



Fondazione IRCCS
Istituto Nazionale dei Tumori

Sistema Socio Sanitario



Regione
Lombardia

Con il patrocinio del



GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI



Ministero della Salute

IL COINVOLGIMENTO DEL RESPONSABILE PROTEZIONE DATI – RPD (DATA PROTECTION OFFICER – DPO)

23 giugno 2023

LA CIRCOLAZIONE DEI DATI PERSONALI IN MODO SICURO PER L'INTERESSATO (Regolamento UE 679/2016)

C 1 - La protezione delle **persone fisiche** con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale.

C 4 – Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il **diritto** alla protezione dei dati personali non è una prerogativa assoluta, ma va considerata alla luce della sua funzione sociale e va temperato con altri diritti fondamentali, in ossequio al principio di proporzionalità.

C 7 – Tale evoluzione [*tecnologica, che consente alle imprese private e alle autorità pubbliche di utilizzare dati personali come mai in precedenza*], richiede un quadro solido e coerente in materia di protezione dei dati nell'Unione, affiancata da efficaci misure di attuazione, data l'importanza di creare un **clima di fiducia** (...).

C 10 – Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e di rimuovere gli ostacoli alla circolazione dei dati personali, il livello di protezione **dovrebbe essere equivalente** in tutti gli Stati membri.



Il Titolare del trattamento dei dati per finalità di ricerca, medica, biomedica ed epidemiologica
agisce per condividere le informazioni sanitarie, prezioso frammento della vita più personale e intima di ciascuno, tutelando gli assistiti da «indebite ingerenze e strumentalizzazioni».

La certezza giuridica e operativa per la tutela delle persone fisiche in merito ai dati personali necessita di essere contestualizzata tramite le conoscenze specialistiche e qualità professionali del DPO.

La struttura organizzativa INT per la protezione dei dati

DPO (art. 37,38 e 39 GDPR)
Interno, con tem di competenze specialistiche

CONSULENZA E SORVEGLIANZA

Informa e vigila sul rispetto delle norme
Fornisce pareri sulla valutazione di impatto.
Coopera con l'Autorità di controllo.

«Cerniera tra Titolare, Garante, Interessati»

TITOLARE
(art. 4 GDPR)

Determina le finalità e i mezzi del trattamento di dati personali.

La Titolarità della Fondazione è esercitata dal Direttore Generale, che è competente, comprovandolo, per il rispetto dei principi applicabili al trattamento e per le attribuzioni previste dal GDPR.

Ha designato (17 aprile 2017) il DPO, assicurandogli indipendenza, risorse e formazione continua.

RESPONSABILE
(art. 28 GDPR)

«Fornitore» esterno, nominato dal titolare per trattare i dati «in suo conto», sulla base di garanzie sufficienti alla protezione dei dati personali.

DESIGNATI DEL TITOLARE
(art. 2 quaterdecies CODICE)

La Determinazione 79/DG del 28/02/2019 designa i livello organizzativi Direzionale Strategici e di struttura quali «Delegati al trattamento», per il rispetto dei principi e la sorveglianza del rispetto del GDPR, nell'ambito delle attribuzioni da normativa di settore, nonché Statuto e POAS INT

PERSONE AUTORIZZATE
(art 29 GDPR)

Il personale della Fondazione, formalmente nominato e istruito all'accesso; soggetto sia alla formazione generale sulla protezione dei dati entro il primo anno di attività, che a quella specifica laddove rilevato il fabbisogno.
Altri soggetti che, temporaneamente, operano sotto l'autorità del titolare, formalmente nominati e istruiti.

«Il Titolare si assicura che il DPO sia tempestivamente e adeguatamente coinvolto nelle questioni sulla protezione dei dati»,
art 38. GDPR

- Direttore/Responsabile di struttura, cui afferisce il progetto di ricerca, disegna la protezione dei dati sin dalla progettazione del trattamento (sin dal disegno dello studio) – art. 25 GDPR
- Descrive il trattamento, in base a criteri predefiniti, nel registro del Titolare - art. 30 GDPR
- Valuta *[il rischio e]* l'impatto del trattamento sulla protezione dei dati, consultandosi con il DPO
- Comunica al DG e al DPO eventi sospetti di violazione da perdita di riservatezza, integrità e disponibilità dei dati personali

- Disamina di questioni privacy emergenti negli studi multicentrici (ruoli privacy, base di liceità, garanzie di sicurezza)
- Policy e format condivisi



