente anche in assenza di violazioni dei dati (situazione fisiologica);

2.b) dalla violazione dei dati (situazione patologica).

Solo a valle della duplice valutazione operata nella seconda fase, comprendente non solo la casistica patologica di data breach ma anche e soprattutto, per la ratio dell'art. 35 GDPR, la carica intrinseca di potenziale impatto negativo sui diritti e le libertà delle persone di un trattamento in sé, sarà possibile andare a individuare misure di mitigazione più o meno mirate ed efficaci da adottare.Se sulla base della valutazione d'impatto il titolare del trattamento riesce a porre rimedio in modo soddisfacente ai rischi emersi, la procedura può dirsi conclusa; diversamente, se la situazione di

[2] Il Titolare del trattamento deve consultarsi con il Data Protection Officer (DPO) - qualora ne sia designato uno ai sensi dell'art. 35, paragrafo 2, GDPR - e il parere ricevuto, così come le decisioni prese dal titolare del trattamento, devono essere documentate all'interno della valutazione d'impatto sulla protezione dei dati. Il DPO deve altresì vigilare sullo svolgimento della valutazione d'impatto come previsto dall'art. 39, par. 1, lett. c), GDPR.
Ulteriori indicazioni e orientamenti in merito sono forniti nelle "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243.

rischio non è stata mitigata ed il trattamento rivela, pertanto, un rischio ancora elevato per i diritti e le libertà fondamentali dei soggetti interessati, sarà necessario rivolgersi all'autorità di controllo per avviare la c.d. consultazione preventiva ex art. 36 GDPR.

Alla luce di tali premesse, la Fondazione ha ritenuto opportuno condurre una valutazione d'impatto sui diritti e sulle libertà fondamentali delle persone fisiche rispetto ai trattamenti di dati personali effettuati nell'ambito della sperimentazione clinica in esame; il seguente report è stato redatto a conclusione del procedimento, allo scopo di documentare il processo valutativo e informare i soggetti coinvolti, interessati o terzi, dei risultati raggiunti, nonché l'autorità di controllo.

Di seguito si procederà ad esporre l'attività svolta dalla Fondazione attraverso la disamina di ciascuna fase del processo intercorso.

3 FASE 1: ANALISI DELLA NECESSITÀ DI PROCEDERE AD UNA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

La Fondazione, quale soggetto promotore dello studio clinico oggetto della presente valutazione d'impatto e titolare del trattamento, in via preliminare, ha esaminato la necessità di condurre o meno la valutazione d'impatto, valutando in concreto se i trattamenti di dati effettuati nell'ambito degli studi clinici presentano o meno un rischio elevato per i diritti e le libertà delle persone fisiche sulla base dei criteri che seguono al par. 3.1; all'uopo si rammenta che il Regolamento, ai sensi dell'art. 35, non impone di condurre una DPIA con riguardo a ogni trattamento che possa comportare rischi peri diritti e le libertà delle persone fisiche, ma che la DPIA è obbligatoria solo qualora un trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" ex art. 35.1 e che,a prescindere dalla sua necessità o meno, è raccomandabile ricorrervi comunque, in quanto rappresenta per il titolare un utile strumento di accountability.

La Fondazione ha compilato il questionario (allegato A) al presente report, contenente alcune *screening questions* che l'hanno guidata nel processo valutativo in oggetto; si rammenta sul punto che i Garanti Europei riconducono l'obbligo di DPIA in caso di concorrenza nell'ambito dei trattamenti oggetto di *assessment* di almeno due criteri di valutazione tra quelli sottoindicati al par. 3.1; tale principio tuttavia, non rappresenta una regola, per cui, in alcuni casi, il trattamento che presenti solo uno di questi criteri potrebbe, comunque, richiedere una DPIA. È necessario, in tali ipotesi, operare un'accurata valutazione in tal senso e, nei casi dubbi, in via cautelativa, procedere comunque alla DPIA.

3.1 CRITERI DI VALUTAZIONE DELLA NECESSITA' EFFETTUARE UNA DPIA

Il Regolamento, all'art. 35, individua alcuni trattamenti che presentano alti rischi intrinsechi, tali per cui la valutazione d'impatto è obbligatoria in presenza di:

a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato;

b) trattamento su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati;

c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Tale elencazione non è esaustiva, pertanto, i Garanti Europei, hanno fornito i seguenti criteri correlati da esempi concreti, per individuare tipologie altamente rischiose di trattamento, che vanno a meglio specificare le indicazioni più generali di cui all'art. 35 e ai considerando nn. 71, 75 e 91 del GDPR, quali:

1) Valutazione o assegnazione di un punteggio, incluse profilazione e predizione: in particolare, riguardanti gli aspetti concernenti le prestazioni della persona interessata al lavoro, la situazione economica, la salute, le preferenze o interessi personali, l'affidabilità o il comportamento, laposizione o gli spostamenti (considerando nn. 71 e 91[3]);

2) Decisioni automatiche con effetti giuridici o similmente significativi: elaborazione che mira a prendere decisioni su soggetti interessati e che produce effetti giuridici riguardanti la persona fisica o che allo stesso modo sia determinante per la persona fisica ex art. 35.3.a GDPR. Ad esempio, il trattamento può comportare l'esclusione o la discriminazione di singoli. Un'elaborazione con scarso o nessun effetto sugli individui non corrisponde a questo criterio specifico, pertanto, non rileva ai fini dei criteri che impongono l'obbligo di DPIA.

3) Controllo sistematico: trattamento utilizzato per osservare, monitorare o controllare soggetti interessati, inclusi i dati raccolti attraverso un controllo sistematico di una zona accessibile al pubblico ex art. 35.3.c. GDPR. Questo tipo di monitoraggio è considerato rischioso perché i dati personali possono essere raccolti in circostanze in cui gli interessati potrebbero non essere a conoscenza di chi sta raccogliendo i loro dati e di come saranno utilizzati. Inoltre, potrebbe essere impossibile per le persone evitare di essere oggetto di tale trattamento in spazi pubblici abituali (o accessibili al pubblico).

4) Dati sensibili: include le categorie particolari di dati ai sensi dell'art. 9 GDPR, nonché i dati personali relativi alle condanne penali o ai reati ex art. 10 GDPR. Un esempio di trattamento di dati sensibili è rappresentato dalla gestione complessiva delle cartelle dei pazienti. Questo criterio include anche i dati che possono più in generale essere considerati come aggravanti del possibile rischio per i diritti e le libertà delle persone, come i dati di comunicazione elettronica, i dati relativi

[3] Esempio: una banca che selezioni i propri clienti tramite una banca dati di riferimento del credito, o una società di biotecnologie che offre test genetici direttamente ai consumatori, al fine di valutare e prevedere i rischi di malattia / salute, o una società di costruzione di profili comportamentali o di marketing in base all'utilizzo o alla navigazione sul suo sito web.

all'ubicazione, i dati finanziari (che potrebbero essere utilizzati per le frodi nei pagamenti). A questo proposito, può essere rilevante definire se i dati siano stati resi pubblici dalla persona interessata o da terze parti. Il fatto che i dati personali siano disponibili al pubblico può essere considerato come un fattore significativo nel valutare se ci si aspetta che i essi siano ulteriormente utilizzati per diversi scopi. Questo criterio può anche includere informazioni elaborate da una persona fisica per l'esercizio di attività di carattere esclusivamente personale o domestico (come servizi informatici di *storage* per la gestione dei documenti personali, servizi di posta elettronica, diari, *e-reader* dotato di caratteristiche per prendere appunti, e varie applicazioni con credenziali che possono contenere dati sensibili), la cui comunicazione o elaborazione per scopi diversi da attività domestiche può essere percepito come trattamento molto invasivo.

5) I dati elaborati su larga scala: il GDPR non definisce espressamente cosa si intenda per "larga scala", anche se il considerando n. 91 fornisce alcune indicazioni. In ogni caso, i Garanti Europei segnalano che i seguenti fattori, in particolare, sono rilevanti al fine di determinare se il trattamento sia effettuato su larga scala:

- il numero di persone interessate, come numero specifico o come percentuale della popolazione di riferimento;
- il volume dei dati e/o la gamma di diversi elementi di dati in corso di elaborazione;
- la durata, o la permanenza, dell'attività di elaborazione dati;
- l'estensione geografica delle attività di elaborazione.

6) Set di dati che sono stati abbinati o combinati, ad esempio provenienti da due o più operazioni di trattamento effettuati per scopi diversi e/o da altri titolari, in modo tale da superare le ragionevoli aspettative dell'interessato.

7) I dati relativi ad interessati vulnerabili ex considerando n. 75: il trattamento di questo tipo di dati può richiedere una DPIA a causa del maggiore squilibrio di potere tra la persona e il titolare, cioè l'individuo non può essere in grado di consentire, od opporsi, al trattamento dei propri dati. Ad esempio, i dipendenti incontrerebbero spesso serie difficoltà nell'opporsi al trattamento effettuato dal datore di lavoro, quando legato alla gestione delle risorse umane. Allo stesso modo, i bambini possono essere considerati come non in grado di opporsi o acconsentire al trattamento dei propri dati consapevolmente e in maniera ponderata. Ciò riguarda anche il segmento più vulnerabile della popolazione che necessita di protezione speciale, come, ad esempio, i malati mentali, i richiedenti asilo, gli anziani, i pazienti, e in ogni caso i soggetti rispetto ai quali può essere identificato uno squilibrio nel rapporto tra la posizione della persona interessata e il titolare.

8) L'uso innovativo o l'applicazione di soluzioni tecnologiche o organizzative, come la combinazione dell'uso di impronte digitali con il riconoscimento del volto per un migliore controllo degli accessi fisici, ecc. Il GDPR chiarisce all'art. 35.1 e nei considerando nn. 89 e 91 che l'uso di una nuova tecnologia può innescare la necessità di effettuare un DPIA, in quanto può comportare nuove forme di raccolta e di uso dei dati, con probabile rischio elevato per i diritti e le libertà degli individui. Infatti,

le conseguenze personali e sociali della diffusione di una nuova tecnologia potrebbero essere sconosciute, pertanto, una DPIA aiuta il titolare del trattamento a comprendere e gestire tali rischi. Ad esempio, alcune applicazioni di "*Internet of things*" potrebbero avere un impatto significativo sulla vita quotidiana e sulla privacy degli individui, tali da rendere necessaria una DPIA.

9) Il trasferimento dei dati oltre i confini dell'Unione europea ex considerando n. 116: prende in considerazione, tra gli altri, il paese o i paesi di destinazione previsto/i, la possibilità di ulteriori trasferimenti o la probabilità di trasferimenti basati su deroghe per situazioni specifiche stabilite dal GDPR.

10) quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.

11) La DPIA è obbligatoria anche quando il trattamento rientra in una delle tipologie soggette al requisito di una valutazione d'impatto sulla protezione dei dati contenuta nell'elenco pubblico che verrà redatto dall'autorità di controllo ai sensi dell'art. 35.4.

3.2 CASI IN CUI LA DPIA NON È OBBLIGATORIA

Diversamente, una DPIA non è obbligatoria nei seguenti casi:

1) Quando il trattamento non è "suscettibile di provocare un rischio elevato per i diritti e le libertà delle persone fisiche" ex art. 35.1 GDPR.

2) Quando la natura, la portata, il contesto e finalità del trattamento sono molto simili a un trattamento per cui la DPIA è già stata effettuata. In tali casi, i risultati di DPIA per analogo trattamento possono essere utilizzati ex art. 35.1 GDPR.

3) Qualora il trattamento effettuato ai sensi dell'articolo 6.1, lettere c) o e) trovi la propria base giuridica nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 dell'art. 35 GDPR non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento [4].

4 Cfr. art. 35.10 del GDPR

4) Quando il trattamento è incluso nella lista opzionale (redatta dall'autorità di controllo) delle operazioni di trattamento per le quali non è necessaria la DPIA ex art. 35.5 GDPR.

5) Per i trattamenti già in essere alla data del 25 maggio 2018, se non sopravvengo cambiamenti tecnologici significativi o altri mutamenti significativi di condizioni[5].

3.3 ESITI DELLA VALUTAZIONE

Alla luce delle premesse e dei criteri suesposti, si è addivenuti alla conclusione che i trattamenti effettuati nell'ambito della sperimentazione clinica in oggetto rientrino nell'ipotesi di trattamenti di dati appartenenti alle categorie particolari relativi a soggetti/interessati vulnerabili.
La categoria di soggetti interessati, la quantità e, soprattutto, la natura sensibile dei dati oggetto di trattamento costituiscono fattori che hanno determinato l'obbligatorietà della valutazione d'impatto. Più specificamente, gli studi clinici, come meglio precisato nei paragrafi che seguono, implicano il trattamento di dati appartenenti alle categorie particolari di cui all'art. 9 del GDPR riferiti a persone vulnerabili. In particolare, nel corso delle sperimentazioni cliniche possono essere trattate notevoli quantità di dati personali idonei a rivelare lo stato di salute, la storia medica, lo stile di vita, la vita sessuale, l'origine etnica, nonché dati biologici e genetici, di numerosi pazienti coinvolti. Tali pazienti, per il loro particolare stato di vulnerabilità, sono suscettibili di essere sottoposti a forme di coercizione o influenza tali da ostacolare la libera espressione del loro consenso. Si pensi, ad esempio, a pazienti affetti da malattie incurabili o a persone indigenti per i quali è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento, nel senso che il singolo individuo potrebbe non disporre della piena capacità di autodeterminazione, con il rischio che si verifichi, di conseguenza, un possibile pregiudizio al diritto di acconsentire o di opporsi con facilità al trattamento dei propri dati personali, nonché di esercitare i propri diritti in materia di protezione dei dati personali.
Ne deriva, come si evince dal questionario allegato e compilato, la sussistenza di alcune delle condizioni che generano l'obbligo di condurre una DPIA. In altre parole, i trattamenti effettuati presentano rischi intrinseci elevati e quindi sono soggetti a valutazione d'impatto ai sensi dell'art. 35 GDPR.

