

(Estratto) DPIA *ex* art. 35 GDPR

Sommario

IL CONTESTO NORMATIVO DEL DATA PROTECTION IMPACT ASSESSMENT 3
Data Protection Impact Assessment 9
A) CONTESTO 9
B) MISURE DI SICUREZZA 13
B.1) MISURE DI SICUREZZA ORGANIZZATIVE 13
B.2) MISURE DI SICUREZZA TECNICHE 14
C.1) ACCESSO ILLEGITTIMO 16
C.2) MODIFICA INDESIDERATA 17
C.3) PERDITA ACCIDENTALE 18
GRAFICO DPIA 20

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*

Contitolari del trattamento: *CRO, Azienda Zero Veneto, Sapienza*

Nome Attività: *Studio internazionale sull'implementazione del modello EPICOST in Europa (Task 8.4: Monitoring access to health care and health care costs on a population level - Joint Action Prevent_NCD).*

Data di creazione: *17 luglio 2026*

A) CONTESTO

Il trattamento si colloca nell'ambito del Progetto di ricerca TASK 8.4-ITALY della JOINT ACTION PREVENT NCD (GA 101128023), finanziata da HADEA nel Programma EU4Health. Il progetto ha come obiettivo principale il monitoraggio dell'impatto delle malattie non trasmissibili sulla spesa sanitaria relativa ai pazienti, come risultato del loro accesso e utilizzo dei servizi sanitari, considerando l'intero percorso della malattia. L'applicazione riguarda i pazienti oncologici.

Sono invece obiettivi secondari la stima dei costi sanitari diretti dei pazienti oncologici, la stima della frequenza delle recidive di malattia e la modellizzazione dei costi sanitari diretti.

I dati preesistono nei Registri tumori di popolazione (PBCR) e nei flussi sanitari amministrativi (SDO, SPS, FT, File F, Hospice, SIAD, PS, FAR, AP), alimentati per finalità diverse da quella di ricerca. Ciascun PBCR seleziona, sui soli casi di propria pertinenza, i casi incidenti per le sedi tumorali di studio (incidenza 2008-2022, follow-up in vita al 31/12/2023) e li sottopone a linkage

individuale con i flussi HCS nella finestra 01/01/2017-31/12/2023: Il dato è quindi identificato e produce un profilo longitudinale settennale di diagnosi, prestazioni e costi. Il dataset è pseudonimizzato mediante codice IDPZ e caricato in area segregata di un applicativo gestito da un fornitore ISS quale Responsabile ex art. 28 GDPR, con accesso limitato per ciascun registro ai propri dati e vista d'insieme in capo all'ISS; la mapping table resta presso il registro di origine, sicché il dato conserva natura personale. Eseguiti i controlli di qualità e la validazione da parte dell'ISS, l'IDPZ è eliminato, è attribuito un codice tecnico interno e le mapping table sono definitivamente distrutte: da tale momento i dati sono trattati e conservati in forma anonimizzata per le analisi e la divulgazione scientifica previste dal protocollo. La conservazione in forma pseudonimizzata non eccede i 6 mesi dall'acquisizione del dataset dal centro partecipante.

Il Progetto ha, pertanto, carattere retrospettivo, e le attività trattamentali sui dati relativi alla salute, sono svolte a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, in relazione alla fattispecie, prevista dall'art. 110 del Codice Privacy, per cui non risulta possibile contattare gli interessati per motivi organizzativi.

Allo stato attuale risulta, infatti, impossibile dal punto di vista organizzativo raccogliere il consenso degli interessati perché contattarli rappresenterebbe uno sforzo sproporzionato rispetto alle finalità e ai mezzi dello studio. Inoltre, un gran numero degli interessati, vista la patologia presa in considerazione, è deceduta. Ad esempio, per il Veneto, la coorte dei casi selezionati per lo studio nel periodo 2008-2022 è di circa 280.000 pazienti, dei quali circa la metà (48%) è deceduta. Nello stesso periodo, le nuove diagnosi di tumori in Friuli Venezia Giulia sono state circa 50.000.

