

DPIA
ex art. 35 GDPR

IL CONTESTO NORMATIVO DEL DATA PROTECTION IMPACT ASSESSMENT

Il *Data Protection Impact Assessment* (per brevità anche DPIA) è uno strumento importante in termini di responsabilizzazione (*principio di accountability*), in quanto soccorre e 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*

"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

La disciplina sul *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

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 in 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 dell'*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,

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 ss.mm.ii.) e rispetto alle Linee Guida e Regole Deontologiche previste

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

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 27002:2017 ("*Information Technology - Security techniques - Code of practice for information security controls*") che indica le linee guida per gli standard di sicurezza delle informazioni organizzative e pratiche di gestione della sicurezza delle informazioni, compresa la selezione, l'implementazione e la gestione dei controlli;

- 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*

- 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,

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

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 psicolgici.

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

- 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



Nome Attività: EPLECO_Study
Data di creazione: 07/09/2026

A) CONTESTO

Valutazione del sistema Eplex per la diagnosi rapida della sepsi: uno studio comparativo con i metodi tradizionali di emocoltura (EPLECO)

1) Finalità del trattamento

- Studio e Ricerca Scientifica

2) Categorie di interessati

- Pazienti

3) Numero di interessati

- Da 100 a 1000

4) Sono somministrate le informazioni privacy all'interessato

- SI

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

- Consegna diretta all'interessato

6) Sono previste modalita' 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

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

- A mezzo mail/PEC

8) Categorie di dati personali

- Dati anagrafici in chiaro

- Dati anagrafici pseudonimizzati

- Dati di identificazione/riconoscimento

- Campioni biologici

- Dati relativi alla salute/sanitari

9) Elencare le attività di trattamento effettuate

- Registrazione

- Conservazione

- Organizzazione

- Consultazione

- Elaborazione

- Selezione

- Estrazione

- Raffronto

- Utilizzo

- Cancellazione

- Distruzione

10) Modalità di conservazione

- Digitale

11) Cancellazione

- I dati necessari ai fini dello studio saranno conservati per la durata dello studio oltre alla previsione di periodi successivi di verifica e monitoraggio del medesimo da parte di terzi e, quindi, per il periodo massimo di 2 anni. Trascorsi i due anni si procederà con la cancellazione dei dati in chiaro/pseudoanonimizzati o ad anonimizzazione completa

12) Categorie di destinatari

- Persona Autorizzata per Designazione ex art. 29 GDPR e 2 quaterdecies Codice Privacy

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

- Microsoft

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

- No

15) Base giuridica del trattamento ex art. 6 gdpr

- Esecuzione di un compito di interesse pubblico o connesso all'esercizio dei pubblici poteri (art. 6, par. 1, lett. E)

16) Base giuridica del trattamento ex art. 9 gdpr

- Archiviazione nel pubblico interesse ,di ricerca scientifica o storica o a i fini statistici (art. 9, par. 2, lett. J)

17) Tipologia di trattamento

- Trattamenti non occasionali di dati relativi a soggetti vulnerabili quali minori, disabili, anziani, infermi di mente, pazienti e richiedenti asilo

- Trattamenti di categorie particolari di dati ex artt. 9 e 10 GDPR interconnessi con altri dati personali raccolti per finalità diverse

18) Nomina delle persone autorizzate per designazione

- Si

19) Nomina dei delegati al trattamento

- Si

20) Nomina dei responsabili del trattamento

- Si

21) Elaborazione ed adozione di policy privacy aziendali

- Si

22) Quali?

- Il titolare ha adottato procedure e policy aziendali in materia di protezione dei dati personali e sicurezza delle informazioni, comprendenti la gestione degli accessi, l'assegnazione dei profili autorizzativi, la gestione degli incidenti ed ei data breach, la conservazione e la cancellazione dei dati, la sicurezza informatica, la continuità operativa, la gestione dei fornitori e la formazione del personale autorizzato al trattamento

23) Controllo degli accessi fisici

- Si

24) Quali?

- - L'accesso fisico ai locali dell'Istituto e alle aree in cui sono ubicati i sistemi informativi è consentito esclusivamente al personale autorizzato mediante le procedure di controllo degli accessi adottate dall'Ente.

25) Formazione del personale

- Si

26) Altra misura di sicurezza fisica e/o organizzativa implementata

- Sono adottate misure organizzative e tecniche finalizzate alla protezione dei dati personali, tra cui: profilazione degli accessi in base ai ruoli, autenticazione degli utenti, tracciamento e monitoraggio degli accessi e delle operazioni effettuate, formazione del personale autorizzato, procedure per la gestione degli incidenti di sicurezza e delle violazioni dei dati personali, obblighi di riservatezza, pseudonimizzazione dei dati ove applicabile, limitazione degli accessi ai soli soggetti autorizzati e applicazione delle procedure aziendali in materia di protezione dei dati personali e sicurezza delle informazioni

B.2) MISURE DI SICUREZZA TECHICHE

27) Crittografia database

- Non Applicabile

28) Sistema operativo workstation

- Windows

- Mac OS

- Linux

29) Aggiornamento sistema operativo

- Windows SI

- Mac OS SI

- Linux SI

30) Configurazione workstation

- Utente con restrizioni

- Crittografia dei dati

- Cambio password temporizzato

31) Tecniche di anonimizzazione

- Non Applicabile

32) Tecniche di pseudonimizzazione

- Pseudonimizzazione randomizzata al documento

- Pseudonimizzazione completamente randomizzata

33) Partizionamento

- Non Applicabile

34) Controllo degli accessi logici

- SI

35) Quali strumenti vengono utilizzati?

