DPIA
ex art. 35 GDPR

INDICE

Il contesto normativo del *Data Protection Impact Assessment* 3

Data Protection Impact Assessment (DPIA) 9

A) Contesto 9

B) Misure di sicurezza 12

B.1) Misure di sicurezza organizzative 12

B.2) Misure di sicurezza tecniche 13

C) DPIA 15

C.1) Accesso illegittimo 15

C.2) Modifica indesiderata 17

C.3) Perdita accidentale 18

Grafico DPIA 19

IL CONTESTO NORMATIVO DEL DATA PROTECTION IMPACT ASSESSMENT

Il *Data Protection Impact Assessment* (per brevità anche DPIA) è uno strumento fondamentale in termini di responsabilizzazione *(principio di accountability),* ai sensi dell'art. 5, par. 2 del Regolamento UE 2016/679 (d'ora in avanti anche "**GDPR**") in quanto sostiene il Titolare del trattamento non soltanto nel rispettare e far rispettare le prescrizioni del GDPR, ma anche nel dimostrare di aver adottato le misure idonee a mitigare il rischio durante tutte le fasi trattamentali. In altri termini, la Valutazione d'Impatto sulla Protezione dei Dati è una procedura di *risk management* che permette di dimostrare la conformità con le norme in materia di protezione dei dati personali europee e domestiche. Muovendo i passi dal dettato normativo, segue il testo dell'art. 35 GDPR:

"ART. 35

Valutazione d'impatto sulla protezione dei dati

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi."

La disciplina sulla *DPIA,* contenuta nel GDPR, deve essere integrata anche da quanto specificato dal *WP29* (oggi *European Data Protection Board* - EDPB) nelle linee guida concernenti la valutazione di impatto sulla protezione dei dati, nonché i criteri per stabilire se un trattamento possa o meno presentare un rischio privacy più o meno elevato.

In particolare, le linee guida citate ampliano l'obbligatorietà della valutazione di impatto, oltre ai casi espressamente indicati dal regolamento all´art. 35, par. 3 GDPR, anche a quelli

che comportano la comunicazione di dati su larga scala tra diversi titolari e/o trattamenti sistematici di dati genetici o sanitari, tenendo conto del volume dei dati, della durata e dell'attività di trattamento.

Il presente documento è, inoltre, uno strumento dedicato alla valutazione del rischio ed ha lo scopo di fornire informazioni basate sia su evidenze che su metodi di analisi, al fine di rendere agevole l'adozione di decisioni informate circa il trattamento di particolari rischi.
Le informazioni ottenute consentono, quindi, di identificare i fattori determinanti, gli eventi potenzialmente dannosi e suggerire le azioni correttive possibili da mettere in atto per prevenire la ripetizione degli eventi stessi.
Nella prospettiva della gestione del rischio privacy, tale documento risponde al principio fondamentale di *accountability*, intesa quale dimostrazione di come il titolare del trattamento abbia posto in essere tutte le misure di sicurezza volte a tutelare i diritti e le libertà degli interessati.

La responsabilizzazione, quale obbligo di rendere conto di ciò che si fa e ciò che si fa fare, rappresenta il fulcro della nuova frontiera della privacy in quanto aspetto essenziale per l'esercizio di una corretta ed efficace *governance*.

Il Regolamento UE 2016/679 pone, altresì, la necessità di rendere conto anche dell'adozione di comportamenti proattivi, tali da "*dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR*" (artt. 23-25, in particolare, e l'intero Capo IV del GDPR).

Ne consegue, dunque, che è affidato al Titolare del trattamento dei dati il compito di decidere autonomamente le modalità, le misure di sicurezza e i limiti del trattamento stesso, nel rispetto delle disposizioni normative ed alla luce dei criteri indicati nel Regolamento UE, oltre che a quelli indicati dall'ordinamento interno (Codice Privacy - D.lgs. 196/2003, come novellato dal D.lgs. 101/2018) e rispetto alle Linee Guida e Regole Deontologiche previste dal Garante per la Protezione dei Dati Personali.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "*data protection by design and by default*" (art. 25 GDPR), ossia dalla necessità di configurare il trattamento prevedendo fin

dall'inizio e per impostazione predefinita le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento stesso e tutelare i diritti e le libertà degli interessati, tenendo conto del contesto complessivo ove il trattamento viene svolto e dei rischi connessi.