- Direzione Scientifica e sue articolazioni competenti per le regole generali di sottomissione e gestione degli studi nel sistema qualità
- Strutture «contraenti», competenti per le soggettività privacy e il trasferimento di dati Extra-UE
- Sistemi informativi, competenti per la sicurezza informatica e la minimizzazione dei dati nelle soluzioni tecnologiche informatiche.
- URP, punto di primo contatto degli interessati per la richiesta di esercizio dei diritti e per i bisogni di informazione

- P.I., Co-ricercatori, Data manager competenti nel rispetto delle misure di sicurezza definite nei documenti di progetto
- Esperti legali acquisiti per i WP «*legal, etical e privacy*» dei progetti, competenti nelle interazioni con il DPO

Le «questioni privacy» che coinvolgono il DPO

- Le Parti che realizzano la ricerca possono avere più ruoli privacy, in base ai trattamenti previsti nello studio
- I soggetti giuridici non sono chiaramente nominati nello studio
- Le basi giuridiche di liceità possono essere diverse per le Parti

CONVERSIONE DEI
RUOLI E ATTRIBUZIONI
SCIENTIFICHE IN RUOLI
E ATTRIBUZIONI
PRIVACY

IDENTIFICABILITÀ
DELL'INTERESSATO

- Gli effetti delle tecniche di pseudonimizzazione o di anonimizzazione sono da verificare
- La qualificazione giuridica di dato personale necessita di essere contestualizzata

DPO

CONSULENZA, FORMAZIONE,
MONITORAGGIO

PROGETTO CON
WORK PACKAGE/
WORK GROUP
«LEGAL»

MISURE TECNICHE E
ORGANIZZATIVE
ADEGUATE ALLA
PROTEZIONE DEI
DATI

- Stato di avanzamento dei lavori
- Contributo per la normativa nazionale

- Corretto utilizzo dei framework di valutazione del rischio e della mitigazione data dalle misure di sicurezza.
- Condivisione del metodo di validazione delle misure.

IL «TOOL KIT» DISPONIBILE PER LA RICERCA

- FAD «IL SISTEMA PRIVACY PER FINALITÀ DI CURA E DI RICERCA NELLA FONDAZIONE IRCCS INT»
- NEWSLETTER Privacy e INFORMATIVE DPO , ai sensi dell'art 39, comma 1, lett. a)

Sistema Socio Sanitario

Fondazione IRCCS Istituto Nazionale dei Tumori

Regione Lombardia

LICEITÀ DEL TRATTAMENTO DEI DATI PERSONALI NEGLI STUDI CON DISEGNO RETROSPETTIVO e impossibilità ad informare e ottenere il consenso dell'interessato al trattamento dei dati personali (informazione e consulenza de DPO al titolare e delegati del titolare, ai sensi dell'art. 39 del GDPR)

- Valutazione d'impatto (DPIA) (framework CNIL)

FORMAZIONE
E
INFORMAZIONE

PROCEDURE
E
FORMAT

DPO

CONSULENZA, FORMAZIONE,
MONITORAGGIO

PIATTAFORMA
GESTIONALE/2

PIATTAFORMA
GESTIONALE/1

CYBERSECURITY

- Procedure di sottomissione degli studi scientifici
 - Format per l'informativa e il consenso al trattamento dei dati personale
 - Format per la dichiarazione di impossibilità a informare e ottenere il consenso degli interessati
 - Format per la nomina di responsabile del trattamento ex art. 28
- Riferimenti per le condizioni del trasferimento dei dati personali extra- UE

- Registro dei trattamenti

ANNA MARIA TERESA ROLI
Amministratore
Delegato del Titolare
Autorizzato
DPO

DASHBOARD

REG. TRATTAMENTI

VALUTAZIONE D'IMPATTO

ASSEGNAZIONI

ACCORDI

INFORMATIVE

DOCUMENTI

DATA BREACH

76 - Valutazione d'impatto PNRR-MAD-2022-12376508

[Torna alla lista](#)

Dati essenziali ?

Indicare il nome del progetto di valutazione di impatto ed il trattamento a cui esso si riferisce.

