DPIA
ex art. 35 GDPR

Sommario

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 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 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 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 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, 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 ss.mm.ii.) 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 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 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: *Istituto Superiore di Sanità*

Nome Attività: *Studio di ricerca scientifica che prevede l'utilizzo di ITA-MASLD, uno strumento per valutare il profilo clinico epidemiologico e l'impatto economico dei pazienti con MASLD e fibrosi del fegato seguiti nei centri di cura multidisciplinari*

Data di creazione: *9 gennaio 2025*

CONTESTO

ITA-MASLD è uno studio osservazionale basato su un campione rappresentativo di pazienti con diagnosi di MASLD, provenienti da 20 Centi Clinici distribuiti sul territorio nazionale.

Lo studio è promosso dall'ISS in stretta collaborazione con le Società Scientifiche Associazione Italiana per lo Studio del Fegato (AISF), Società Italiana dell'Obesità (SIO), Società Italiana di Medicina Interna (SIMI), Società Italiana di Diabetologia (SID) e il Club Epatologi Ospedalieri (CLEO) e svolto in collaborazione con i Centri Clinici multidisciplinari di pertinenza sia epatologica che di medicina interna distribuiti sul territorio nazionale.

Lo studio osservazionale multicentrico è svolto su una coorte di pazienti arruolati consecutivamente presso i Centri Clinici e si propone l'obiettivo di sviluppare evidenze scientifiche utili a supportare decisioni strategiche per la gestione dei pazienti, valutando l'impatto economico e farmaco-economico

della condizione e analizzando il costo-beneficio di strategie terapeutiche e di screening.

I dati personali verranno, pertanto, raccolti dal Centro Clinico nel corso della visita di arruolamento e nelle successive visite di follow-up per mezzo di appositi questionari contenuti in schede elettroniche e caricati in forma pseudonimizzata su una piattaforma in dotazione del Centro Clinico – ITA-MASLD- dalla quale l'ISS potrà scaricare i dati per poi conservarli sul proprio server per l'esecuzione delle analisi previste. L'ISS potrà accedere al sistema web mediante credenziali rilasciate ad hoc esclusivamente per scaricare i dati inseriti dai singoli Centri.

I dati potranno essere diffusi esclusivamente in forma aggregata, attraverso riunioni, convegni e pubblicazioni scientifiche.

1) Finalità del trattamento:

- ✓ Studio e ricerca scientifica

2) Categorie di interessati:

- ✓ Pazienti

3) Numero di interessati:

- ✓ Oltre i 1000

4) Sono somministrate le informazioni privacy all'interessato?

- ✓ Si

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

- ✓ Le informazioni privacy saranno rese disponibili dai Centri Partecipanti, nonché pubblicate sul sito web dell'ISS

6) Come si ottiene il consenso degli interessati?

- ✓ Tramite modulo di consenso al trattamento dei dati personali presente in calce alle informazioni privacy somministrate dal Centri Partecipanti

7) 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, tramite apposita comunicazione al Centro Clinico arruolante e non anche all'ISS, in quanto trasferiti a tale Istituto in forma pseudonimizzata

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

- ✓ A mezzo mail/PEC

9) Categorie di dati personali:

- ✓ Dati anagrafici in chiaro (per i Centri Partecipanti)
- ✓ Dati anagrafici pseudonimizzati (per l'ISS)
- ✓ Dati di contatto (per i Centri Partecipanti)
- ✓ Dati relativi all'origine razziale o etnica
- ✓ Dati relativi alla salute/sanitari
- ✓ Dati antropometrici

10) Elencare le attività di trattamento effettuate:

- ✓ Raccolta presso terzi
- ✓ Registrazione
- ✓ Conservazione
- ✓ Organizzazione
- ✓ Consultazione
- ✓ Selezione
- ✓ Estrazione
- ✓ Elaborazione
- ✓ Utilizzo
- ✓ Blocco/Limitazione
- ✓ Comunicazione
- ✓ Cancellazione
- ✓ Distruzione

11) Modalità di conservazione:

- ✓ Digitale (attraverso archiviazione su apposito *server*; i *file* scaricati verranno salvati su cartella OneDrive dedicata e condivisa al personale ISS facente parte del progetto)

12) *Data retention*:

- ✓ Sino al raggiungimento della finalità (nello specifico, i dati verranno conservati per la durata necessaria al raggiungimento della finalità per cui sono stati raccolti e/o conferiti, corrispondente a 15 anni o fino alla richiesta di modifica o cancellazione da parte dell'interessato)
- ✓ Mai, previa anonimizzazione (conservazione illimitata a seguito di totale anonimizzazione dei dati personali oggetto dello studio)

13) Categorie di destinatari:

- ✓ Nessuno

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

- ➢ *Database* interno all'ISS; piattaforma ITA-MASLD; OneDrive

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

- ✓ No

16) Base giuridica del Trattamento *ex* art. 6 GDPR:

- ✓ Consenso dell'interessato (art. 6, par. 1, lett. a)

17) Base giuridica del trattamento *ex* art. 9 GDPR

- ✓ Consenso rafforzato dell'interessato (art. 9, par. 2, lett. a)

18) Tipologia di trattamento:

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

B) MISURE DI SICUREZZA

B.1) MISURE DI SICUREZZA ORGANIZZATIVE

19) Sicurezza dell'archiviazione della documentazione cartacea:

- ✓ Non applicabile

20) Nomina delle Persone autorizzate per designazione

- ✓ Si

21) Nomina dei delegati al trattamento:

- ✓ Si

22) Nomina dei Responsabili del trattamento:

- ✓ No

23) Elaborazione ed adozione di policy privacy aziendali:

- ✓ Si

24) Quali?