Fondamentali fra tali attività sono quelle relative al successivo criterio del rischio inerente al trattamento; quest'ultimo è da ritenersi, infatti, come il rischio capace di impattare negativamente sulle libertà e sui diritti degli interessati (considerando 75-77).

Tali criticità dovranno essere analizzate attraverso un apposito processo di valutazione (artt. 35 e 36 GDPR) tenendo conto dei rischi noti o ipotizzabili e delle misure tecniche, fisiche e organizzative che il Titolare ritiene di dover adottare per mitigare tali rischi.

In ossequio a tali criteri, il presente documento viene redatto in base alle tecniche ed alle modalità della norma ISO/IEC 31000:2018, "*Risk Management – Principles and guidelines*", che descrive in dettaglio il processo logico e sistematico che porta alla mitigazione e controllo dei rischi.

La *ratio* della scelta risiede nella necessità di conferire connotati positivi alla gestione del rischio, anche attraverso la percezione dello stesso come opportunità, mediante una lettura del pericolo quale possibilità di innovazione.

Ulteriore ed importante elemento di valutazione è il contenuto dello standard ISO/IEC 31010:2009 (*Risk Management e Risk Assessment Techniques*) ove vengono riportati i concetti della gestione dei rischi e le diverse tecniche atte alla loro valutazione nei diversi ambiti.

È, infine, doveroso adeguarsi alle disposizioni contenute nelle norme:

- ISO/IEC 29134:2017 ("*Information technology – Security techniques – Guidelines for privacy impact assessment*") che indica linee guida applicabili a tutte le tipologie di strutture, pubbliche e private, al fine di creare, organizzare ed implementare progetti GDPR *compliant*;

- ISO/IEC 27005:2018 ("*Information security risk management*") che, è in parte applicabile anche alla valutazione del rischio connesso al trattamento dei dati personali; assumono importanza determinante le appendici dedicate all'approfondimento di alcuni aspetti della gestione dei rischi e, in particolare, quella relativa al catalogo delle minacce;

- ISO/IEC 27701:2019 ("*Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines*") che fornisce requisiti e linee guida per costruire, implementare, mantenere e migliorare costantemente un PIMS (*Privacy Information Management System* o sistema di gestione delle informazioni sulla privacy), sia qualora l'organizzazione operi come titolare del Trattamento (*Data Controller*), che come Responsabile (*Data Processor*).

- ISO 31000:2018 ("Risk management -- Principles and guidelines") fornisce principi e linee guida generali per la gestione del rischio ed è applicabile a tutte le tipologie di organizzazioni. La ISO 31000 può essere applicata a qualsiasi tipo di rischio e nel corso dell'intero ciclo di vita di un'organizzazione, in merito a molteplici attività come la definizione di strategie e decisioni, operazioni, processi, funzioni, progetti, prodotti, servizi e beni.

In conclusione, il rischio può essere definito come la combinazione delle probabilità di un evento e della gravità delle sue conseguenze. Qualunque tipo di iniziativa implica potenzialmente eventi e conseguenze che rappresentano possibili benefici (elementi positivi) o minacce alla sicurezza dell'attività trattamentale posta in essere (elementi negativi).

I principali impatti sui diritti e le libertà degli interessati, qualora il rischio di accesso illegittimo, modifica indesiderata e/o perdita di dati dovesse concretizzarsi, sono rappresentati da:

- perdita del controllo dei dati personali;
- limitazione dei diritti;
- discriminazione;
- furto o usurpazione d'identità;
- frodi;
- perdite finanziarie;
- decifratura non autorizzata alla pseudonimizzazione;

- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale;
- conoscenza da parte di terzi non autorizzati;
- qualsiasi altro danno economico o sociale significativo;
- danni fisici o psicologici.