Nome

Valutazione d'impatto PNRR-MAD-2022-12376508

Reporter

CESARE FATTORI

- CREAZIONE PROGETTO
- STIMA DEL RISCHIO E PRE-ASSESSMENT
- VALUTAZIONE PROPORZIONALITÀ
- DIRITTI E PRINCIPI FONDAMENTALI
- COMPONENTI DEL TRATTAMENTO
- VALUTAZIONE DEL RISCHIO
- GIUDIZIO DI SINTESI
- CONTROLLO E MANUTENZIONE

ANNA MARIA TERESA ROLI
Amministratore
Delegato del Titolare
Autorizzato
DPO

DASHBOARD

REG. TRATTAMENTI

VALUTAZIONE D'IMPATTO

ASSEGNAZIONI

ACCORDI

INFORMATIVE

DOCUMENTI

DATA BREACH

RICHIESTE INTERESSATI

Registro dei Trattamenti

In questa sezione vengono mantenuti in formato elettronico i registri delle attività di trattamento effettuati come titolare o come responsabile. È possibile, tramite gli appositi bottoni, creare o modificare trattamenti, filtrare i registri, generarli in formato documentale, esportarli in fogli di calcolo.

[Pagina di documentazione](#)

✓	02/09/2022	116	PUBBLICATO	STUDIO INT 189/15	sull'inibitore di EZH2 tazemetostat in soggetti adulti affetti da tumori INI1-negativi o sarcoma sinoviale recidivato/refrattario"; PRESSO la s.c. Oncologia Medica2 Mesenchimali [...]	Nessuna unità	ELEVAT
---	------------	-----	------------	-------------------	---	---------------	--------

Visualizzati da 1 a 25 di 114 | Mostra: [Ricarica](#)

116 - STUDIO INT 189/15

Il trattamento appartiene al Registro del Titolare

Data di creazione: 2 settembre 2022 15:55

Data dell'ultima modifica: 3 febbraio 2023 17:54

Percentuale di completamento

100%

Dati essenziali

Soggetti

Trasferimenti e comunicazione

Misure di sicurezza

Altre informazioni

Stima del rischio e pre assessment

Unità associate

Valutazione d'impatto (DPIA) nella ricerca

In base alla complessità del progetto possono essere necessario integrare più framework e/ documentare tare misure

FRAMEWORK CNIL

Stima del rischio e preassessment

Valutazione proporzionalità

Diritti e principi fondamentali

Componenti del trattamento

Valutazione del rischio

Giudizio di sintesi

Controllo e manutenzione

FRAMEWORK ENISA

Id.	Categorie delle misure
A.1	Politica di sicurezza e procedure per la protezione dei dati personali
B.1	Ruoli e responsabilità
C.1	Politica di controllo degli accessi
D.1	Gestione risorse/asset
E.1	Gestione delle modifiche
F.1	Responsabili del trattamento
G.1	Gestione degli incidenti / Personal data breaches
H.1	Continuità operativa
I.1	Obblighi di riservatezza imposti al personale
J.1	Formazione
K.1	Controllo degli accessi e autenticazione
L.1	Generazione di file di log e monitoraggio
M.1	Sicurezza di Server e Database
N.1	Sicurezza delle Postazioni di lavoro
O.1	Sicurezza della rete e delle Infrastrutture di comunicazione elettronica
P.1	Backup
Q.1	Dispositivi mobili / portatili
R.1	Sicurezza del ciclo di vita delle applicazioni
S.1	Cancellazione / eliminazione dei dati
T.1	Sicurezza fisica

Altre misure – es. re-identificazione

Esistono informazioni per identificare i soggetti?

Queste informazioni sono pubbliche?

Il soggetto che dispone del database originario è lo stesso che tratta i dati pseudonimizzati?

Senza la tabella di decodifica, potrebbe ragionevolmente invertire il processo e identificare gli interessati?

Quali azioni dovrebbe compiere il terzo per tentare di identificare gli interessati?

Le misure di sicurezza per evitare la re-identificazione sono adeguate

RIFLESSIONI FINALI

Il comportamento dei professionisti sanitari, nella cura come nella ricerca, è già improntato alla tutela della persona, in base ai codici di deontologia professionale e alle carte dei diritti dell'uomo e del malato, prevenendo rischi di danni materiali e immateriali

La protezione dei dati personali integra questa competenza professionale con principi giuridici sulla tutela delle persone per i rischi di danno materiale e immateriale

Il senso dell'operato del DPO è quello di consolidare questo spazio di fiducia, di alleanza, tra l'istituzione e i cittadini ai quali si rivolge