- ➢ Policy informazioni privacy

25) Controllo degli accessi fisici:

- ✓ Si

26) Quali?

- ➢ Si previene l'accesso di personale non autorizzato ai locali mediante l'utilizzo di *badge* personali ed un servizio di guardiania posto all'ingresso della struttura; è attivo un sistema di videosorveglianza e viene tenuto un apposito registro; l'accesso fisico al *server* dell'ISS è consentito soltanto al personale tecnico; i *data center* sono situati in un luogo sicuro e vigilato da sistemi di video-sorveglianza con registrazione, sistemi di identificazione personale, portineria e utilizzo di porte di accesso blindate; vengono adottate tutte le misure necessarie per evitare fenomeni di accesso ai dati da parte di persone non autorizzate; gli accessi fisici alle sedi ISS sono protetti e vigilati dal Servizio Sorveglianza e Controllo Accessi dell'Istituto. Le stanze presso cui sono collocate le postazioni sono chiuse a chiave

27) Formazione del personale:

- ✓ Si

28) Altra misura di sicurezza fisica e/o organizzativa implementata:

- ➢ Gli edifici ed i locali in cui risiedono i *server* sono dotati di un sistema di allarme antincendio e di un impianto elettrico a norma CE, che è dotato di un gruppo elettrogeno per garantire la continuità dei sistemi informatici ospitati e di un sistema di allarme; le postazioni di lavoro dell'ISS sono gestite centralmente, il cui accesso è consentito ai soli utenti autorizzati, tramite credenziali istituzionali; l'infrastruttura fisica che ospita gli impianti informatici dell'ISS è suddivisa su *data center* multipli; le postazioni sono collocate in aree non soggette a rischi elevati e sono protette contro urti e danneggiamento

B.2) MISURE DI SICUREZZA TECNICHE

29) Crittografia *Database*:

- ✓ I dati saranno ricevuti in formato Excel in un *file* criptato e protetto da *password* che verrà inserita dagli utenti autorizzati al momento del *download*

30) Sistema operativo *workstation*:

- ✓ Windows

31) Aggiornamento sistema operativo:

- ✓ Windows Si

32) Configurazione *workstation*:

- ✓ Utente con restrizioni

33) Tecniche di anonimizzazione:

- ✓ Non applicabile

34) Tecniche di pseudonimizzazione:

- ✓ Si, ad opera dei Centri Clinici (Lo pseudonimo viene generato al momento dell'inserimento dei dati da parte del Centro Clinico nel *database*; codice *random* non parlante, non generato a partire da dati personali; l'ISS riceve dai Centri Partecipanti

i dati pseudonimizzati; nello specifico, il codice fiscale verrà digitato dal medico del Centro Clinico arruolante per creare un codice ITA-MASLD univoco non invertibile; ad ogni codice fiscale potrà essere associato un solo codice; inoltre, ai dati esportati verrà assegnato un secondo codice, al fine di disaccoppiarli da quelli residenti in piattaforma; la lista di corrispondenza tra i dati anagrafici e i codici identificativi dei pazienti sarà conservata presso il Centro Clinico, che ne sarà responsabile)

35) Partizionamento:

- ✓ Non applicabile

36) Controllo degli accessi logici:

- ✓ Si

37) Quali strumenti vengono utilizzati?

- ✓ L'ISS accede alla piattaforma ITA-MASLD dei Centri Clinici arruolanti mediante credenziali fornite *ad hoc* esclusivamente per scaricare i dati ivi contenuti; l'accesso a OneDrive, su cui vengono archiviati i dati oggetto di trattamento, è consentito ai soli soggetti autorizzati mediante l'utilizzo di credenziali istituzionali e autenticazione a due fattori; l'accesso alle *workstation* utilizzate per l'attività trattamentale in oggetto, nonché alle risorse di rete eventualmente messe a disposizione da ISS, avviene mediante credenziali istituzionali

38) Tracciabilità:

- ✓ Si

39) Quali strumenti vengono utilizzati?