Le principali minacce che potrebbero concretizzare il rischio di accesso illegittimo, modifica indesiderata e/o perdita dei dati personali consistono in:

- danni fisici, ossia azioni offensive finalizzate a distruggere, esporre, alterare, disabilitare, sottrarre o ottenere l'accesso non autorizzato a risorse fisiche come l'infrastruttura, l'hardware o l'interconnessione. Rientrano in questa categoria atti di vandalismo, furto, sabotaggio, perdita di informazioni e attacchi massivi riguardanti qualsiasi tipo di infrastruttura, anche quella Internet;
- eventi naturali, ossia eventi che possono distruggere, danneggiare o rendere irrecuperabili risorse fisiche come l'infrastruttura, l'hardware o l'interconnessione (ad esempio fenomeni climatici, incendi, allagamenti, ecc.);
- perdita di servizi essenziali, ossia interruzioni, perdite o malfunzionamenti dei servizi accessori fondamentali per il corretto funzionamento dell'infrastruttura hardware o di interconnessione alle reti informatiche e dati (ad esempio interruzioni nei collegamenti di rete, blackout);
- disturbi, ossia disturbi elettromagnetici o di contorno che possono causare interruzioni o malfunzionamenti dell'infrastruttura hardware o di interconnessione (ad esempio disturbi di rete di tipo intermittente o continuo);
- compromissione di informazioni, ossia azioni mirate ad ascoltare, interrompere o prendere il controllo di una comunicazione di terzi senza il consenso. Le minacce 'legali' comprendono la violazione di norme e leggi, nonché il mancato rispetto dei requisiti contrattuali da parte di prestatori di servizi verso gli utilizzatori

dell'infrastruttura di rete (ad esempio furto di documenti o di supporti di memorizzazione);

- problemi tecnici, definiti come guasto o malfunzionamento. Ne sono esempi guasti o interruzioni di dispositivi di rete o sistemi, bug di software o errori di configurazione. Le 'interruzioni' sono disordini inattesi del servizio o riduzione della qualità che scendono al di sotto di un livello richiesto (ad esempio problemi ai software, uso dei servizi da parte di persone non autorizzate);
- azioni non autorizzate, ossia azioni che mirano ai sistemi, alle infrastrutture e/o alle reti mediante azioni dannose. Le minacce comuni sono generalmente definite come attacchi informatici e azioni correlate (ad es. spam, malware, spyware, botnet, manipolazione di hardware e software, alterazioni delle configurazioni, DDoS, sfruttamento di bug dei software, violazione di dati, furto di identità);
- compromissione di funzioni, ossia un danno involontario o accidentale che si riferisce a distruzione, danni fisici e perdite di informazioni per lo più dovuti ad alterazioni del sistema o all'utilizzo inadeguato dei sistemi;
- attacchi di ingegneria sociale, ossia danni veicolati attraverso una serie di tecniche basate su processi cognitivi di influenzamento, inganno e manipolazione che, sfruttando l'ingenua disponibilità e buona fede, nonché l'ignoranza e poca attenzione della vittima, sono finalizzate all'ottenimento di informazioni riservate o sensibili (ad esempio attacchi phishing, divulgazione involontaria delle informazioni).

Data Protection Impact Assessment (DPIA)

Titolare del trattamento: *Centro Nazionale Sangue*

Ulteriori Titolari del trattamento: *Istituto Superiore di Sanità*

Centri Partecipanti allo Studio

Nome Progetto: *Studio sull'appropriatezza dell'utilizzo clinico delle Immunoglobuline polivalenti ("IG") in Italia*

Data di creazione: 12 gennaio 2026

A) CONTESTO

1) Finalità del trattamento:

- Studio e ricerca scientifica

2) Categorie di interessati:

- ✓ Pazienti soggetti alla somministrazione di IG polivalenti

3) Numero di interessati:

- ✓ Circa 35.000 interessati

4) Sono somministrate le informazioni privacy all'interessato?

- ✓ No, non è possibile somministrare le informazioni privacy *ex* art. 13 GDPR e reperire il consenso degli interessati in quanto lo Studio è retrospettivo e prevede, dunque, il trattamento di dati personali già raccolti in una fase antecedente dalle singole Unità Operative partecipanti. Per tale ragione verrà utilizzata la procedura descritta all'art. 110 del Codice Privacy potendosi effettuare lo studio anche in assenza del consenso degli interessati. A seguito del parere favorevole del Comitato Etico, è stata

pubblicata sul sito istituzionale del CNS la presente DPIA e le informazioni privacy ex art. 13 GDPR.

5) Come sono rese all'interessato le informazioni privacy?

- ✓ Le informazioni privacy sono consultabili sul sito istituzionale del CNS.