4 FASE 2: DESCRIZIONE SISTEMATICA E FUNZIONALE DELLE OPERAZIONI DI TRATTAMENTO E DEL FLUSSO DI INFORMAZIONI

[5] L'obbligo di effettuare una DPIA si applica alle operazioni di trattamento che soddisfano i criteri di cui all'articolo 35 e avviate dopo che il GPDR diventa applicabile il 25 maggio 2018. Il Gruppo di Lavoro ex Art. 29 raccomanda vivamente di effettuare le DPIA per operazioni di trasformazione già in corso prima del maggio 2018. Se è intervenuto un cambiamento significativo per l'operazione di elaborazione dopo maggio 2018, ad esempio perché una nuova tecnologia è entrata in uso o perché i dati personale vengono utilizzati per scopi diversi, il trattamento diventa una nuova operazione di trattamento dati e potrebbe richiedere un DPIA. Il DPIA dovrebbe certamente essere rivisto quando c'è un cambiamento del rischio presentato da tale trattamento (articolo 35 (11)).

Una volta stabilito di procedere alla valutazione d'impatto, è stata effettuata la seguente ricognizione sistematica e funzionale dei trattamenti di dati personali effettuati nel corso dello studio clinico che presentano rischi elevati**.**

4.1 DESCRIZIONE DEL FLUSSO DELLE INFORMAZIONI

a) Raccolta, registrazione e archiviazione dei dati dei pazienti per il consenso informato

Il centro di sperimentazione, nell'ambito degli studi clinici, ha in via esclusiva il rapporto diretto coi pazienti e, pertanto, raccoglie i dati sensibili (relativi alla salute, genetici, biologici, sanitari, idonei a rivelare l'origine razziale ecc.) e comuni dei soggetti partecipanti allo studio clinico, direttamente, attraverso i moduli contenenti il consenso informato e le schede CRF in formato elettronico e, indirettamente, dagli eventuali laboratori di analisi esterni.
In conformità al protocollo, lo sperimentatore, prima che abbia inizio qualsiasi procedura correlata allo studio clinico, raccoglie i moduli di consenso informato ICF, contenenti nome e cognome del partecipante alla sperimentazione (cfr. all. 1), unitamente all'informativa sul trattamento dei dati personali ex art. 13 GDPR (cfr. all. 2). Il paziente e il principal investigator firmano due copie dell'ICF, una delle quali è rilasciata al paziente, mentre l'altro esemplare è archiviato dallo sperimentatore nel file del centro di sperimentazione *(*cd. *trial center file "TCF")*.

b) Pseudonimizzazione e conservazione dei log di identificazione

Al fine di tutelare l'identità delle persone coinvolte nello studio in conformità alle disposizioni previste dalla normativa di settore[6], il principal investigator (i.e. lo sperimentatore principale)**,** al momento dell'arruolamento del paziente nello studio clinico, assegna a questi un codice di identificazione alfanumerico (ad esempio: ab0001), che non permette di risalire direttamente alla sua identità e che viene utilizzato, al posto del relativo nominativo, in ciascuna comunicazione di dati collegati allo studio fra il centro partecipante alla sperimentazione e il promotore.
Il registro che contiene gli *identification log* è custodito, esclusivamente, dal centro di sperimentazione e detenuto separatamente dal resto della documentazione come documento riservato essenziale alla conduzione dello studio clinico. Soltanto il centro di sperimentazione, i medici sperimentatori e i soggetti autorizzati per legge sono in grado di collegare il codice all'identità ed ai risultati dello studio.

[6] Nell'ambito delle sperimentazioni cliniche di medicinali, si veda il d.m. 15 luglio 1997 nonché l'art. 16, co. 5, D.Lgs. 211/2003.

c) Raccolta dei dati dei pazienti nel corso della visita di screening preliminare allo studio clinico

Secondo il protocollo dello studio clinico, dopo la sottoscrizione da parte del paziente del consenso informato (ICF) e dell'informativa sul trattamento dei dati personali ex art. 13 GDPR (cfr. all. 2), il medico sperimentatore**,** attraverso una visita di screening, verifica l'idoneità del paziente alla partecipazione allo studio clinico; a tal fine, gli viene assegnato un codice identificativo di screening, solitamente tramite IXRS (Interactive Voice/Web Response System) ovvero manualmente.

Durante la visita è prevista la raccolta di una serie di informazioni ulteriori rispetto ai dati medico/clinici riferiti all'interessato, quali dati di carattere demografico (es. data di nascita, età, sesso ecc.) o relativi alla storia medica del paziente, agli stili di vita o alla vita sessuale. Dette informazioni, riportate sui documenti essenziali alla conduzione dello studio, sono conservate dai centri partecipanti e dal promotore per il periodo di tempo necessario al completamento dello studio clinico e, successivamente, per tutta la durata stabilita dal protocollo.

d) Raccolta e comunicazione dei dati dei pazienti allo sponsor nel corso dello studio clinico

I dati dei pazienti raccolti dal centro di sperimentazione - sia durante la visita di screening volta a verificare la loro idoneità alla partecipazione allo studio clinico sia nel corso dello studio stesso - vengono riportati dallo sperimentatore nelle "CRF" (*Case Report Form*), ovverosia schede di raccolta dei dati dello studio clinico, il cui schema è stabilito dal promotore. Più precisamente, tutti i dati raccolti dal centro di sperimentazione direttamente dai pazienti o indirettamente dai laboratori locali, confluiscono, *in primis*, nella cartella clinica elettronica dello studio *cd. investigator trial center file* "TCF" presso il centro di sperimentazione e, successivamente (ad eccezione del nominativo del paziente e del suo codice identificativo, età, anno di nascita e sesso), vengono inseriti dallo sperimentatore in CRF. I dati sono quindi trasferiti al promotore (Fondazione), che li registra e conserva nella cartella clinica principale dello studio, identificata col codice pseudonimizzato del paziente, che risiede nei sistemi informativi del promotore stesso.

e) Trasferimento extra UE dei dati dei pazienti

Nell'ambito dello studio clinico in esame, i dati dei pazienti non vengono trasferiti al di fuori dello Spazio Economico Europeo. È esclusa, inoltre, la possibilità di accesso da remoto ai dati relativi allo studio clinico da parte di soggetti ubicati in Paesi extra SEE.

f) Conservazione e archiviazione dei dati

I documenti essenziali ai fini dello studio clinico, tra i quali le CRF, le segnalazioni ed i rapporti relativi a eventi avversi, gli ICF, i rapporti delle visite di monitoraggio, il documento che contiene i *log* di identificazione del paziente, e, in generale, tutti i dati raccolti dal centro di sperimentazione direttamente dai pazienti o, eventualmente, indirettamente dai laboratori locali sono conservati sia dal promotore (la Fondazione) che dallo sperimentatore al fine di verificare la conduzione della sperimentazione clinica e la qualità dei dati ottenuti (monitoraggio da parte del promotore e ispezione da parte delle autorità regolatorie).

Le informazioni summenzionate sono conservate in maniera cifrata presso i sistemi della Fondazione in un *secured repository,* a cui hanno accesso soltanto i soggetti dotati di apposite credenziali e profili di autenticazione.

Nella fase di memorizzazione o archiviazione dei dati sono adottati accorgimenti adeguati a garantire la qualità dei dati dello studio e la loro protezione dai rischi di accesso abusivo, furto o smarrimento - parziale o integrale – dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, mediante l'applicazione di tecnologie crittografiche a *file system* o database) nelle operazioni di registrazione e archiviazione dei dati.

4.2 RUOLI PRIVACY DEI SOGGETTI COINVOLTI

Preliminarmente appare opportuno esaminare, anche sulla base delle disposizioni normative e regolamentari di settore applicabili, il rapporto intercorrente tra i promotori di studi clinici e i centri di sperimentazione, al fine di ricostruire in maniera puntuale i ruoli effettivamente svolti dai predetti soggetti in relazione ai trattamenti di dati personali.

Al riguardo, va evidenziato, in termini generali, che il promotore, prima dell'avvio della sperimentazione, identifica i possibili centri partecipanti verificandone l'idoneità e il relativo interesse; inoltre, predispone il protocollo da osservare nel corso dello studio e impartisce ai centri le necessarie direttive sul trattamento dei dati, ivi compresi i profili relativi alla loro custodia e sicurezza, nonché le istruzioni relative alle modalità di utilizzo dei sistemi informativi eventualmente previsti; verifica poi, a mezzo di propri collaboratori, l'osservanza del protocollo e delle proprie procedure interne da parte del centro; predispone i documenti da impiegare per informare le persone partecipanti circa il trattamento dei dati personali che li riguardano; infine, avverte i centri quando non è più necessario conservare la documentazione relativa allo studio.

Il promotore non effettua, pertanto, alcuna attività di raccolta diretta dei dati, né può interloquire con gli individui inclusi nello studio clinico - compiti, questi, spettanti ai medici sperimentatori. Tuttavia, il promotore può acquisire, in diverse ipotesi, i dati dei pazienti raccolti dai centri, effettuando sugli stessi diverse operazioni di trattamento (es. tramite i propri collaboratori addetti al monitoraggio, il promotore può esaminare presso i centri le informazioni contenute nella documentazione medica

originale e nella lista di identificazione delle persone coinvolte nello studio, ovvero riceve i dati registrati da ciascun centro sulle schede di raccolta dati e sulle segnalazioni di eventi avversi).

Va rilevato che il centro di sperimentazione non è assoggettato a vincoli di subordinazione nei confronti del promotore: accetta il protocollo concordandone con il promotore alcuni aspetti ed esegue lo studio clinico con propria autonomia organizzativa, pur nel rispetto del protocollo e delle direttive del promotore; si avvale di collaboratori che ritiene idonei ed è responsabile del loro operato; egli inoltre fornisce l'informativa alle persone coinvolte nello studio, acquisendo, se richiesto, il loro consenso anche per ciò che attiene al trattamento dei dati personali che le riguardano; autorizza i collaboratori dello sponsor (interni o esterni) - c.d. monitor-CRA - ad accedere ai documenti medici originali dei pazienti nell'ambito di attività di monitoraggio; inoltre, egli gestisce e custodisce sotto la propria responsabilità detta documentazione.

Dalla ricostruzione delle attività poste in essere dai vari attori nell'ambito degli studi clinici, atteso che i singoli centri di sperimentazione e i promotori hanno in genere responsabilità distinte, prendendo decisioni importanti quanto alle modalità di trattamento dei dati personali relativi agli studi clinici, emerge come, nel caso di specie, il rapporto intercorrente tra la Fondazione (soggetto promotore) e i centri di sperimentazione, per ciò che riguarda il trattamento dei dati personali, sia da qualificarsi come rapporto tra due autonomi titolari del trattamento dei dati personali.

Il promotore può inoltre stipulare un contratto con soggetti esterni (es. organizzazioni di ricerca a contratto, laboratori di analisi, ecc.) allo scopo di delegare loro specifici compiti afferenti allo studio clinico (es. attività di monitoraggio). Tali soggetti (persone fisiche o giuridiche), cui sono affidate specifiche attività di trattamento per conto del promotore, devono essere inquadrati quali responsabili del trattamento ai sensi dell'art. 28 del GDPR.

4.3 NATURA E TIPI DI DATI TRATTATI

I dati raccolti e trattati nell'ambito dello studio clinico sono da qualificare come dati personali ai sensi dell'art. 4, n. 1) del Regolamento, ovverosia *"[…] qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")"* e risulta pertanto applicabile la disciplina in materia di protezione dei dati personali di cui al GDPR e al Codice Privacy. Possono inoltre formare oggetto di trattamento i dati personali appartenenti alle categorie particolari di cui all'art. 9 del GDPR, ovverosia i *"[...] dati personali che rivelino l'origine razziale o etnica...dati genetici...dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".*

In merito alla possibilità di identificare i soggetti partecipanti a uno studio clinico, il promotore, quale misura di sicurezza a tutela dell'identità dei pazienti, attua una procedura interna di codificazione dell'identità dei soggetti coinvolti nello studio clinico: detta procedura prevede l'utilizzo di codici alfanumerici che consentono di identificare univocamente i singoli interessati all'interno dello studio,

senza utilizzare il nominativo, l'indirizzo o numeri di identificazione personale. I predetti accorgimenti, tuttavia, non sono in grado di rendere effettivamente anonimi i dati oggetto di trattamento: infatti, la quantità e la tipologia di dati forniti al promotore, sebbene siano pseudonimizzati, comporta la possibilità di riconoscere l'interessato.