Non risulta neanche possibile un'eventuale esclusione dallo studio dei soggetti deceduti (che rappresentano un numero elevato rispetto al numero complessivo di soggetti arruolabili nella ricerca) perché ciò determinerebbe conseguenze significative per la qualità dello studio stesso, rischiando di pregiudicare il conseguimento delle finalità della ricerca. Infatti, uno degli outcome del progetto è calcolare il profilo di costo dei pazienti nell'ultimo anno di vita, periodo nel quale i costi sanitari aumentano sensibilmente.

Finalità del trattamento:

- ✓ Studio e ricerca scientifica

2) Categorie di interessati:

- ✓ Pazienti
- ✓ Dipendenti

3) Numero di interessati:

- ✓ Oltre i 1000

4) Sono somministrate le informazioni privacy all'interessato?

- ✓ Sì

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

- ✓ Tramite informativa privacy pubblicata sui siti internet dei contitolari del trattamento.

6) Come si ottiene il consenso degli interessati?

- ✓ N.A.

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)

- ✓ Sì

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

- ✓ A mezzo mail/PEC
- ✓ Raccomandata A/R

9) Categorie di dati personali:

- ✓ Dati personali anagrafici pseudonimizzati
- ✓ Dati relativi alla salute e sanitari

10) Elencare le attività di trattamento effettuate:

- ✓ Raccolta
- ✓ Registrazione
- ✓ Conservazione digitale
- ✓ Consultazione
- ✓ Elaborazione
- ✓ Selezione
- ✓ Estrazione
- ✓ Utilizzo

11) Modalità di conservazione:

- ✓ Digitale

12) *Data retention*:

I dati pseudonimizzati sono conservati finché non viene effettuata la validazione e comunque non oltre i 6 mesi dall'acquisizione degli stessi.

13) Categorie di destinatari:

- ✓ Contitolari del trattamento ex art. 26 GDPR
- ✓ Soggetti nominati Responsabili del trattamento ex art. 28 GDPR

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

- ➢ Piattaforma centralizzata presso ISS

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

- ✓ No

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

- ✓ Esecuzione di un interesse pubblico o trattamento connesso all'esercizio di pubblici poteri (art. 6, par. 1, lett. e);

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

- ✓ Trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici sulla base del diritto dell'Unione Europea o degli Stati Membri (art. 9, par. 2, lett. j)
- ✓ Art. 110 Codice Privacy D.Lgs. 196/2003 e ss.mm.ii.

18) Tipologia di trattamento:

- ➢ Elaborazione dati su larga scala con conseguenze per un gran numero di parti interessate; Analisi statistica per la produzione di indicatori

B) MISURE DI SICUREZZA

B.1) MISURE DI SICUREZZA ORGANIZZATIVE

19) Sicurezza dell'archiviazione della documentazione cartacea:

- ✓ ISS: N.A.
- ✓ Sapienza: N.A.
- ✓ Azienda Zero Veneto: N.A.
- ✓ CRO: N.A.

20) Nomina delle Persone autorizzate per designazione

- ✓ Si

21) Nomina dei delegati al trattamento:

- ✓ No

22) Nomina dei Responsabili del trattamento:

- ✓ Sì

23) Elaborazione ed adozione di policy privacy aziendali:

- ✓ Si

24) Quali?

ISS, CRO, Sapienza, Azienda Zero Veneto:

- ➢ Policy informazioni privacy
- ➢ Procedura data breach

25) Controllo degli accessi fisici:

- ✓ Sì

26) Quali?

- *(omissis)*

27) Formazione del personale:

- ✓ Si

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

ISS: L'ISS adotta un Sistema di Gestione per la Sicurezza delle Informazioni ISO 27001 e procedure di gestione incidenti informatici conformi NIS2.

Sapienza: La Sapienza Università di Roma adotta procedure di gestione incidenti informatici conformi NIS2.

Azienda Zero Veneto: Azienda Zero adotta un sistema di gestione degli incidenti informatici.

CRO: Il CRO di Aviano adotta procedure di gestione incidenti informatici conformi NIS2.

B.2) MISURE DI SICUREZZA TECNICHE

29) Crittografia *Database*:

- (omissis)

30) Sistema operativo *workstation*:

- ✓ *(omissis)*

31) Aggiornamento sistema operativo:

- ✓ Si

32) Configurazione *workstation*:

- ✓ *(omissis)*

33) Tecniche di anonimizzazione:

(omissis)

34) Tecniche di pseudonimizzazione:

- ✓ *(omissis)*

35) Partizionamento:

(omissis)

36) Controllo degli accessi logici:

- ✓ Si

37) Quali strumenti vengono utilizzati?