- ➢ Gli accessi alle risorse ICT dell'ISS sono registrati secondo quanto previsto dalla relativa procedura operativa, al fine di garantire tracciabilità degli accessi e delle operazioni

40) Misure anti malware:

- ✓ *Next-generation Anti-virus*
- ✓ *Anti-spam*
- ✓ *Anti-malware*

41) Backup:

- ✓ Si (L'ISS esegue il *backup* giornaliero dei dati presenti sulla propria infrastruttura, seguendo quanto descritto nella procedura operativa dedicata al tema. Il *backup* dei dati esclusivamente locali -non in *cloud* o su *share* di rete- contenuti nelle *workstation* è demandato agli utenti finali. Per i dati archiviati su OneDrive si utilizzano le funzionalità di *versioning* e protezione offerte da SharePoint)

42) Sicurezza dei canali informatici:

- ✓ Sistema di autenticazione
- ✓ *Web Application Firewall*
- ✓ Protocolli di rete *HTTPS*

43) Altra misura di sicurezza tecnica implementata:

- ✓ Nessuna

C) DPIA

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

- ✓ No

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

- ✓ **Specifica**: è ben delineata ed individuata nella finalità del Titolare di condurre uno studio volto alla raccolta di dati relativi a pazienti affetti da MASLD (malattia epatica associata a disfunzione metabolica) provenienti dai Centri Clinici arruolanti;
- ✓ **Esplicita**: si, in quanto rappresentata agli interessati per il tramite delle Informazioni privacy *ex* art. 13 e 14 GDPR sottoposte all'attenzione di questi con pubblicazione sul sito *web* istituzionale, nonché somministrate personalmente agli interessati da parte dei Centri Partecipanti;
- ✓ **Legittima:** in quanto conforme alla normativa privacy, poiché è sorretta da un'idonea base giuridica del trattamento e, nello specifico: art. 6, par. 1, lett. a) GDPR, nonché art. 9, par. 2, lett. a) GDPR, in quanto "*l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati personali*".

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

- ✓ Sono trattati esclusivamente i dati necessari al perseguimento della finalità del Titolare, consistente nella volontà di condurre uno studio di ricerca scientifica su pazienti affetti da MASLD. Difatti, i dati personali oggetto di raccolta risultano fondamentali per l'esecuzione dell'attività trattamentale descritta nel contesto; pertanto, i dati raccolti risultano adeguati, pertinenti e limitati rispetto alla specifica finalità, con la conseguenza che il trattamento è legittimo e proporzionato rispetto alla finalità che il Titolare del trattamento intende perseguire

C.1) ACCESSO ILLEGITTIMO

47) 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
- ✓ Decifratura non autorizzata della pseudonimizzazione
- ✓ Discriminazione
- ✓ Perdita di riservatezza dei dati personali protetti da segreto professionale
- ✓ Conoscenza da parte di terzi non autorizzati

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

- ✓ Danni fisici
- ✓ Compromissione di informazioni
- ✓ Problemi tecnici
- ✓ Azioni non autorizzate
- ✓ Attacchi di ingegneria sociale

49) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne
- ✓ Fonti umane esterne

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

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

- ✓ Discriminazione
- ✓ Limitazione dei diritti

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

- ✓ Danni fisici
- ✓ Azioni non autorizzate

52) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne
- ✓ Fonti umane esterne

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

53) 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
- ✓ Discriminazione

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

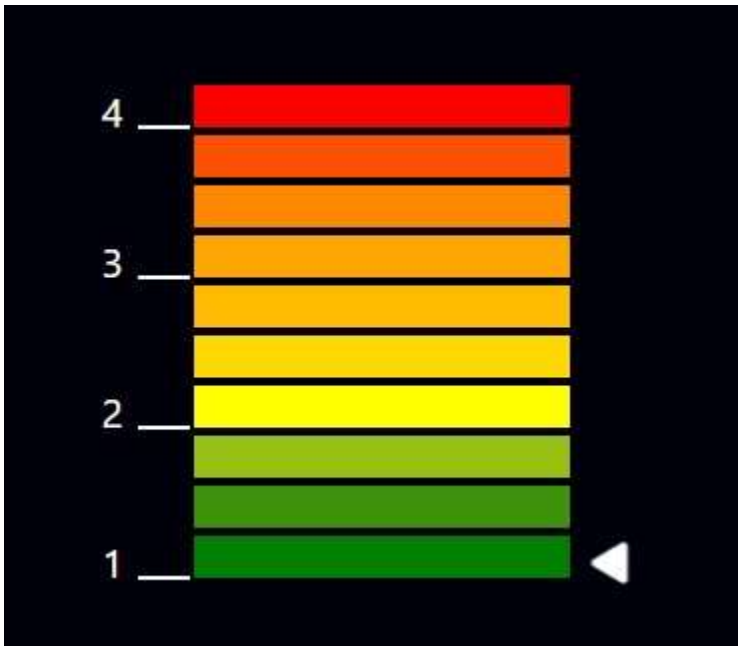
- ✓ Danni fisici
- ✓ Eventi naturali
- ✓ Perdita di servizi essenziali
- ✓ Azioni non autorizzate
- ✓ Compromissione di funzioni

55) 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)

GRAFICO DPIA



TRASCURABILE
LIMITATO
SIGNIFICATIVO
MASSIMO