Tra le informazioni raccolte nel corso dello studio clinico risultano, in genere, uno o più elementi caratteristici dell'identità delle persone coinvolte (come ad esempio l'anno di nascita, età, sesso, razza, etnia, peso, altezza), nonché informazioni di carattere medico/clinico o relative agli stili di vita e a particolari patologie, per cui la combinazione di tali elementi con altri, come la collocazione geografica (desumibile in alcuni casi dai dati identificativi del centro di sperimentazione e/o dello sperimentatore), potrebbero condurre all'identificazione del paziente.

Sebbene soltanto i centri di sperimentazione abbiano la disponibilità della lista che consente di associare il nominativo della persona al relativo codice identificativo ed il promotore non debba venire a conoscenza dell'identità dei partecipanti allo studio, quest'ultimo, tramite propri collaboratori addetti al monitoraggio, nell'ambito delle visite effettuate presso il centro di sperimentazione volte a controllare che lo studio sia condotto in osservanza del protocollo, ha accesso, sotto il controllo dei medici, sia alla documentazione sanitaria originale delle persone coinvolte nello studio (per verificare l'accuratezza e la completezza dei dati) sia alla lista contenente i nominativi degli interessato (per controllare le procedure riguardanti l'acquisizione del consenso informato).

Nello studio clinico in esame, la quantità e la tipologia di informazioni raccolte, le modalità di trattamento previste nonché le diverse categorie di soggetti che possono avervi accesso, comportano pertanto la possibilità concreta di identificare gli interessati. Ciò, sia pure indirettamente, mediante il riferimento ad altre informazioni detenute dal medesimo promotore o a qualsiasi altra informazione non necessariamente nella disponibilità di quest'ultimo, ma detenuta da terzi.

Sul punto va soggiunto che, in conformità a quanto disposto nel considerando 26 e all'art. 4 del GDPR, i dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile; ove, per stabilire l'identificabilità, è opportuno considerare tutti i mezzi, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente.

Alla luce delle suddette considerazioni e dei principi espressi dal Garante per la Protezione dei Dati personali nelle *Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali - 24 luglio 2008*[7] - applicabili, su indicazione dell'Autorità stessa, anche agli studi clinici condotti su dispositivi medici - le informazioni legate al codice identificativo di ciascun paziente non possono essere considerate quali dati anonimi, bensì dati personali – nella specie, biologici, genetici, idonei a rivelare lo stato di salute ecc. – che riguardano i pazienti coinvolti nello

[7] *(G.U. n. 190 del 14 agosto 2008)* Registro delle deliberazioni n. 52 del 24 luglio 2008 doc. web n. 1533155.

studio clinico, con tutte le conseguenze derivanti in termini di normativa applicabile in materia di trattamento dei dati personali.

4.4 ASPETTI DEI TRATTAMENTI RILEVANTI SUSCETTIBILI DI GENERARE UN RISCHIO PIÙ ELEVATO PER I DIRITTI FONDAMENTALI DELLE PERSONE FISICHE

In linea generale, l'affidabilità e l'idoneità delle procedure adottate negli studi clinici – dal promotore e dal centro di sperimentazione – al fine di tutelare la riservatezza degli interessati dipende anche dalla validità delle tecniche di pseudonimizzazione implementate, dall'integrità e dall'adeguatezza del centro di sperimentazione, dello sperimentatore e del suo *team* e dei *monitor* nonché dall'efficienza dei sistemi di sicurezza informatici e cartacei predisposti.
Nonostante nell'ambito di uno studio clinico sia stato adottato un sistema di codificazione idoneo a limitare fortemente il numero delle persone che possono accedere alle informazioni dei soggetti partecipanti, allo stesso tempo non è da escludere che sussista la possibilità di collegare il codice con la documentazione originale, risalendo in questo modo alla identità della persona fisica che partecipa alla ricerca. Tale possibilità di collegamento, oltre che un vantaggio, costituisce un limite alla riservatezza delle persone fisiche coinvolte nello studio clinico.

a) Adeguatezza dei soggetti che collaborano con i promotori

Rispetto al trattamento dei dati personali effettuato nel corso degli studi clinici, il centro di sperimentazione, titolare autonomo del trattamento dei dati, è direttamente responsabile della procedura di pseudonimizzazione e dei profili di conservazione e sicurezza dei *log* di identificazione.
La particolare delicatezza dei dati trattati nello studio clinico impone, inoltre, che siano puntualmente adottate le ulteriori cautele richiamate dal Garante nelle citate "Linee guida" con riferimento ai soggetti, interni o esterni, che collaborano con i promotori per svolgere attività o parti di attività inerenti agli studi e, in particolare, per l'attività di monitoraggio.
Si fa riferimento, per esempio, ai collaboratori del promotore – personale dipendente o personale delle CRO – autorizzati ad accedere e consultare tutta la documentazione originale dello studio clinico presso il centro di sperimentazione (compresa la lista contenente i dati nominativi degli interessati) nel corso dello svolgimento dell'attività di monitoraggio.
È dunque necessario sottoporre tali soggetti a regole di condotta analoghe al segreto professionale e di predisporre interventi formativi specifici nei loro confronti in merito ai rischi e alle responsabilità derivanti dal trattamento dei dati, alle istruzioni da osservare per la loro custodia e sicurezza, alle regole di riservatezza e confidenzialità previste dalle disposizioni normative applicabili, nonché alle precauzioni da utilizzare per tutelare l'identità degli interessati.

b) Custodia e trasmissione dei dati

Aspetti critici in tema di sicurezza dei dati che riguardano direttamente il promotore, si rilevano rispetto a:

- la custodia dei dati personali, intesa come conservazione nel corso dello studio e archiviazione, una volta concluso lo studio clinico, dei dati sensibili, dei campioni biologici e dei dati genetici dei pazienti da parte dello sponsor (tali criticità riguardano anche i centri di sperimentazione per la propria parte di competenza, in relazione al ruolo ricoperto nel trattamento dei dati e alle conseguenti responsabilità, ai fini dell'adozione delle misure di sicurezza);
- le operazioni di registrazione attraverso strumenti elettronici dei dati sensibili delle persone coinvolte nello studio clinico;
- la trasmissione per via telematica dei dati al promotore o ai soggetti esterni che collaborano con lo stesso per l'esecuzione dello studio (ad esempio, che svolgono attività di validazione ed elaborazione statistica e gestione della banca dati).

Più precisamente, la sensibilità dei dati trattati impone l'adozione di misure idonee ad evitare rischi di accesso abusivo ai dati, come tecnologie crittografiche a file system o database che rendano inintelligibili i dati ai soggetti non legittimati, nonché, idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento, avendo cura di utilizzare credenziali di validità limitata alla durata dello studio e di disattivarle al termine dello stesso, oltre a procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati del trattamento e sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

Particolare attenzione va riservata, inoltre, alla necessità di proteggere i dati nel corso della trasmissione ai soggetti esterni di cui lo stesso promotore si avvale per la conduzione dello studio. A questo proposito, sono utilizzati canali di trasmissione protetti che prevedono l'uso di protocolli di comunicazione sicuri basati su standard crittografici.

A ciò si aggiunga che il promotore, per quel che concerne l'accesso ai dati dello studio clinico memorizzati nel proprio database, ha implementato idonei sistemi di autenticazione e di autorizzazione per il personale preposto al trattamento in funzione dei ruoli ricoperti e delle esigenze di accesso e trattamento, che prevedono l'utilizzo di credenziali di autenticazione di validità limitata alla durata dello studio e la loro disattivazione al termine dello stesso. Sono stati altresì adottate procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati ai soggetti autorizzati al trattamento ai sensi degli artt. 29 e 32 del GDPR e 2 – *quaterdecies* del Codice Privacy.

Da ultimo, il promotore ha previsto sistemi di audit log per il controllo degli accessi dal database e per il rilevamento di eventuali anomalie.

5 FASE 3: ANALISI DELLA CONFORMITA' NORMATIVA

5.1 LICEITA' DEL TRATTAMENTO E TRASFERIMENTO EXTRA UE

In via preliminare si osserva che il trattamento di dati personali per scopi di ricerca scientifica deve essere effettuato nel rispetto del Regolamento, del Codice privacy, delle Prescrizioni relative al trattamento dei dati genetici (se necessario) e delle Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, allegati 4 e 5 al provvedimento del 5 giugno 2019, delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, che costituiscono condizione essenziale di liceità e correttezza dei trattamenti (v. art. 2-*quater* del Codice Privacy e art. 21, comma 5 del D.Lgs. 10 agosto 2018, n. 101) nonché, da ultimo, delle garanzie da osservare ai sensi dell'art. 106, comma 2, lett. d) del Codice Privacy individuate dal Garante per la Protezione dei Dati Personali con il provvedimento n. 298 del 9 maggio 2024.

Ciò posto, in base all'art. 110 del Codice Privacy, rubricato *"Ricerca medica, biomedica ed epidemiologica"*, il trattamento dei dati relativi alla salute ai fini di ricerca scientifica in campo medico, biomedico ed epidemiologico può essere effettuato senza la previa acquisizione del consenso dell'interessato, a condizione che la ricerca sia eseguita in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'art. 9, par. 2, lett. j) del GDPR (compreso il caso in cui la ricerca rientri in un programma di ricerca biomedica o sanitaria previsto dall'art. 12-bis del D.Lgs. 502/1992) e sia condotta e resa pubblica una valutazione d'impatto ai sensi degli artt. 35 e 36 del GDPR.

Un'ulteriore ipotesi in cui non risulta necessaria la raccolta del consenso dell'interessato è ravvisabile nelle situazioni in cui, per particolari motivi, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato da parte del titolare del trattamento (si pensi, ad esempio, agli interessati non contattabili ovvero deceduti), oppure rischi di rendere impossibile o pregiudicare gravemente il conseguimento delle finalità di ricerca. In tali casi, il programma di ricerca è oggetto di motivato parere favorevole del competente Comitato Etico a livello territoriale; tuttavia, ferma la necessità di svolgere una valutazione d'impatto ex art. 35 del GDPR, a seguito dell'intervenuta modifica dell'art. 110 del Codice Privacy ad opera dell'art. 44, comma 1-bis della Legge 29 aprile 2024, n. 56, di conversione del D.L. n. 19 del 2 marzo 2024, recante ulteriori disposizioni urgenti per l'attuazione del PNRR, **non è più necessario sottoporre il protocollo dello studio alla consultazione preventiva dell'Autorità garante ai sensi dell'art. 36 del GDPR**. Tale ultimo adempimento implicava che il titolare del trattamento sottoponesse all'Autorità anche la valutazione d'impatto sul trattamento dei dati personali necessari per la realizzazione del progetto di ricerca.

Nello specifico, qualora il trattamento dei dati sulla salute per finalità di ricerca medica, biomedica ed epidemiologica si riferisca a soggetti deceduti o non contattabili per motivi etici od organizzativi - quindi siano riconducibile alla seconda fattispecie di esonero dal consenso normata dall'art. 110 del

Codice Privacy -, trovano applicazione anche le garanzie individuate dal Garante con il provvedimento n. 298 del 9 maggio 2024 adottato ai sensi del combinato disposto degli artt. 106, co. 2, lett. d) e 110 cpv del Codice Privacy.

In particolare, sono considerati motivi etici quelli *"riconducibili alla circostanza che l'interessato ignora la propria condizione".* Rientrano in questa categoria le ricerche per le quali l'informativa sul trattamento dei dati da rendere agli interessati comporterebbe la rivelazione di notizie concernenti la conduzione dello studio la cui conoscenza potrebbe arrecare un danno materia o psicologico agli interessati stessi.

Sono invece motivi di impossibilità organizzativa quelli *"riconducibili alla circostanza che la mancata raccolta dei dati riferiti al numero di interessati che non è possibile contattare, rispetto al numero complessivo dei soggetti che si intende arruolare nella ricerca, produrrebbe conseguenze significative per lo studio in termini di qualità dei risultati della ricerca stessa..."*. Ciò tenuto conto, in particolare, dei criteri di inclusione previsti dallo studio, delle modalità di arruolamento, della numerosità statistica del campione prescelto, nonché del periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti. Si precisa, a questo proposito, che i motivi di impossibilità organizzativa concernono sia quelli derivanti dalla circostanza, da considerarsi del tutto residuale, che contattare gli interessati implicherebbe uno sforzo sproporzionato vista la particolare elevata numerosità del campione, sia quelli derivanti dalla circostanza, alternativa alla precedente, che all'esito di ogni ragionevole sforzo compiuto per contattarli (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto pubblicamente accessibili) essi risultino al momento dell'arruolamento nello studio, deceduti o non contattabili.

In tali casi, il titolare del trattamento, oltre ad adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, ed acquisire il parere favorevole del competente Comitato Etico a livello territoriale sul progetto di ricerca come previsto dall'art. 110 del Codice Privacy, deve accuratamente motivare e documentare, nel progetto di ricerca, la sussistenza delle ragioni etiche od organizzative per le quali informare gli interessati e, quindi, acquisire il consenso, risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, se del caso documentando altresì i ragionevoli sforzi profusi per tentare di contattarli.

Nel caso in cui non ricorra alcuno dei casi sopra richiamati di deroga all'obbligo di acquisizione di un preventivo consenso dell'interessato, il trattamento dei dati personali – di natura particolare - per finalità di ricerca medica dovrà sottostare alla condizione di liceità del consenso esplicito dell'interessato ai sensi dell'art. 9, par. 2, lett. a) del Regolamento, quale presupposto volto a garantire la legittimità del trattamento.