(omissis)

38) Tracciabilità:

- ✓ Si

39) Quali strumenti vengono utilizzati?

- ➢ *(omissis)*

40) Misure anti malware:

(omissis)

41) Backup:

- (omissis)

42) Sicurezza dei canali informatici:

(omissis)

43) Altra misura di sicurezza tecnica implementata:

ISS: N.A.
Sapienza: N.A.
Azienda Zero Veneto: N.A.
CRO: N.A.

C) DPIA

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

Si. Titolare e contitolari dello studio sono certificati:

- ✓ ISO 27001

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

Specifica: è ben delineata ed individuata nella ricerca scientifica in campo medico, biomedico ed epidemiologico e, nello specifico, per lo svolgimento del Progetto di ricerca

scientifica svolto nell'ambito della JOINT ACTION PREVENT NCD (GA –101128023), quale azione finanziata dalla European Health and Digital Executive Agency (HADEA), agenzia della Commissione Europea nell'ambito del Programma di Ricerca europeo EU4Health in materia di salute.

Esplicita: si, in quanto rappresentata agli interessati per il tramite delle Informazioni privacy *ex* art. 13 e 14 GDPR rese accessibili agli interessati da parte dei contitolari mediante pubblicazione sui siti internet dei contitolari stessi;

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. e) GDPR, nonché art. 9, par. 2, lett. j) e art. 110 Codice Privacy D.Lgs. 196/2003 e ss.mm.ii.

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

Sono trattati esclusivamente i dati necessari al perseguimento della finalità dei contitolari, consistente nella volontà di svolgere attività di ricerca al fine di raccogliere dati dei Registri Tumori partecipanti al task 8.4 della JA Prevent NCD. 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;
- ✓ Danni fisici o psicologici;
- ✓ Conoscenza da parte di terzi non autorizzati;

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

- ✓ Azioni non autorizzate
- ✓ Attacchi di ingegneria sociale

49) Quali sono le principali fonti di rischio?

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)

- ✓ Fonti umane interne
- ✓ Fonti umane esterne

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?

- ✓ Perdita del controllo dei dati personali;
- ✓ Conoscenza da parte di terzi non autorizzati;

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

- ✓ Azioni non autorizzate
- ✓ Attacchi di ingegneria sociale

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?

- ✓ Perdita di controllo dei dati personali
- ✓ Danni fisici o psicologici

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

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

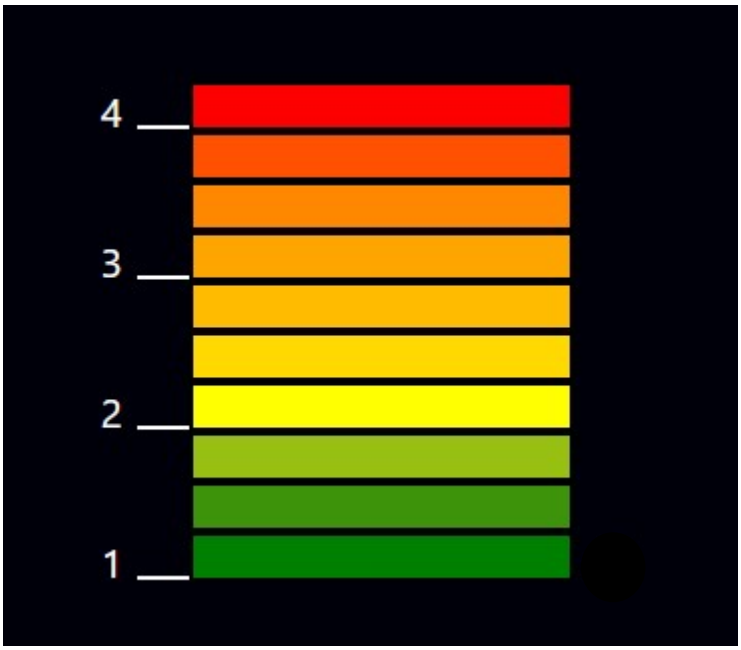
55) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne

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)

- ✓ Fonti umane esterne
- ✓ Fonti non umane

GRAFICO DPIA



TRASCURABILE
LIMITATO
SIGNIFICATIVO
MASSIMO