6) Sono previste modalità per l'esercizio dei diritti dell'interessato? (quali, il diritto di accesso, di rettifica, di cancellazione, di limitazione, di portabilità dei dati, di opposizione)

- ✓ Si, inviando apposita comunicazione esclusivamente all'indirizzo PEC del Centro partecipante allo Studio e non anche al CNS poiché il CNS riceverà esclusivamente dati pseudonimizzati e, dunque, non è a conoscenza dell'identità degli interessati.

7) Quali sono le modalità per l'esercizio dei diritti dell'interessato?

- ✓ A mezzo mail/PEC

8) Categorie di dati personali:

- ✓ Dati anagrafici pseudonimizzati (sesso e fascia di età)
- ✓ Dati relativi alla salute

9) Elenco delle attività di trattamento effettuate:

- ✓ **Raccolta** per il tramite degli operatori dell'Unità Operativa di riferimento partecipante allo Studio. Le fonti dalle quali i dati verranno estratti sono i c.d. File F, i Piani Terapeutici e le Schede di Dimissione Ospedaliera (anche dette SDO). Ad eccezione delle SDO, presenti in forma pseudonimizzata presso l'Istituto Superiore di Sanità che effettuerà anche l'analisi statistica su tali dati, i File F e i Piani Terapeutici verranno inviati in forma pseudonimizzata al CNS da parte dei Centri partecipanti.
- ✓ **Registrazione** sui server ISS tramite flusso mail con in allegato il file Excel contenente le informazioni proprie dello studio protetto da password
- ✓ **Conservazione** sui server dell'ISS
- ✓ **Consultazione** da parte del CNS e dell'ISS che avranno visione dei dati personali di tutti i partecipanti allo studio in forma pseudonimizzata

- ✓ **Utilizzo** al fine di definire la misura del grado di inappropriatezza di utilizzo di IG attraverso l'individuazione di utilizzi off-label e la rilevazione dei dati di consumo, per singola struttura sanitaria e singola specialità, per patologia e intervento terapeutico
- ✓ **Comunicazione** intesa come messa a disposizione dei dati personali pseudonimizzati da parte delle Unità Operative partecipanti al CNS come allegati alla mail, protetti da password che verrà comunicata mediante altro canale
- ✓ **Cancellazione** trascorsi 36 mesi dalla data di approvazione del Comitato Etico

10) Modalità di conservazione:

- ✓ Digitale

11) Cancellazione:

- ✓ Trascorsi 36 mesi dalla data di approvazione del Comitato Etico;
- ✓ Spirato tale termine i dati personali verranno cancellati o resi anonimi e, dunque, conservati *sine die* in quanto non più soggetti alla normativa sulla protezione dei dati personali.

12) Categorie di destinatari:

- ✓ Enti, Organismi, Autorità verso i quali i Titolari del trattamento (Centro partecipante allo studio, CNS e ISS) hanno un obbligo di comunicazione previsto dalla legge.

13) Piattaforme, dispositivi e/o applicativi utilizzati nell'ambito dell'attività di trattamento in esame:

- ➢ I dati verranno inviati tramite file Excel allegati alla mail, protetti da password che sarà comunicata mediante altro canale

14) Avviene un trasferimento di dati personali al di fuori dei confini nazionali?

- ✓ No

15) Base Giuridica del Trattamento *ex* art. 6 GDPR:

- ✓ Attività di ricerca medica, biomedica ed epidemiologica (art. 110 d.lgs. 30 giugno 2003, n. 196)

16) Base giuridica del trattamento ex art. 9 GDPR:

- ✓ Attività di ricerca medica, biomedica ed epidemiologica (art. 110 d.lgs. 30 giugno 2003, n. 196)

17) Tipologia di trattamento:

- ✓ Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;
- ✓ Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

B) MISURE DI SICUREZZA

B.1) MISURE DI SICUREZZA ORGANIZZATIVE

Presenti nella DPIA integrale non oggetto di pubblicazione sul sito istituzionale del CNS

C) DPIA

40) Vengono applicate e/o osservate linee guida, *best practice* di settore, norme UNI/ISO/IEC, codice di condotta, regolamenti aziendali, etc.?

- ✓ No

41) La finalità di trattamento è specifica, esplicita e legittima?