In questi casi, il consenso deve consistere in una manifestazione di volontà che presenti le caratteristiche elencate nell'art. 4, par. 1, n. 11, GDPR, ovverosia *"[…] libera, specifica, informata e inequivocabile".* Allo stesso tempo, l'interessato deve essere adeguatamente informato circa la possibilità di revocare il consenso in qualunque momento e senza giustificazioni con la stessa facilità con cui l'ha prestato nonché le possibili conseguenze in caso di rifiuto di prestarlo.

È altresì opportuno specificare che il consenso quale base giuridica per il trattamento dei dati personali dell'interessato rappresenta un presupposto diverso e distinto dal **consenso informato** alla partecipazione alla ricerca e allo studio clinico, previsto dalla disciplina di settore. A questo proposito, è necessario che i soggetti coinvolti nello studio clinico, dopo essere stati informati di tutti gli aspetti della sperimentazione – ed in particolare dei rischi e benefici derivanti dalla partecipazione - confermino volontariamente ed in maniera documentata la propria disponibilità a prendervi parte, tramite la compilazione e sottoscrizione del modulo di consenso informato (ICF) loro somministrato.

Prima di ottenere il consenso informato, è essenziale che lo sperimentatore permetta ai pazienti di comprendere le caratteristiche dello studio clinico, concedendo loro il tempo necessario per decidere se partecipare o meno, se del caso rispondendo in maniera esaustiva alle domande poste dal paziente.

Il consenso informato deve essere scritto, datato e firmato dal membro del centro di sperimentazione che tiene il colloquio preliminare e dal soggetto che prende parte allo studio clinico o, qualora il soggetto non sia in grado di fornire un consenso informato, dal suo rappresentante legale designato, dopo essere stato debitamente informato circa le caratteristiche dello studio clinico – es. natura, obiettivi, benefici, rischi ecc. -, i diritti e le garanzie riconosciuti ai partecipanti allo studio, le condizioni in base alle quali viene condotto lo studio, la sua durata nonché i possibili trattamenti alternativi, comprese le misure di *follow-up* qualora la partecipazione del soggetto allo studio venga sospesa. Il paziente partecipante allo studio deve ricevere una copia del modulo contenente il consenso informato.

I dati acquisiti dal centro di sperimentazione vengono trasmessi al promotore (nella specie, la Fondazione) e alle persone da questi debitamente autorizzate ai sensi degli artt. 29 e 32 del GDPR e 2-*quaterdecies* del Codice Privacy, o alle eventuali società esterne, designate responsabili del trattamento ai sensi dell'art. 28 del GDPR, che agiscono per suo conto e alle quali sono affidate alcune o tutte le mansioni riguardanti la sperimentazione (es. monitoraggio e verifica dello studio, inserimento, validazione e analisi dei dati, esecuzione degli esami clinici e di laboratorio previsti dal protocollo ecc.).

I dati conferiti dagli interessati sono trattati dalla Fondazione anche per l'adempimento degli obblighi normativi – compresi quelli in materia di affidabilità e sicurezza, archiviazione della documentazione clinica e comunicazione dei dati della sperimentazione alle autorità nazionali competenti nel corso di un'ispezione conformemente alle pertinenti norme nazionali -, sulla base degli artt. 6, par. 1, lett.

a) – per i dati personali comuni – e 9, par. 2, lett. i) e g) del GDPR e 2-*sexies* del Codice Privacy – in riferimento ai dati particolari di cui all'art. 9 del GDPR.

Infine, nell'informativa rilasciata ai sensi dell'art. 13 del GDPR (cfr. all. 2) la Fondazione ha specificato che il trattamento svolto nell'ambito dello studio clinico non comporta alcun trasferimento di dati personali verso Paesi situati al di fuori dello Spazio Economico Europe ("SEE").

Nell'eventualità in cui, nel corso del trattamento, emerga la necessità di trasferire i dati personali verso Paesi situati al di fuori dello Spazio Economico Europeo che non garantiscono un livello adeguato di protezione ai dati personali dell'interessato, il Titolare sarà tenuto ad utilizzare uno degli strumenti di trasferimento previsti dagli artt. 45 e ss. del GDPR, e, prima di procedervi, dovrà verificare il rischio insito nel trasferimento stesso mediante un *Transfer Impact Assessment,* richiedendo al soggetto importatore l'eventuale adozione delle misure di sicurezza supplementari previste nelle "*Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE"* adottate dall'European Data Protection Board il 18 giugno 2021. Il trasferimento di dati personali extra SEE dovrà inoltre essere indicato all'interno dell'informativa privacy rilasciata agli interessati.

5.2 PRINCIPIO DI LIMITAZIONE DELLE FINALITÀ

L'oggettiva individuazione preventiva delle finalità del trattamento rappresenta un elemento fondamentale nella disciplina della protezione dei dati personali, atteso che, da tale identificazione, può essere tracciato il perimetro all'interno del quale il titolare del trattamento è legittimato a svolgere le attività di trattamento predeterminate.

La corretta applicazione del principio di limitazione delle finalità di cui all'art. 5, par. 1, lett. b) del GDPR presuppone infatti che l'interessato sia posto nelle condizioni di scegliere consapevolmente se affidare o meno a un terzo i propri dati personali, basando tale decisione anche su informazioni sufficientemente chiare e dettagliate che gli permettano di comprendere gli scopi per i quali tali dati verranno usati.

Nel caso di specie, i dati personali dei pazienti vengono raccolti unicamente per finalità esplicite e legittime di ricerca scientifica, indicate dal titolare del trattamento.

Nell'informativa somministrata agli interessati ai sensi dell'art. 13 GDPR (cfr. all. 2), tali finalità sono comunicate in maniera chiara e inequivocabile e i dati sono successivamente trattati in modo compatibile con le finalità per cui sono stati raccolti.

5.3 PRINCIPIO DI LIMITAZIONE DELLA CONSERVAZIONE

In relazione alla conservazione dei dati, in linea generale si osserva che, nell'ambito di un trattamento di dati personali, il titolare ha l'obbligo di garantire che il periodo di conservazione dei dati personali sia limitato al minimo necessario. Onde assicurare che i dati personali non siano

conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica (cfr. *Cons. 39, GDPR*).

Pertanto, affinché il trattamento sia conforme al principio di limitazione della conservazione dei dati previsto dall'art. 5, par. 1, lett. e), GDPR, è necessario che il titolare indichi i periodi di conservazione applicabili nei singoli casi ovvero, qualora non sia possibile stabilire in via diretta ed immediata un preciso termine temporale, dia evidenza dei criteri utilizzati per determinarne la durata.

Ne consegue che, qualora i dati risultino eccedenti o non pertinenti o non indispensabili, non potranno essere utilizzati, salvo che si renda necessaria la conservazione per periodi di tempo ulteriori, come, per esempio, quando il titolare debba assolvere ad obblighi di legge o di regolamento, od ottemperare ad un provvedimento dell'Autorità giudiziaria o dell'Autorità di controllo ovvero debba accertare, esercitare o difendere un diritto del titolare in sede giudiziaria.

Nell'ambito dello studio clinico in esame, i dati raccolti e trattati dal promotore per l'esecuzione della ricerca sono conservati mediante l'applicazione di idonei accorgimenti – es. tecniche di cifratura o l'utilizzo di codici identificativi – atti ad impedire che tali dati possano risultare direttamente riconducibili agli interessati.

I dati sono conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali gli stessi sono stati raccolti e successivamente trattati. In particolare, i documenti essenziali relativi allo studio (compresa la documentazione medica riferita ai singoli individui) devono essere conservati presso il promotore e i centri partecipanti per almeno **sette anni** dopo il completamento della sperimentazione, ovvero per un periodo di tempo più lungo in conformità alla disciplina applicabile allo studio clinico o agli accordi intervenuti fra il promotore medesimo e i centri partecipanti o, ancora, secondo quanto espressamente indicato nel progetto di ricerca.

Decorso il periodo di conservazione stabilito in relazione allo studio clinico, i dati sono anonimizzati in maniera irreversibile o cancellati definitivamente.

5.4 PRINCIPIO DI MINIMIZZAZIONE DEI DATI

Il principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. c), GDPR impone al titolare del trattamento di raccogliere e trattare soltanto i dati necessari (*id est* non eccedenti) in relazione alle finalità perseguite.

Nell'ambito degli studi clinici, al fine di tutelare l'identità delle persone coinvolte nella sperimentazione, la normativa applicabile prevede che il centro partecipante assegni un codice di identificazione a ciascun interessato, al momento del suo coinvolgimento, e lo utilizzi al posto del relativo nominativo in ciascuna comunicazione al promotore di dati collegati allo studio. Una lista, che consente di associare ai codici i dati nominativi dei pazienti, è detenuta esclusivamente dal centro di sperimentazione che la custodisce come documento riservato essenziale alla conduzione dello studio clinico.

Il principio di minimizzazione dei dati è pienamente soddisfatto tenuto conto della procedura di pseudonimizzazione adottata dai centri di sperimentazione, i quali codificano i dati identificativi dei pazienti, trasmettendoli con comunicazioni cifrate al promotore, il quale, pertanto, tratta solo dati pseudonomizzati.

Ne consegue, pertanto, che i dati oggetto dell'attività di trattamento svolte nell'ambito dello studio clinico non vengono raccolti in misura maggiore rispetto a quella necessaria ed appaiono, inoltre, adeguati e pertinenti rispetto alla finalità perseguite dal titolare del trattamento.

5.5 PRINCIPIO DI TRASPARENZA

Il principio di trasparenza sancito dall'art. 5, par. 1, lett. a) del Regolamento impone ai titolari di informare l'interessato sui principali elementi del trattamento, al fine di renderlo consapevole delle caratteristiche essenziali dello stesso. Detto principio risponde altresì alla necessità di permettere all'interessato, se del caso, l'esercizio del diritto di revoca del consenso sancito dall'art. 7, par. 3 del Regolamento.

In particolare, come precisato dal Considerando 39, devono essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati i dati personali che le riguardano nonché la misura in cui tali dati personali sono o saranno trattati.

Al riguardo, si rappresenta che, in ambito sanitario, pur nel rispetto dell'obbligo di comunicare gli elementi di cui agli artt. 13 e 14 del Regolamento, le informazioni vanno rese nei confronti dell'interessato in forma concisa, trasparente, intelligibile e facilmente accessibile nonché con linguaggio semplice e chiaro (cfr. art. 12, par. 1 del Regolamento, e artt. 78 e 79 del Codice Privacy).

Per quanto concerne le modalità con cui fornire l'informativa, alla luce del principio di responsabilizzazione di cui all'art. 5 del Regolamento, spetta al titolare scegliere le modalità più appropriate al caso di specie, tenendo conto di tutte le circostanze del trattamento e del contesto in cui viene effettuato (ad esempio, il dispositivo utilizzato, la natura dell'interazione con il titolare e le eventuali limitazioni che implicano certi fattori ecc.).

Nell'ambito degli studi clinici, i promotori, di regola, individuano le informazioni da comunicare alle persone coinvolte nello studio e la procedura da seguire per raccogliere il loro consenso informato tramite i centri di sperimentazione, e, se necessario, anche il consenso per ciò che concerne i trattamenti dei dati che li riguardano, per consentirne l'esame da parte dei comitati etici interessati.

All'interno dell'informativa resa all'interessato devono essere esplicitate, in maniera chiara e puntuale, gli elementi obbligatori previsti dall'art. 13 del Regolamento e, in particolare, la natura dei dati trattati dal promotore e se tali dati siano trasmessi al di fuori dello Spazio Economico Europeo; il ruolo effettivamente svolto dal promotore riguardo al trattamento dei dati nonché le basi di liceità e le finalità di quest'ultimo; i soggetti o le categorie di soggetti ai quali di dati possono essere comunicati; i diritti che possono essere esercitati dall'interessato. In mancanza di tali indicazioni, o

qualora queste non appaiano sufficientemente comprensibili, l'informativa fornita non potrà essere considerata idonea a rendere sufficientemente edotto l'interessato circa il trattamento dei suoi dati e l'eventuale consenso raccolto dal titolare non sarà ritenuto valido.
L'informativa deve, inoltre, evidenziare la natura obbligatoria o facoltativa del conferimento dei dati rispetto al perseguimento delle finalità del trattamento.
Inoltre, deve essere cura dei centri di sperimentazione assicurarsi che il personale coinvolto nello studio clinico, in particolare nei colloqui preliminari volti all'acquisizione del consenso informato, sia formato adeguatamente anche in merito agli aspetti rilevanti della disciplina sulla protezione dei dati personali, in modo da essere in grado di spiegare accuratamente e con completezza agli interessati gli elementi essenziali riguardanti il trattamento dei dati personali.
Qualora i dati siano ottenuti presso terzi il titolare del trattamento può non rendere le informazioni di cui ai parr. da 1 a 4 dell'art. 14 del Regolamento, nella misura in cui ciò risulti impossibile o implichi uno sforzo sproporzionato. Ciò, in particolare, nell'ambito dei trattamenti svolti per finalità di ricerca scientifica, ferme restando le condizioni e le garanzie di cui all'articolo 89, paragrafo 1 del Regolamento. In tali casi, il titolare del trattamento è comunque tenuto ad adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni (v. art. 14, par. 5, lett. b) del Regolamento).
Nell'ambito dello studio clinico oggetto della presente DPIA, l'informativa somministrata ai pazienti partecipanti allo studio clinico e il consenso informato da questi acquisito prima della raccolta dei dati appaiono conformi alla normativa in materia di protezione dei dati personali e, nello specifico, al principio di trasparenza sancito dall'art. 5, par. 1, lett. a), GDPR nonché alle norme di settore applicabili.

