Linee Guida Per la conduzione delle attività di Data Protection Impact Assessment

1.GENERALITA’

Il Data Protection Impact Assessment (DPIA) o “Valutazione di impatto sulla protezione dei dati” rappresenta una delle fondamentali attività previste dal Regolamento UE 679/2016, “GDPR”, relativamente agli obblighi dei Titolari (cfr. art 35), nell’ambito della gestione del rischio correlato al trattamento di dati personali.

Il DPIA è un processo inteso a gestire i rischi per i diritti e le libertà delle persone fisiche che potrebbero derivare da un particolare trattamento ed a determinare le misure per ridurli. La valutazione d’impatto sulla protezione dei dati è uno strumento importante di responsabilizzazione in quanto supporta il titolare del trattamento non soltanto nel rispetto dei requisiti del Regolamento ma anche ai fini della dimostrazione che sono state adottate misure appropriate.

Il principio di “proporzionalità e necessità del trattamento”, caposaldo del GDPR, rappresenta il punto prodromico di ogni valutazione circa il trattamento dei dati personali (art 35 GDPR, Considerando 4,156), per cui la mancata esecuzione di una valutazione d’impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa, l’esecuzione in maniera errata di detta valutazione oppure la mancata consultazione del Garante per la protezione dei dati personali laddove richiesto potrebbero comportare l’irrogazione di sanzioni.

In linea con l’approccio basato sul rischio, adottato dal Regolamento, è necessario realizzare un DPIA quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"; risulta pertanto fondamentale svolgere un’analisi preliminare per individuare tali trattamenti e dotarsi di principi e metodologie comuni per lo svolgimento delle attività di valutazione.

1.1 FINALITÀ DEL DOCUMENTO

Il presente documento descrive le linee guida per la conduzione delle attività di Data Protection Impact Assessment attuate dalla A.O. Santobono Pausilipon al fine di garantire l’adozione di un approccio rigoroso basato sul rischio ed in linea con i requisiti del Regolamento.

1.2 AMBITO DI APPLICAZIONE

Gli indirizzamenti definiti nel presente documento si applicano ai trattamenti della A.O. Santobono Pausilipon e sono da ritenersi estesi anche ai responsabili e agli eventuali sub-responsabili del trattamento di dati personali, nei modi e nei termini definiti nell’art. 28 del GDPR.

1.3 DOCUMENTI DI RIFERIMENTO

[1] Regolamento (UE) 2016 del Parlamento Europeo e del Consiglio, del 27 Aprile 2016, relativo alla protezione delle persone con riguardo al trattamento dei dati personali – Regolamento Generale sulla Protezione dei Dati (GDPR) e ss.mm.ii.

[2] D.lgs. 10 agosto 2018, n. 101. “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)”

[3] D.lgs. 30 Giugno 2003, n. 196 “Codice in materia di protezione dei dati personali” e s.m.i.

[4] ISO/IEC 27001:2013 “Information Security Management Systems”, 01/10/2013

[5] ISO/IEC 27002:2013 “Code of practice for information security controls", 01/10/2013

[6] ISO/IEC 27005: 2011 “Information technology — Security techniques — Information security risk management, Second edition 2011-06-01
[7] ISO/IEC 29134:2017(E) “Information technology - Security techniques - Guidelines for privacy impact assessment”, First edition 2017-06
[8] ISO/IEC 29100:2011 “Privacy Framework”
[9] ISO/IEC 29151:2017 “Code of practice for personally identifiable information protection”
[10] “Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation”, European Data Protection Supervisor, Febbraio 2018
[11] “Privacy Impact Assessment (PIA) Methodology”, Autorità francese per la protezione dei dati (CNIL), Febbraio 2018
[12] “Privacy Impact Assessment (PIA) Knowledge Bases”, Autorità francese per la protezione dei dati (CNIL), Febbraio 2018
[13] WP29 Gruppo istituito ai sensi dell’art. 29 della direttiva 95/46 CE (dal 25 Maggio prende il nome di EDPB – European Data Protection Board)
[14] “Linee guida in materia di valutazione d’impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679”, WP 248 rev.01, 04/04/2017
[15] “Linee guida sui responsabili della protezione dei dati”, WP 243 rev. 01, 05/04/17