- Gestione degli accessi privilegiati: Applicazione parziale in corso di implementazione

36) Tracciabilità

- Si

37) Quali strumenti vengono utilizzati?

- SIEM: raccoglie i log (Domain Controller, Firewall, Switch, Server, Workstation tramite delle sonde) analizzati da un servizio SOC security operation center h24 7/7 gestito mediante contratto SGM

38) Misure anti malware

- Anti-virus

- Anti-malware

- Anti-spyware

- Gestione e aggiornamento delle patch di sicurezza

- Soluzioni Whitelisting

39) Backup

- Backup remoto

- Backup a caldo

- Backup integrale

- Backup incrementale

- Backup continuo

40) Sicurezza dei canali informatici

- Firewall

- Protocolli di rete

- SSL

- TLS

- SSH

- IPsec

- HTTPS

- Sistema di Autenticazione

- Mandatory Access Control (MAC)

- Intrusion Detection System (IDS)

- Network Intrusion Detection System (NIDS)

- XDR

- SOC

- SIEM

C) DPIA

41) Vengono applicate e/o osservate linee guida, best practice di settore, norme uni/iso/iec, codice di condotta, regolamenti aziendali etc.?

- Si

42) Quali sono? elencare

- Il trattamento è svolto nel rispetto del Regolamento (UE) 2016/679 (GDPR), del D.Lgs. 196/2003 e s.m.i. (Codice Privacy), delle Regole deontologiche per trattamenti a fini statistici e di ricerca scientifica adottate ai sensi del D.Lgs. 101/2018, delle procedure e policy aziendali INMI in materia di protezione dei dati personali e sicurezza delle informazioni, delle procedure di gestione degli accessi, degli incidenti di sicurezza e dei data breach. Per gli aspetti microbiologici e diagnostici sono applicati gli standard EUCAST vigenti. Il trattamento è inoltre effettuato nell'ambito della Ricerca Corrente Ministero della Salute e secondo le norme di buona pratica della ricerca scientifica e sanitaria

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

- La finalità del trattamento è specifica, esplicita e legittima. Il trattamento è effettuato esclusivamente per la realizzazione dello studio osservazionale retrospettivo EPLECO finalizzato alla valutazione delle prestazioni diagnostiche del sistema ePlex (Roche) nel contesto delle infezioni del sangue e della sepsi, mediante analisi di dati clinici e microbiologici raccolti nell'ambito della normale attività assistenziale. La finalità è specifica in quanto chiaramente individuata e limitata agli obiettivi scientifici del progetto; esplicita in quanto gli interessati sono informati, attraverso le informative privacy istituzionali dell'INMI, della possibilità che i dati raccolti per finalità di cura possano essere successivamente utilizzati per attività di ricerca scientifica svolte dall'Istituto; legittima in quanto il trattamento è fondato sugli articoli 6, paragrafo 1, lettera c), e 9, paragrafo 2, lettera j), del Regolamento (UE) 2016/679, nonché sugli articoli 110 e 110-bis del D.Lgs. 196/2003 e s.m.i., trattandosi di ricerca scientifica svolta da IRCCS nell'ambito della Ricerca Corrente del Ministero della Salute. I dati sono trattati esclusivamente per finalità di ricerca biomedica ed epidemiologica e non sono utilizzati per finalità incompatibili con quelle originarie di raccolta

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

- Il principio di minimizzazione è rispettato mediante la raccolta e il trattamento esclusivamente dei dati strettamente necessari al raggiungimento degli obiettivi scientifici dello studio EPLECO. I dati sono estratti dai sistemi aziendali limitatamente alle variabili cliniche, microbiologiche ed epidemiologiche indispensabili per le analisi previste dal protocollo. Successivamente i dati vengono sottoposti a pseudonimizzazione mediante attribuzione di un codice univoco al partecipante, con rimozione degli identificativi diretti. Il file sorgente contenente dati identificativi è conservato solo per il tempo strettamente necessario alla predisposizione del database di studio e successivamente eliminato. Non vengono raccolti né trattati dati eccedenti rispetto alle finalità della ricerca

45) 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

- Limitazione dei diritti

- Perdita di riservatezza dei dati personali protetti da segreto professionale

- Conoscenza da parte di terzi non autorizzati

- Danni fisici o psicologici

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

- Compromissione di informazioni

- Problemi tecnici

- Azioni non autorizzate

- Attacchi di ingegneria sociale

47) Quali sono le principali fonti di rischio?

- Fonti umane interne

- Fonti umane esterne

- Fonti non umane

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

- Perdita del controllo dei dati personali

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

- Problemi tecnici

- Azioni non autorizzate

50) Quali sono le principali fonti di rischio?

- Fonti umane interne

- Fonti umane esterne

- Fonti non umane

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

- Perdita del controllo dei dati personali

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

- Problemi tecnici

- Azioni non autorizzate

53) Quali sono le principali fonti di rischio?

- Fonti umane interne

- Fonti umane esterne

- Fonti non umane