5.6 DIRITTI DELL'INTERESSATO

Le persone partecipanti agli studi clinici possono esercitare in ogni momento i diritti di cui agli artt. da 15 a 22 del GDPR, trai quali quello di accesso ai dati che li riguardano e di ottenerne la comunicazione in forma intelligibile, ovvero l'aggiornamento o la rettifica, rivolgendosi direttamente al centro di sperimentazione o, per il tramite del medico sperimentatore (che è a conoscenza della loro identità e, mediante l'accesso alla lista di identificazione, può individuare il codice identificativo di ciascun interessato), al promotore.

Rispetto alle richieste di esercizio dei diritti dell'interessato, la Fondazione si è dotata di una Procedura sull'esercizio dei diritti dell'interessato ai sensi del Regolamento (cfr. all. 3), che prevede misure semplici e adeguate per garantire all'interessato, gratuitamente, l'esercizio dei diritti di cui agli artt. da 15 a 22 del GDPR, previa verifica della identità dell'interessato-richiedente o della validità della rappresentanza da parte di un terzo-richiedente, per l'esercizio degli stessi.

In particolare, la procedura prevede, in caso di istanza di accesso ex art. 15 GDPR, la possibilità per l'interessato che lo richieda di avere una copia dei dati personali oggetto di trattamento anche in un formato elettronico di uso comune. Per quanto concerne le richieste di rettifica e/o di cancellazione ex artt. 16 e 17 GDPR, è previsto che le eventuali modifiche richieste vadano annotate e registrate, a cura dello sperimentatore, a margine dei dati originari della ricerca senza modificare questi ultimi, in quanto la modifica dei dati originari può avere effetti significativi sui risultati dello studio. Infine, relativamente alla conduzione di studi clinici, l'interessato ha il diritto di esercitare in ogni momento la revoca del consenso ex art. 7 GDPR – se il trattamento si basa su tale presupposto di liceità - senza fornire alcuna giustificazione, nonché di opporsi al trattamento ai sensi dell'art. 21 del GDPR, per motivi legati alla sua condizione personale.

La procedura, in conformità alla normativa di settore, prevede che i campioni biologici riconducibili all'interessato vengano distrutti e non debbano essere raccolti ulteriori dati che lo riguardano, ferma restando l'utilizzazione di quelli eventualmente già raccolti per determinare, senza alterarli, i risultati della ricerca.

Nella procedura, infine, sono previste misure per comunicare all'interessato i destinatari cui sono stati trasmessi i dati personali e, qualora lo richieda, per trasmettere direttamente i dati personali a un altro titolare del trattamento in un formato interoperabile ex art. 18 del GDPR.

5.7 RESPONSABILI DEL TRATTAMENTO

La Fondazione ha adottato un'efficace misura relativa alla scelta dei responsabili del trattamento a cui deciderà di ricorrere nell'ambito dello studio clinico, volta a verificare la loro adeguatezza.

Si tratta di una *check list* (cfr. all. 5) da somministrare, in fase precontrattuale, ai soggetti designati quali responsabili del trattamento, che rappresenta un valido strumento per verificare che tali soggetti esterni che collaborano alla ricerca clinica - es. nell'esecuzione delle varie attività di monitoraggio e/o di analisi e/o di elaborazione dei dati - risultino adeguate, ossia conformi rispetto agli aspetti più rilevanti della disciplina in materia di protezione dei dati personali anche relativamente alla formazione e all'adeguatezza del proprio personale.

Inoltre, la Fondazione ha adottato un modello di accordo sul trattamento dei dati personali ex art. 28 del GDPR basato sulle Clausole contrattuali tipo per la designazione dei responsabili del trattamento a norma dell'art. 28, par. 7 del GDPR adottate il 4 giugno 2021 dalla Commissione europea con la decisione di esecuzione (UE) 2021/915 per regolamentare la relazione fra titolare e responsabile del trattamento, disponibile anche in formato elettronico.

L'accordo disciplina tassativamente le materie di cui all'art. 28.3 del GDPR e, in particolare, sono previsti una serie di obblighi in capo ai responsabili del trattamento affinché questi non operino solo

su istruzione del titolare, ma attuino anche una serie di misure tecniche e organizzative al fine di trattare i dati lecitamente, in conformità al Regolamento, coadiuvando il titolare del trattamento nell'esecuzione degli obblighi ad essi attribuiti, soprattutto relativamente alla procedura di valutazione di impatto, alla notificazione delle violazioni di dati personali e all'esercizio dei diritti dell'interessato ex artt. 15 e ss. GDPR.

In primis, contrattualmente, è previsto che il responsabile del trattamento dei dati si impegni a garantire la riservatezza del proprio personale autorizzato al trattamento e adotti tutte le misure richieste dall'art. 32 del GDPR tese ad assicurare un livello di sicurezza adeguato al rischio del trattamento. Ulteriori elementi stabiliti nell'accordo attengono all'obbligo del responsabile di restituire al titolare o cancellare tutti i dati personali eliminandone anche le copie esistenti e alla messa a disposizione del titolare, da parte del responsabile, di tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del GDPR.

Nell'accordo è stato pattuito, inoltre, che il responsabile del trattamento e gli eventuali sub-responsabili attuino misure adeguate a informare il titolare qualora ritengano che una istruzione da questi impartita violi il Regolamento o altre disposizioni nazionali o dell'Unione in materia di trattamento dei dati personali. Le disposizioni contrattuali prevedono altresì che, qualora il responsabile del trattamento determini le finalità e i mezzi del trattamento, sarà considerato alla stregua di un titolare del trattamento e potrà incorrere nel regime sanzionatorio previsto dal GDPR.

L'accordo prevede, conformemente all'art. 28 del GDPR, un'autorizzazione preventiva e scritta generale al responsabile del trattamento per ricorrere a sub-responsabili, a condizione che la designazione del secondo responsabile contenga tutti gli elementi obbligatori ex art. 28.3 del GDPR. È inoltre stabilito che il responsabile del trattamento sia tenuto ad informare il titolare di eventuali modifiche relative all'aggiunta o alla sostituzione di altri responsabili del trattamento, in modo da consentire al titolare, se del caso, di opporsi a tali modifiche.

*

6 FASE 4: ANALISI, INDIVIDUAZIONE E GESTIONE DEI RISCHI

6.1 PREMESSA

Attraverso l'analisi della documentazione generata nella fase progettuale, si è proceduto alla individuazione e alla valutazione scritta dei rischi, patologici e fisiologici, per i diritti e le libertà degli interessati e dei terzi derivanti dal trattamento in oggetto.

Il rischio si configura come uno scostamento da quanto atteso ed è caratterizzato dal presentarsi di un evento che ha potenziali conseguenze. Il rischio, pertanto, è espresso in termini di combinazione dell'impatto di un evento e della verosimiglianza del suo verificarsi.

L'identificazione dei rischi si è estrinsecata tramite un processo di ricerca, individuazione e descrizione dei rischi, che ha coinvolto l'esame di dati storici, analisi teoriche, opinioni basate su conoscenze precise e pareri di esperti. Una volta analizzate le fonti del rischio, elementi che possiedono il potenziale intrinseco di originare il rischio, e, di conseguenza, identificati i rischi, si è passati alla loro valutazione in termini di impatto e verosimiglianza.

I rischi identificati sono stati analizzati in tre diverse fasi e, pertanto, il criterio adottato ha dato luogo ad una triplice valutazione:

a. Analisi dei rischi ***inerenti*** **(in)**, ovvero i rischi scevri dell'elemento relativo alle misure di sicurezza tecniche e organizzative;
b. Analisi dei rischi ***attuali*** **(at)**, basata sulla presenza di misure di sicurezza tecniche e organizzative che hanno la funzione di mitigare il rischio inerente;
c. Analisi dei rischi ***residuali*** **(rs)**, basata sulle raccomandazioni fornite per abbassare ulteriormente il livello di rischio.

VEROSIMIGLIANZA:

Si è stimata la percentuale di verosimiglianza che il rischio si materializzi (E), e gli si è assegnato un valore da 1 a 4 secondo la tabella che segue.

Nella terminologia della gestione del rischio, il termine verosimiglianza rappresenta la plausibilità di un accadimento ipotizzabile, non in termini meramente stocastici ma come frutto di una proiezione futuribile.

L'indice di verosimiglianza, nonostante l'obiettivo sia fornire un'espressione quantitativa dell'entità del rischio, si è fondato sull'identificazione soggettiva diretta della plausibilità di accadimento, in quanto le variabili in gioco non sono trattabili ricorrendo a modelli matematici o probabilistici e si riferiscono ad eventi non stimabili statisticamente sulla base di dati appositamente acquisiti.

La verosimiglianza dell'accadimento degli eventi, pertanto, è stata stimata facendo ricorso alla valutazione dei soggetti interessati alle attività di analisi, sulla base delle esperienze accumulate nel tempo in azienda, di correlazioni dirette e indirette tra organizzazione aziendale e danno, ipotizzabili seppure non ancora riscontrate, e delle indagini svolte fra gli incaricati del trattamento sulla reazione in termini di meraviglia o stupore che un determinato evento provocherebbe al suo verificarsi.

Nella seguente tabella ad ogni valore di verosimiglianza è stato associato un livello e più definizioni o criteri di giudizio.

VEROSIMIGLIANZA (E)

Valore	Significato	Definizioni/livelli di giudizio
1	Molto inverosimile	(0%-20%) - Data l'organizzazione aziendale l'evento ipotizzato può verificarsi solo per la concomitanza di fattori poco probabili e indipendenti; - non sono noti episodi in cui l'evento ipotizzato si è già verificato; - il verificarsi dell'evento ipotizzato provocherebbe incredulità.
2	Poco verosimile	(21%-40%) - Data l'organizzazione aziendale l'evento ipotizzato può verificarsi solo in circostanze sfortunate; - sono noti solo pochi episodi in cui l'evento ipotizzato si è già verificato; - il verificarsi dell'evento ipotizzato susciterebbe una modesta sorpresa fra gli interessati.
3	Molto verosimile	(41%-80%) - Data l'organizzazione aziendale l'evento ipotizzato può verificarsi, anche se non in modo automatico o diretto; - è noto qualche episodio in cui l'evento ipotizzato si è verificato; - il verificarsi dell'evento ipotizzato susciterebbe poca sorpresa fra gli interessati.
4	Altamente verosimile	(81%-100%) Esiste correlazione diretta fra l'organizzazione aziendale ed il verificarsi dell'evento; - si sono già verificati spesso eventi dello stesso tipo in azienda o in aziende simili; - il verificarsi dell'evento ipotizzato non susciterebbe alcuno stupore fra gli interessati.

IMPATTO IN CASO DI MATERIALIZZAZIONE DEL RISCHIO (I): Consiste nella portata in termini di effetti negativi sui diritti e sulle libertà delle persone fisiche, derivanti dal rischio qualora questo si materializzi; all'impatto è stato assegnato un valore da 1 a 4 a seconda della gravità dello stesso secondo la tabella che segue:

IMPATTO (I)

			Descrizione
1	1	Irrilevante	Gli individui potrebbero andare incontro a pochi minimi inconvenienti che saranno in grado di superare senza nessun problema (tempo sprecato per reinserire informazioni, fastidi, irritazioni di poco conto, danno economico di valore irrilevante, perdite finanziarie di valore irrilevante ecc.)
	2		
	3		
	4		
2	5	Trascurabile	Gli individui potrebbero andare incontro a significativi inconvenienti, che saranno in grado di superare malgrado alcune difficoltà (extra-costi, rifiuto di accesso a servizi business, paura, mancanza di comprensione, stress, leggeri disagi fisici, perdite finanziarie di valore trascurabile, danno economico di valore trascurabile ecc.)
	6		
	7		
	8		
3	9	Notevole	Gli individui potrebbero andare incontro a significative conseguenze, che dovrebbero essere in grado di superare sebbene con serie difficoltà (appropriazione indebita di fondi, iscrizione in centrali rischi finanziarie, danni ai beni di proprietà, perdita del lavoro, citazioni in giudizio, peggioramento della salute, privazione o limitazione di diritti, perdite finanziarie di notevole valore, danno economico di notevole valore ecc.).
	10		
	11		
	12		
4	13	Consistente	Gli individui potrebbero andare incontro a significative, o perfino irreversibili conseguenze, che potrebbero non essere in grado di superare (inabilità al lavoro, disagi psicologici e fisici a lungo termine, morte, privazione o limitazione di diritti o libertà fondamentali degli interessati, pregiudizio alla reputazione, discriminazione, furto e usurpazione di identità, danno sociale, impedito controllo sui dati personali all'interessato, perdita di riservatezza, danno economico di valore consistente, perdite finanziarie di valore consistente ecc.)..
	14		
	15		
	16		

Si sono considerate nella valutazione dell'impatto sui diritti e le libertà degli interessati le seguenti circostanze aggravanti la cui ricorrenza fa aumentare per un terzo la gravità dell'impatto anche se concorrono più circostanze.