- ✓ **Specifica**: è ben delineata e consiste nella realizzazione dello "*Studio sull'appropriatezza dell'utilizzo clinico delle immunoglobuline polivalenti in Italia*", proposto dal CNS e svolto in collaborazione con l'ISS e i vari Centri partecipanti, al fine di analizzare la qualità dei dati e armonizzare le fonti dati relative all'impiego terapeutico di IG polivalenti e delle singole modalità di somministrazione, analizzare, attraverso metodologie di statistica descrittiva e inferenziale, i dati estratti dai flussi informativi individuati e, dunque, definire il grado di appropriatezza di utilizzo clinico delle Immunoglobuline polivalenti in Italia.

- ✓ **Esplicita**: nonostante non sia possibile fornire le informazioni privacy all'interessato al momento della raccolta dei dati, in quanto lo studio è retrospettivo, l'informativa sarà comunque consultabile sul sito istituzionale del CNS, insieme alla presente DPIA;
- ✓ **Legittima:** in quanto conforme alla normativa privacy e sorretta da idonea base giuridica come rappresentato ai punti 15 e 16 della presente DPIA.

42) Come viene rispettato il principio di minimizzazione dei dati?

- ➢ Sono raccolti esclusivamente i dati personali necessari al conseguimento della specifica finalità del trattamento e i dati vengono sottoposti precedentemente a pseudonimizzazione al fine di non rendere direttamente identificabili gli interessati per il CNS e per l'ISS.

C.1) ACCESSO ILLEGITTIMO

43) Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di accesso illegittimo dovesse concretizzarsi?

- ✓ Perdita del controllo dei dati personali
- ✓ Perdita di riservatezza dei dati personali protetti da segreto professionale
- ✓ Conoscenza da parte di terzi non autorizzati
- ✓ Decifratura non autorizzata alla pseudonimizzazione

44) Quali sono le principali minacce che potrebbero concretizzare il rischio?

- ✓ Danni fisici
- ✓ Azioni non autorizzate
- ✓ Attacchi di ingegneria sociale

Per la descrizione dettagliata delle minacce si rimanda a pag. 7 e 8 della presente DPIA.

45) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne
- ✓ Fonti umane esterne

Di seguito il risultato, sotto forma di tabella, degli impatti e della probabilità che l'evento si verifichi.

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
1, 2, 3 TRASCURABILE 4, 6, 8 LIMITATO 9, 12, 16 MASSIMO	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

C.2) MODIFICA INDESIDERATA

46) Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di modifica indesiderata dei dati dovesse concretizzarsi?

- ✓ Limitazione dei diritti
- ✓ Discriminazione

47) Quali sono le principali minacce che potrebbero concretizzare il rischio?

- ✓ Danni fisici
- ✓ Azioni non autorizzate

Per la descrizione dettagliata delle minacce si rimanda a pag. 7 e 8 della presente DPIA.

48) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne
- ✓ Fonti umane esterne

Di seguito il risultato, sotto forma di tabella, degli impatti e della probabilità che l'evento si verifichi.

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
1, 2, 3 TRASCURABILE 4, 6, 8 LIMITATO 9, 12, 16 MASSIMO	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

C.3) PERDITA ACCIDENTALE

49) Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di perdita di dati dovesse concretizzarsi?

- ✓ Limitazione dei diritti

50) Quali sono le principali minacce che potrebbero concretizzare il rischio?

- ✓ Danni fisici
- ✓ Eventi naturali
- ✓ Perdita di servizi essenziali
- ✓ Disturbi
- ✓ Azioni non autorizzate

Per la descrizione dettagliata delle minacce si rimanda a pag. 7 e 8 della presente DPIA.

51) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne
- ✓ Fonti umane esterne
- ✓ Fonti non umane

ALTAMENTE PROBABILE (4)	**4**	**8**	**12**	**16**
PROBABILE (3)	**3**	**6**	**9**	**12**
POCO PROBABILE (2)	**2**	**4**	**6**	**8**
IMPROBABILE (1)	**1**	**2**	**3**	**4**
1, 2, 3 TRASCURABILE 4, 6, 8 LIMITATO 9, 12, 16 MASSIMO	**LIEVE (1)**	**MEDIO (2)**	**GRAVE (3)**	**GRAVISSIMO (4)**

Di seguito il risultato, sotto forma di tabella, degli impatti e della probabilità che l'evento si verifichi.

GRAFICO DPIA

TRASCURABILE
LIMITATO
SIGNIFICATIVO
MASSIMO