Circostanze aggravanti:

A. trattamento di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; dati di comunicazione elettronica, i dati relativi all'ubicazione, i dati finanziari;
B. valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali
C. trattamento di dati di persone fisiche vulnerabili, come lavoratori, pazienti e in particolare minori
D. trattamento che riguarda una notevole quantità di dati personali
E. trattamento che riguarda un vasto numero di interessati (su larga scala)

Nella circostanza in cui il trattamento contemperi una delle circostanze aggravanti riportate nell'elenco precedente, il valore di rischio complessivo attuale è aumentato di 1.

Una volta determinate la verosimiglianza (E) e l'impatto (I), il livello di rischio è stato ottenuto determinando il prodotto dei due fattori

R= (E)(I)

La matrice sotto riportata evidenzia i livelli di rischio così determinati.

Impatto	4	4 Medio Basso	8 Medio Alto	12 Alto	16 Alto
	3	3 Basso	6 Medio Basso	9 Medio Alto	12 Alto
	2	2 Basso	4 Medio Basso	6 Medio Basso	8 Medio Alto
	1	1 Basso	2 Basso	3 Basso	4 Medio Basso
		1	2	3	4
		Verosimiglianza			

Dal punto di vista della gestione dei livelli di rischio, le metriche sopra evidenziate, corrispondono alle seguenti indicazioni:

RISCHIO (R)		
Valore	**Significato**	**Descrizione**
R≥12	**Alto**	Rischi inaccettabili che richiedono immediate azioni correttive
12>R≥8	**Medio Alto**	Rischi inaccettabili che richiedono azioni correttive, ma ne è consentita la gestione discrezionale in termini di priorità
8>R≥4	**Medio Basso**	Rischi accettabili, ma che richiedono un controllo periodico e sistematico dei controlli in essere
4>R	**Basso**	Rischi accettabili che richiedono un controllo periodico dell'esistenza stessa del rischio

6.2 ANALISI DEI RISCHI INDIVIDUATI PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE

Le misure di sicurezza poste a presidio della sicurezza del trattamento e funzionali a mitigare la verosimiglianza delle minacce identificate derivano dall'applicazione delle misure di sicurezza tecniche e organizzative all'interno dell'Organizzazione. Sono stati identificati n. 9 rischi, di seguito elencati:

1. Malware documentato e zero – day;
2. Intrusione dall'esterno (logica);
3. Impersonificazione/Furto d'identità;
4. Furto/perdita di dati ospitati;
5. Pubblicazione di informazioni;
6. Insider Threat;
7. Errore umano;
8. Denial of Service (DoS);
9. Man In The Middle.

Id	Minaccia per i diritti e le libertà delle persone fisiche interessate	Verosimiglianza inerente che il rischio si materializzi (E)		Impatto inerente sui diritti e le libertà fondamentali (I)	
		range 1-4	Ratio	range 1-4	Ratio
Inerente	Malware documentato e zero-day	1	Le misure di sicurezza poste in essere sono riportate all'interno del documento "Linee guida di Data Protection & Cybersecurity by Design": - Sezione I: paragrafi 2.1 (Standard internazionali relativi alla cybersecurity by design), 2.3 (Gestione dei profili autorizzativi) e 3.6.3 (Sistemi di audit log), con riferimento a quanto indicato al paragrafo 2.4 (Caratteristiche dei log), della sezione I; - Sezione II: paragrafi 2.1 (Backup e ripristino) e 3.1 (Sviluppo sicuro delle applicazioni) della sezione II; - Sezione III: controlli della tabella 4, al paragrafo 3.2 (Checklist Cybersecurity).	2	Un'infezione da malware o un exploit zero-day possono comportare una compromissione di confidenzialità, integrità e/o disponibilità dei dati presenti sui sistemi con conseguenti impatti sulle attività di ricerca. Nello specifico, l'indisponibilità dei dati comporterebbe un rallentamento, o un blocco delle attività di analisi degli stessi sulle quali la ricerca è basata. Un'eventuale compromissione in termini di riservatezza potrebbe essere causa di condivisione dei dati a soggetti non autorizzati, potenzialmente per lo svolgimento di attività illecite o che, in ogni caso, potrebbero pregiudicare gli esiti e il valore delle attività di ricerca in corso.
Risultati dell'analisi		Livello di rischio calcolato			
		2			
Inerente	Intrusione dall'esterno (logica)	2	Le misure di sicurezza poste in essere sono riportate all'interno del documento "Linee guida di Data Protection & Cybersecurity by Design": - Sezione I: paragrafi 2.1 (Standard internazionali relativi alla cybersecurity by design), 2.2 (Autenticazione), 2.3 (gestione dei profilli autorizzativi), 2.4 (Caratteristiche dei log) in congiunzione con quanto descritto al paragrafo 3.6.3 (Sistemi di audit log) - Sezione II: paragrafo 3.1 (Sviluppo sicuro delle applicazioni) della sezione II; - Sezione III: controlli della tabella 4, al paragrafo 3.2 (Checklist Cybersecurity).	2	L'intrusione dall'esterno (logica) ai sistemi potrebbe compromettere seriamente la riservatezza, l'integrità e la disponibilità dei dati. A seguito di un'intrusione, ad esempio, i dati potrebbero essere distrutti rendendo impossibile la prosecuzione delle attività di ricerca, o alterati pregiudicando la correttezza dei risultati delle attività di analisi. I suddetti dati, inoltre, potrebbero essere diffusi in rete come conseguenza dell'esfiltrazione da parte di un attaccante.
Risultati dell'analisi		Livello di rischio calcolato			
		4			

Inerente	Impersonificazione/ Furto d'identità	1	Le misure di sicurezza poste in essere sono riportate all'interno del documento "Linee guida di Data Protection & Cybersecurity by Design": - Sezione I: paragrafi 2.1 (Standard internazionali relativi alla cybersecurity by design), 2.2 (Autenticazione) - considerando le specifiche misure dei paragrafi della sezione II: 2.3 (Adaptive authentication), 2.4 (DAC), 2.5 (ABC)-, 2.3 (Gestione dei profili autorizzativi); - Sezione III: paragrafo1.2 (Pseudonimizzazione) e controlli della tabella 4, al paragrafo 3.2 (Checklist Cybersecurity). -	2	L'impersonificazione (o il furto di identità) comporterebbero un accesso ai dati degli interessati da parte di uno o più soggetti non autorizzati. I suddetti dati potrebbero essere oggetto di manomissione con conseguente impatto sulla correttezza dei risultati delle attività di analisi e/o essere diffusi in rete dando luogo ad un'ulteriore compromissione della riservatezza.
Risultati dell'analisi		Livello di rischio calcolato			
		2			
Inerente	Furto/perdita di dati ospitati	2	Le misure di sicurezza poste in essere sono riportate all'interno del documento "Linee guida di Data Protection & Cybersecurity by Design": - Sezione I: paragrafi 2.1 (Standard internazionali relativi alla cybersecurity by design), 2.2 (Autenticazione), 2.3 (Gestione dei profili autorizzativi); - Sezione II: paragrafi 2.1 (Backup e ripristino), 3.1 (Sviluppo sicuro delle applicazioni); - Sezione III: controlli della tabella 4, al paragrafo 3.2 (Checklist Cybersecurity).	2	L'indisponibilità dei dati, a seguito di furto o perdita degli stessi, comporterebbe un rallentamento o un blocco delle attività di analisi, su cui la ricerca è basata. In caso di furto i dati potrebbero essere condivisi con uno o più soggetti non autorizzati, potenzialmente per lo svolgimento di attività illecite o che, in ogni caso, potrebbero pregiudicare gli esiti e il valore delle attività di ricerca in corso.
Risultati dell'analisi		Livello di rischio calcolato			
		4			
Inerente	Pubblicazione di informazioni	1	Le misure di sicurezza poste in essere sono riportate all'interno del documento "Linee guida di Data Protection & Cybersecurity by Design": - Sezione I: paragrafi 2.1 (Standard internazionali relativi alla cybersecurity by design), 2.3 (Gestione dei profili autorizzativi), 2.5 (Gestione e minimizzazione dei dati trattati); - Sezione III: controlli della tabella 4, al paragrafo 3.2 (Checklist Cybersecurity).	2	La pubblicazione non autorizzata dei dati comporterebbe una violazione del diritto alla riservatezza degli interessati. A seguito della pubblicazione, i suddetti dati potrebbero usati per fini illeciti e/o per lo svolgimento di attività che potrebbero pregiudicare gli esiti e/o il valore delle attività di ricerca in corso.
Risultati dell'analisi		Livello di rischio calcolato			
		2			

Inerente	Insider Threat	1	Le misure di sicurezza poste in essere sono riportate all'interno del documento "Linee guida di Data Protection & Cybersecurity by Design": - Sezione I: paragrafi 2.1 (Standard internazionali relativi alla cybersecurity by design), 2.3 (Gestione dei profili autorizzativi), 2.5 (Gestione e minimizzazione dei dati trattati), 3.6 e sottoparagrafi (Dossier sanitario – Misure di sicurezza); - Sezione II: paragrafi 2.3 (Adaprtive authentication), 2.4 (DAC), 2.5 (ABC); - Sezione III: controlli della tabella 4, al paragrafo 3.2 (Checklist Cybersecurity).	3	La minaccia di Insider Threat ha origine da soggetti interni all'organizzazione che operano in contrasto o ai danni dell'organizzazione stessa, perseguendo i propri interessi. Un soggetto interno all'organizzazione potrebbe compromettere le caratteristiche di disponibilità, integrità e riservatezza dei dati mediante la loro eliminazione, alterazione o condivisione con terzi non autorizzati.
Risultati dell'analisi		Livello di rischio calcolato			
		3			
Inerente	Errore Umano	2	Le misure di sicurezza poste in essere sono riportate all'interno del documento "Linee guida di Data Protection & Cybersecurity by Design": - Sezione I: paragrafi 2.1 (Standard internazionali relativi alla cybersecurity by design), 2.3 (Gestione dei profili autorizzativi), 2.5 (Gestione e minimizzazione dei dati trattati), 3.6 e sottoparagrafi (Dossier sanitario – Misure di sicurezza); - Sezione II: paragrafi 2.3 (Adaprtive authentication), 2.4 (DAC), 2.5 (ABC); - Sezione III: controlli della tabella 4, al paragrafo 3.2 (Checklist Cybersecurity).	2	La minaccia di Human Error ha origine da soggetti interni all'organizzazione che involontariamente compiono azioni potenzialmente dannose per l'organizzazione. Tali azioni potrebbero rendere l'organizzazione maggiormente vulnerabile ad attacchi volti a compromettere le caratteristiche di disponibilità, integrità e riservatezza dei dati mediante la loro eliminazione, alterazione o condivisione con terzi non autorizzati.
Risultati dell'analisi		Livello di rischio calcolato			
		4			
Inerente	Denial of Service (DoS)	1	Le misure di sicurezza poste in essere sono riportate all'interno del documento "Linee guida di Data Protection & Cybersecurity by Design": - Sezione I: paragrafi 2.1 (Standard internazionali relativi alla cybersecurity by design); - Sezione III: controlli della tabella 4, al paragrafo 3.2 (Checklist Cybersecurity).	2	Un attacco DoS o DDoS comporterebbe l'indisponibilità dei dati e delle applicazioni ospitati online causando un rallentamento, o un blocco dei processi e delle attività di analisi sulle quali la ricerca è basata.
Risultati dell'analisi		Livello di rischio calcolato			
		2			

Inerente	Man In The Middle	1	Le misure di sicurezza poste in essere sono riportate all'interno del documento "Linee guida di Data Protection & Cybersecurity by Design": - Sezione I: paragrafi 2.1 (Standard internazionali relativi alla cybersecurity by design); - Sezione III: paragrafi 1.1.4 (Sicurezza dei canali di comunicazione), 1.1.5 (Cifratura end-to-end), 1.1.6 (Onion Routing), controlli della tabella 4, al paragrafo 3.2 (Checklist Cybersecurity).	2	L'intercettazione delle comunicazioni per mezzo di un attacco del tipo Man-in-the-middle comporta la condivisione dei dati a uno o più soggetti non autorizzati, potenzialmente per lo svolgimento di attività illecite o che, in ogni caso, potrebbero pregiudicare gli esiti e il valore delle attività di ricerca in corso. Inoltre, le informazioni raccolte tramite tale tipologia di attacco potrebbero essere alterate, inficiando la bontà dell'attività di ricerca.
Risultati dell'analisi		Livello di rischio calcolato			
		2			

ALLEGATO A

QUESTIONARIO PER LA VALUTAZIONE DELLA NECESSITÀ DI UN DPIA	
CODICE	
DATA COMPILAZIONE	
TITOLO E DESCRIZIONE SOMMARIA DELL'APPLICATIVO/PROGETTO OGGETTO DI VALUTAZIONE	**STUDIO CLINICO AYA**
NOME E RUOLO DEL RESPONSABILE DEL PROGETTO/APPLICATIVO	
RESPONSABILE PER I SISTEMI IT DEL PROGETTO/APPLICATIVO	
DPO	

SCREENING QUESTIONS		
DOMANDE	**RISPOSTE**	**NOTE**
1) **Vengono trattati dati personali?** (N.B. per dato personale si intende: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;) - SE LA RISPOSTA ALLA PRECEDENTE DOMANDA È **SI, PROSEGUIRE CON LA** DOMANDA 2) - SE LA RISPOSTA ALLA PRECEDENTE DOMANDA È **NO: STOP** **IL PROGETTO / APPLICATIVO NON RICHIEDE UNA DPIA.**	☒ SI, indicare le finalità: SPERIMENTAZIONE CLINICA E RICERCA ☐ NO	

2) **I trattamenti del progetto/applicativo rientrano nell'elenco dei trattamenti che l'autorità di controllo ritiene sottoposti all''obbligo di DPIA ex art. 35.4?[8]** - SE LA RISPOSTA ALLA PRECEDENTE DOMANDA È **SI: STOP** **IL PROGETTO / APPLICATIVO RICHIEDE UN DPIA** **- SE** LA RISPOSTA ALLA PRECEDENTE DOMANDA È **NO, PROSEGUIRE CON LA** DOMANDA 3)	☒ SI ☐ NO	
3) **I trattamenti del progetto/applicativo rientrano nell'elenco dei trattamenti che l'autorità di controllo ritiene esenti dall''obbligo di DPIA ex art. 35.5?[9]** - SE LA RISPOSTA ALLA PRECEDENTE DOMANDA È **SI: STOP** **IL PROGETTO / APPLICATIVO NON RICHIEDE UN DPIA**	☐ SI ☒ NO	

8 ***Ex art. 35.5 del GDPR:*** *"l'autorità di controllo può redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta la valutazione d'impatto sulla protezione. L'autorità di controllo comunica tali elenchi al comitato".*

9 ***Ex art. 35.5:*** *"l'autorità di controllo può redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta la valutazione d'impatto sulla protezione. L'autorità di controllo comunica tali elenchi al comitato.*

- SE LA RISPOSTA ALLA PRECEDENTE DOMANDA È NO, **VAI ALLA** DOMANDA 4)		
4) **Solo nel caso in cui il trattamento sia effettuato ai sensi degli artt. 6.1.c) o 6.1.e) del GDPR, esiste una base giuridica o il trattamento è specificatamente previsto da una norma UE o nazione per cui sia stato già valutato l'impatto da chi l'ha emanata (es. nei consideranda, nei lavori preparatori, nello statuto dell'Università etc.)**[10] - SE SI HA RISPOSTO **SI: STOP IL PROGETTO / APPLICATIVO NON RICHIEDE UN DPIA** - SE HAI RISPOSTO NO, **PROSEGUIRE CON LA** DOMANDA 5)	☐ SI indicare qual è la base giuridica: …… ☐ NO ☒ N/A	
5) **Considerato il contesto del progetto/applicativo e le finalità indicate alla risposta 1, è già stato svolto un DPIA per trattamenti simili?** - SE LA RISPOSTA ALLA PRECEDENTE DOMANDA È **SI: STOP IL PROGETTO / APPLICATIVO NON RICHIEDE UN DPIA**	☐ SI, indicare in quale dei precedenti DPIA rientra il progetto/applicativo: ……. ……. ☒ NO	

10 Ex. art. 35.10 GDPR

- SE LA RISPOSTA ALLA PRECEDENTE DOMANDA È NO, **PROSEGUIRE CON LA** DOMANDA 6)		
QUALORA SI RISCONTRINO ALMENO DUE RISPOSTE POSITIVE ALLE DOMANDE CHE SEGUONO, L'ATTIVITÀ DI TRATTAMENTO DEI DATI PERSONALI OGGETTO DI ANALISI RICHIEDERÀ UNA VALUTAZIONE D'IMPATTO DEI DATI PERSONALI		
6) **Le operazioni di trattamento coinvolgono valutazioni o attribuzioni di punteggi?** Nota: La valutazione o l'attribuzione di punteggi, compresa l'attività di analisi e di previsione, nello specifico di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi professionali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando n. 71 e 91). Esempi relativi a quanto sopra specificato potrebbero consistere in una Banca che controlli i suoi clienti su database di gestione del credito, o in un'impresa di biotecnologie che offra test genetici direttamente ai clienti al fine di rilevare e prevedere malattie/rischi per la salute, o ancora in un'impresa che strutturi i profili comportamentali e di	☐ SI ☒ NO	

marketing basandosi sull'utilizzo o la navigazione sul proprio sito.		
7) **Le operazioni di trattamento permettono decisioni automatizzate idonee a produrre effetti giuridici o analoghi effetti significativi sui dati degli interessati?** Nota: Per decisioni automatizzate con effetti giuridici o analoghi effetti significativi si intende che il trattamento mira a prendere decisioni su soggetti interessati che producano "effetti giuridici sulla persona fisica" o che "incidano in modo analogo significativamente su dette persone fisiche" (art. 35, paragrafo 3, lett. a del GDPR). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento con scarso o assente effetto sugli individui non corrisponde a questo criterio specifico.	☐ SI ☒ NO	
8) **Le operazioni di trattamento comportano un monitoraggio sistematico?** Nota: Il monitoraggio sistematico è il trattamento effettuato per osservare, monitorare o controllare gli interessati, compresi i dati raccolti attraverso "la sorveglianza sistematica su larga scala di una	☐ SI ☒ NO	

zona accessibile al pubblico" (art. 35, paragrafo 3, lett. c) del GDPR. Questo tipo di monitoraggio è un criterio poiché i dati personali possono essere raccolti in circostanze in cui i soggetti interessati potrebbero non essere a conoscenza di chi raccoglie i propri dati e come gli stessi verranno utilizzati. Inoltre, può essere impossibile per gli individui evitare di essere soggetti a tale trattamento in spazi pubblici (o pubblicamente accessibili).		
9) **Vengono svolte operazioni di trattamento aventi ad oggetto dati "sensibili"?** Nota: I dati “sensibili" comprendono speciali categorie di dati definite all'articolo 9 del GDPR (ad esempio, informazioni sulle opinioni politiche degli individui), nonché dati personali relativi a crimini o condanne. Questo criterio include anche dati che possono essere considerati più in generale come idonei ad aumentare il possibile rischio per i diritti e le libertà degli individui, quali i dati di comunicazione elettronica, i dati di posizione, i dati finanziari (che potrebbero essere utilizzati per frodi al momento del pagamento). A questo proposito, se i dati sono già stati resi pubblici dall'interessato o da terzi, essi possono essere rilevanti. Il fatto che i dati personali siano pubblicamente	☒ SI ☐ NO	

disponibili può essere considerato come un fattore per valutare se i dati sono stati destinati ad essere ulteriormente utilizzati per determinati scopi.		
10) **L'operazione di trattamento è svolta "su larga scala"?** Note: Il GDPR non definisce cosa debba intendersi per "larga scala", anche se il considerando n. 91 fornisce alcune indicazioni. In ogni caso, devono, in particolare, essere presi in considerazione i seguenti fattori quando si deve determinare se il trattamento venga eseguito su larga scala: a. il numero di soggetti interessati, sia come numero specifico che come percentuale della popolazione rilevante; b. il volume dei dati e/o l'intervallo di diverse voci di dati nel trattamento; c. la durata o la permanenza del trattamento; **d.** l'estensione geografica del trattamento**.**	☒ SI ☐ NO	
10) **Le basi dati vengono abbinate o combinate tra loro?** Nota: Le basi dati che vengono abbinate o combinate sono, a titolo esemplificativo, quelle che derivano da due o più operazioni di trattamento di dati poste in essere per	☐ SI ☒ NO	

differenti finalità e/o da differenti titolari del trattamento, in modo da eccedere potenzialmente le ragionevoli aspettative dell'interessato.		
11) **Vengono svolte operazioni di trattamento su persone fisiche vulnerabili?** Nota: Il trattamento di questo tipo di dati può richiedere un DPIA a causa del crescente squilibrio di potere tra l'interessato e il titolare del trattamento dati, il che significa che l'individuo potrebbe non essere in grado di acconsentire o opporsi al trattamento dei propri dati. Ad esempio, spesso i dipendenti incontrano serie difficoltà per opporsi al trattamento svolto dal proprio datore di lavoro quando questo è legato alla gestione delle risorse umane. Allo stesso modo, i bambini possono essere considerati come non in grado di essere edotti e consapevoli in merito al consenso o all'opposizione al trattamento dei propri dati. Ciò riguarda anche un segmento più vulnerabile della popolazione che richiede una protezione speciale, come ad esempio i malati mentali, i richiedenti asilo, gli anziani, i pazienti o	☒ SI - Pazienti ☐ NO	

comunque soggetti rispetto ai quali sia rilevabile uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento.		
12) **Le operazioni di trattamento coinvolgono nuove soluzioni organizzative o tecnologiche?** Nota: L'uso innovativo o l'applicazione di soluzioni tecnologiche o organizzative, come l'uso combinato delle impronte digitali e del riconoscimento facciale per implementare il controllo fisico degli accessi, ecc. Il GDPR chiarisce (articolo 35, paragrafo 1 e considerando nn. 89 e 91) che l'uso di una nuova tecnologia può comportare la necessità di eseguire un DPIA. Questo perché l'utilizzo di tale nuova tecnologia può implicare nuove forme di raccolta ed utilizzo dei dati, con un elevato rischio potenziale per i diritti e le libertà degli individui. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Un DPIA aiuterà il titolare del trattamento dati a comprendere e affrontare tali rischi. Ad esempio, alcune applicazioni di "*Internet of things*" potrebbero avere un	☐ SI ☒ NO	

impatto significativo sulla vita quotidiana dei singoli individui e sulla privacy e, conseguentemente, richiedere un DPIA.		
14) **Vi è un trasferimento di dati fuori dall'Unione Europea inteso come caratteristica intrinseca del progetto e/o basato sulle deroghe di cui all'articolo 49 del GDPR?** Nota: Il titolare del trattamento dovrebbe considerare, tra l'altro, il o i paesi di destinazione previsti, nonché la possibilità di ulteriori trasferimenti o la probabilità di trasferimenti basati su deroghe per situazioni specifiche previste dal GDPR.	☐ SI ☒ NO	
15) **L'operazione di trattamento si basa unicamente sulla necessità di soddisfare un legittimo interesse del titolare del trattamento (es. videosorveglianza a tutela del patrimonio aziendale, interrogazioni database, *credit risk*)?** Nota: Ciò include trattamenti eseguiti in un'area pubblica che i passanti non possono evitare, o trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati ad un servizio o alla stipula di un contratto. Un esempio di questo genere di	☐ SI ☒ NO	

trattamenti è rinvenibile nel caso di una banca che controlli i suoi clienti grazie ad un database di gestione del credito per decidere se concedere loro un prestito.		
QUALORA NON SI RISCONTRINO ALMENO DUE RISPOSTE POSITIVE ALLE DOMANDE CHE PRECEDONO DA 6-15 PROSEGUI E VAI ALLA DOMANDA 16)		
16) Può il trattamento presentare un alto rischio per i diritti e le libertà delle persone fisiche? - SE LA RISPOSTA ALLA PRECEDENTE DOMANDA È **SI: STOP** **IL PROGETTO RICHIEDE UN DPIA** - SE LA RISPOSTA ALLA PRECEDENTE DOMANDA È NO: **STOP** **IL PROGETTO** NON RISCHIEDE UN DPIA	☒ SI ☐ NO	

QUESTIONARIO PER ANALISI CONFORMITÀ GDPR		
DOMANDE	**COMFORMITÀ**	**AZIONI RACCOMANDATE**
LICEITA' DEL TRATTAMENTO		

1) il trattamento dei dati personali si basa su una delle seguenti basi di liceità? Art. 6, par 1., lett.: a) consenso dell'interessato e, se minore di 14 anni, sul consenso autorizzato o prestato dal titolare della potestà genitoriale; b) è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) è effettuato per adempiere ad un obbligo di legge al quale il titolare è soggetto; d) è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica e solo se nessuna altra condizione di liceità può trovare applicazione[11]; e) 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;	☒ SI indicare quale: Artt. 9, par. 2, lett. j) del GDPR e 110 del Codice Privacy ☐ NO	

11 es. se è essenziale ai fini umanitari, per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione, in casi di emergenze umanitarie, di catastrofi naturali o umane etc.…

f) vi è un interesse legittimo del titolare o di terzi che prevale sui diritti e sulle libertà fondamentali dell'interessato[12]. *Solo per il trattamento di dati "particolari", ex c. 51 ed ex art 9 del GDPR, si aggiungono (oltre a quelle suddette) le ulteriori condizioni di legittimità:* Art. 9, par. 2, lett.: a) consenso esplicito dell'interessato, e se minore di 14 anni, sul consenso autorizzato o prestato dal titolare della potestà genitoriale; b) è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare in materia di diritto del lavoro, sicurezza sociale, protezione sociale, e se autorizzato dalla legge o dalla contrattazione collettiva nazionale in materia di lavoro e in presenza di garanzie adeguate per i diritti fondamentali e gli interessi dell'interessato; c) è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona in caso di incapacità fisica nel prestare il consenso;		

12 es. se l'interessato è un cliente o è alle dipendenze del titolare, o trattare i dati per finalità di marketing diretto; trasmettere i dati all'interno del gruppo imprenditoriale ai fini amministrativi interni, compreso il trattamento dei dati personali dei clienti e dei dipendenti; trattare dati relativi al traffico in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione ecc...

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) riguarda dati personali resi manifestamente pubblici dall'interessato; f) è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria[13]; g) è necessario per motivi di interesse pubblico rilevante sulla base del diritto nazionale o europeo[14]; h) è necessario ai fini della medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia		

13 o ogni volta che le autorità giurisdizionali esercitino le loro funzioni giurisdizionali

[14] es. nei settori della sanità pubblica;

sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali[15] sulla base del diritto europeo o nazionale o conformemente al contratto con un professionista della sanità; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) 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.		

[15] conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al par. 3 del c. 53 del GDPR.

TRASFERIMENTO EXTRA UE		
2) Il trasferimento extra UE avviene in presenza di una di queste basi di legittimità? a) Adeguatezza del paese terzo riconosciuta tramite decisione della Commissione Europea; b) In assenza di decisioni di adeguatezza della Commissione, **garanzie adeguate** di natura contrattuale o pattizia quali: 1. clausole contrattuali tipo approvate dalla (cd. *standard model clauses*) adottate dalla Commissione; 2. norme vincolanti d'impresa (cd. BCR)	☐ SI indicare quale ☐ NO ☒ N/A	

approvate secondo la procedura ex art. 47 del GDPR; 3. adesione a codici di condotta; 4. adesione schemi di certificazione ex art. 46 GDPR; 5. clausole tipo di protezione dei dati adottate da una autorità di controllo; 6. clausole contrattuali ad hoc autorizzate da una autorità di controllo; 7. accordi amministrativi stipulati da autorità pubbliche autorizzati da una autorità di controllo; 8. in assenza di ogni altro presupposto, sulla base di “deroghe al divieto di trasferimento applicabili in specifiche situazioni” quali: a) consenso esplicito dell’interessato; b) il trasferimento è necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;		

c) il trasferimento è necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato; d) il trasferimento è necessario per importanti motivi di interesse pubblico; e) il trasferimento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; f) il trasferimento è necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; g) il trasferimento è effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.		

h) solo in via residuale, se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali.		
PRINCIPIO DI MINIMIZZAZIONE DEI DATI		
3) Sono predisposti strumenti e procedure nonché sviluppate tecnologie e processi idonei a garantire la minimizzazione dei dati ex art. 5.1.c GDPR by design e by default?	☒ SI Pseudonimizzazione ☐ NO	
PRINCIPIO DI LIMITAZIONE DELLE FINALITÀ		
4) I dati vengono raccolti per finalità legittime, determinate (ossia chiare ed univoche) ed esplicite (ossia comunicate chiaramente all'interessato affinché sia in grado di conoscere le specifiche finalità); saranno successivamente trattarli in	☒ SI ☐ NO	

modo compatibile con le finalità per cui sono stati raccolti?		
PRINCIPIO DI LIMITAZIONE DELLA CONSERVAZIONE		
5) Sono predisposti strumenti e/o procedure idonee a garantire la limitazione della conservazione dei dati non superiore al conseguimento delle finalità per cui sono stati trattati ex art. 5.1.e?	☒ SI ☐ NO	
DIRITTI DELL'INTERESSATO		
6) È fornita all'interessato una Informativa coi contenuti minimi ex art. 13.1 e 13.2?	☒ SI ☐ NO	
7) È fornita all'interessato una Informativa coi contenuti minimi ex art 14.1 e 14.2 e secondo i criteri ex art. 14.3?	☒ SI ☐ NO	

8) Sono state adottate misure per la fornitura di informazioni ex art. 13 e/o 14 per iscritto o con mezzi elettronici per una finalità diversa da quella per cui essi sono stati raccolti?	☒ SI ☐ NO	
9) Sono adottate misure per garantire la verifica dell'identità o la validità della rappresentanza da parte di un terzo, per l'esercizio dei diritti?	☒ SI ☐ NO	
10) Sono state adottate misure semplici e gratuite per l'esercizio dei diritti?	☒ SI ☐ NO	
11) Sono adottate misure volte a confermare all'interessato se sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, fornirgli l'accesso ai dati e alle seguenti informazioni di cui all'art.15? Sono adottate misure volte a fornire una copia dei dati personali oggetto di trattamento? Sono adottate misure volte a fornire all'interessato le informazioni ex art. 15 in un formato elettronico di uso comune?	☒ SI Quali misure? L'azienda ha adottato una Procedura per l'esercizio dei diritti degli interessati (cfr. all. 4) che soddisfa il requisito ☐ NO	
12) Sono adottate misure volte a rettificare/integrare i dati personali dell'interessato?	☒ SI Quali misure?	

	L'azienda ha adottato una Procedura per l'esercizio dei diritti degli interessati (cfr. all. 4) che soddisfa il requisito ☐ NO	
13) Sono adottate misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali, se ha reso pubblici dati personali, ed ha l'obbligo di cancellare i dati ex art. 17.1.?	☒ SI Quali misure? L'azienda ha adottato una Procedura per l'esercizio dei diritti degli interessati (cfr. all. 4) che soddisfa il requisito ☐ NO	
14) Sono adottate misure idonee a limitare il dato?	☒ SI Quali misure? ☐ NO	
15) Sono adottate misure da parte del titolare per la fornitura all' interessato prima che la limitazione sia revocata, dell'informazione che ha ottenuto la	☒ SI Quali misure? L'azienda ha adottato una Procedura per l'esercizio	

limitazione del trattamento a norma dell'art.18.1?	dei diritti degli interessati (cfr. all. 4) che soddisfa il requisito ☐ NO	
16) Sono adottate misure per informare a ciascun destinatario cui sono trasmessi i dati delle rettifiche, cancellazioni o limitazioni sugli stessi?	☒ SI Quali misure? L'azienda ha adottato una Procedura per l'esercizio dei diritti degli interessati (cfr. all. 4) che soddisfa il requisito ☐ NO	
17) Sono adottate misure per comunicare all'interessato i destinatari cui sono stati trasmessi i dati personali qualora lo richieda? Sono adottate misure necessarie per trasmettere direttamente i dati personali a un altro titolare del trattamento?	☒ SI Quali misure? L'azienda ha adottato una Procedura per l'esercizio dei diritti degli interessati (cfr. all. 4) che soddisfa il requisito ☐ NO	
	☒ SI	

18) Sono adottate misure tecniche necessarie a produrre i dati richiesti in un formato interoperabile	☐ NO	
19) Sono adottate misure per consentire all'interessato di esercitare il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano ai sensi dell'art. 6.1 e); 6.1 f), compresa la profilazione sulla base di tali disposizioni?	☒ SI Quali misure? L'azienda ha adottato una Procedura per l'esercizio dei diritti degli interessati (cfr. all. 4) che soddisfa il requisito ☐ NO	
20) Sono adottate misure per consentire all'interessato di esercitare il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano trattati per finalità di marketing diretto, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto?	☐ SI ☐ NO ☒ N/A	
21) Sono adottate misure per astenersi dal trattamento dei dati qualora l'interessato si opponga al trattamento?	☒ SI Quali misure? L'azienda ha adottato una Procedura per l'esercizio dei diritti degli interessati (cfr. all. 4) che soddisfa il requisito	

	☐ NO	
22) Sono adottate misure per informare l'interessato dei diritti di cui all'art. 21.1 e 21.2?	☐ SI Quali misure? L'azienda ha adottato una Procedura per l'esercizio dei diritti degli interessati (cfr. all. 4) e un modello di informativa ex art. 13 GDPR che soddisfano il requisito (cfr. all. 2) ☐ NO ☒ N/A	
23) Sono adottate misure per consentire all'interessato di esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche?	☒ SI ☐ NO	
24) Sono adottate misure, qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89.1, per consentire all'interessato, per motivi connessi alla sua situazione particolare, di opporsi al trattamento di dati personali che lo riguardano?	☒ SI ☐ NO ☐ N/A Quali misure? L'azienda ha adottato una Procedura per l'esercizio dei diritti degli interessati	

	(cfr. all. 4) e un modello di informativa ex art. 13 GDPR (cfr. all. 2) che soddisfano il requisito	
25) Nel caso in cui, ex art. 22.2, lettere a) e c), si adottino decisioni basate unicamente sul trattamento automatizzato compresa la profilazione, che produca effetti giuridici sull'interessato o che incida significativamente sulla sua persona, sono adottate misure per tutelare i diritti le libertà e i legittimi interessi dell'interessato, tra cui almeno la possibilità di ottenere l'intervento umano da parte del titolare, di far esprimere la opinione all'interessato e di consentirgli di contestare la decisione? Sono adottate ulteriori misure di cautela per le decisioni ex art. 22.2 basate su categorie particolari di dati personali di cui all'articolo 9.1?	☐ SI ☐ NO ☒ N/A quali misure_____	
26) Sono adottate misure per consentire all'interessato di revocare in ogni momento il consenso con la stessa facilità con cui è accordato?	☒ SI Quali misure? L'azienda ha adottato una Procedura per l'esercizio dei diritti degli interessati (cfr. all. 4) e un modello di informativa ex art. 13	

	GDPR (cfr. all. 2) che soddisfano il requisito ☐ NO	
27) I dati personali si conservano in una forma tale da facilitare in maniera rapida l'esercizio dei diritti?	☒ SI ☐ NO	
RESPONSABILI DEL TRATTAMENTO		
28) Sono adottate misure, che nella scelta dei responsabili del trattamento cui ricorrere, siano volte a verificare la loro adeguatezza?	☒ SI Quali? L'azienda ha adottato una check list da somministrare in fase precontrattuale al fine di verificare l'adeguatezza dei provider (Cfr. all. 5) ☐ NO	
29) Si disciplina la relazione tra il titolare e il responsabile a mezzo di un contratto o per altro atto giuridico in forma scritta, anche in formato elettronico, che disciplini tassativamente almeno le materie di cui all'art. 28.3?	☒ SI ☐ NO	

30) Si è stabilito contrattualmente l'autorizzazione preventiva e scritta specifica o generale al responsabile per ricorrere a sub-responsabile che contenga elementi obbligatori ex art 28.3?	☒ SI ☐ NO	
31) Si è stabilito contrattualmente che, in caso di autorizzazione generale, il responsabile deve informare preventivamente il titolare della sostituzione o aggiunta di sub-responsabili;	☒ SI ☐ NO	
32) Si è stabilito contrattualmente che il responsabile e il sub-responsabile potranno trattare i dati solo in maniera conforme all'istruzione documentata impartita dal titolare?	☒ SI ☐ NO	
33) Si è stabilito contrattualmente che il responsabile e il sub-responsabile, adottino delle misure adeguate, in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, per informare il titolare circa l'obbligo di dare istruzione documentata prima del trattamento?	☒ SI ☐ NO	

34) Si è stabilito contrattualmente che il responsabile e il sub-responsabile, adottino delle misure adeguate per vincolare i propri incaricati alla riservatezza?	☒ SI ☐ NO	
35) Si è stabilito contrattualmente che il responsabile e il sub-responsabile, adottino delle misure adeguate richieste ai sensi dell'articolo 32?	☒ SI ☐ NO	
36) Si è stabilito contrattualmente che il responsabile e il sub-responsabile, adottino delle misure adeguate per rispettare le condizioni di cui all'art. 28.1 e 28.4 nel ricorrere a un sub-responsabile del trattamento	☒ SI ☐ NO	
37) Si stabilisce contrattualmente che il responsabile e il sub-responsabile non comunicheranno i dati oggetto di trattamento a nessun'altra persona né li diffonderanno?	☒ SI ☐ NO	
38) Si è stabilito contrattualmente che il responsabile e il sub-responsabile, adottino delle misure adeguate per assistere il titolare nel dare seguito alle richieste per l'esercizio dei diritti	☒ SI ☐ NO	

dell'interessato di cui al capo III (ex artt. da 12-23)?		
39) Si è stabilito contrattualmente che il responsabile e il sub-responsabile, adottino delle misure adeguate per assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36.?	☒ SI ☐ NO	
40) Si è stabilito contrattualmente che al termine della prestazione di servizi relativi al trattamento, su scelta del titolare, il responsabile cancelli o gli restituisca tutti i dati personali e cancelli le copie esistenti?	☒ SI ☐ NO	
41) Si è stabilito contrattualmente che il responsabile e il sub-responsabileadottino delle misure adeguate per cancellare o restituire al Titolare, tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti?	☒ SI ☐ NO	
42) Si è stabilito contrattualmente che il responsabile e il sub-responsabile, adottino delle misure adeguate per mettere a disposizione del titolare del trattamento tutte le informazioni	☒ SI ☐ NO	

necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28?		
43) Si è stabilito contrattualmente che il responsabile e il sub-responsabile, adottino delle misure adeguate per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato?	☒ SI ☐ NO	
44) Si è stabilito contrattualmente che il responsabile e il sub-responsabile, adottino delle misure adeguate per fornire informazione al titolare qualora ritengano che una istruzione da questi impartita violi il regolamento UE 2016/679 o altre disposizioni nazionali o dell'Unione in materia?	☒ SI ☐ NO	
45) Si è stabilito contrattualmente che il responsabile e il sub-responsabile, adottino delle misure adeguate per la verifica del rispetto degli obblighi di cui all'art. 28 e cooperazione alle attività di revisione, comprese le ispezioni?	☒ SI ☐ NO	
46) Si informa il responsabile che, qualora violi il GDPR determinando le finalità e i mezzi del trattamento, è considerato	☒ SI ☐ NO	

titolare del trattamento in questione e potrà incorrere nel regime sanzionatorio del GDPR?		

7 ALLEGATI

1. Modulo di consenso informato ICF;
2. Informativa sul trattamento dei dati personali ex art. 13 del GDPR;
3. Procedura sull'esercizio dei diritti dell'interessato ai sensi del Regolamento (UE) 679/2016;
4. Check list provider (se applicabile);