1.4 ACRONIMI E DEFINIZIONI

Categorie particolari di dati personali	Dati personali che rivelano l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona.
Consenso dell’interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell’interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l’identificazione univoca, quali l’immagine facciale o i dati dattiloscopici.
Dati genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall’analisi di un campione biologico della persona fisica in questione.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Dati relativi alla salute	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
Destinatario	La persona fisica o giuridica, l’autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell’ambito di una specifica indagine conformemente al diritto dell’Unione o degli Stati 4.5.2016 IT Gazzetta ufficiale dell’Unione europea L 119/33 membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.
Dossier sanitario	Il dossier sanitario è lo strumento costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es. ospedale, azienda sanitaria, casa di cura) al cui interno operino più professionisti, attraverso il quale sono rese accessibili informazioni, inerenti allo stato di salute di un individuo, relative ad eventi clinici presenti e trascorsi (es., referti di laboratorio,

	documentazione relativa a ricoveri, accessi al pronto soccorso), volte a documentarne la storia clinica.
DPIA	Data Protection Impact Assessment (art. 35 del GDPR).
DPO/RDP	Data Protection Officer./ Responsabile della Protezione dei Dati.
FSE	Il fascicolo sanitario elettronico (FSE) è l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito.
GDPR	Regolamento Generale per la Protezione dei Dati.
IaaS	Infrastructure as a Service.
SaaS	Software as a Service
PaaS	Platform as a Service.
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
Pseudonimizzazione	Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Rappresentante	La persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento.
Referto online	Possibilità di accedere al referto tramite modalità digitali (Fascicolo sanitario elettronico, sito Web, posta elettronica anche certificata, supporto elettronico).
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
RPO	Recovery Point Objective.
RTO	Recovery Time Objective.
Terzo	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Trattamento transfrontaliero	a) Trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) Trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.
Violazione dei dati personali	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

1.5 RUOLI E RESPONSABILITÀ

La responsabilità di condurre un DPIA è assegnata al Titolare del trattamento in base all'art. 35, par. 1 del Regolamento.
Nello svolgimento di tale attività, il Titolare è assistito dalla UO Controllo Interno e Tutela della Privacy e supportato dal Responsabile della Protezione dei Dati (RDP/DPO).
In particolare è necessario il parere del DPO aziendale sulle seguenti tematiche[15]:

- Necessità del DPIA;
- Metodologia da adottare nel condurre un DPIA;
- Se condurre un DPIA con le risorse interne ovvero esternalizzandola;
- Quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e le libertà degli interessati;
- Se il DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano in linea con il Regolamento.

Qualora il titolare del trattamento non concordi con le indicazioni fornite dal DPO, è necessario che la documentazione relativa al DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.
In ogni caso, il DPO sorveglia lo svolgimento delle attività di DPIA al fine di rilevare eventuali difformità da quanto previsto dal Regolamento e/o dalle presenti linee guida e funge da punto di contatto con il Garante per la protezione dei dati personali in caso di consultazione preventiva di cui all'articolo 36 del GDPR.
Tutte le Unità Operative, ciascuna per il proprio ambito di competenza, supportano il titolare ed il DPO nello svolgimento delle valutazioni di impatto.
Qualora il trattamento venga eseguito in toto o in parte da un responsabile esterno del trattamento dei dati, quest'ultimo deve assistere il titolare del trattamento nell'esecuzione del DPIA e fornire tutte le informazioni necessarie.

2. PRINCIPI CHE INDIRIZZANO LE ATTIVITÀ DI DPIA

Nella conduzione delle attività di DPIA è necessario garantire la scrupolosa osservanza dei seguenti principi guida:

- i criteri per valutare il rischio e definire la strategia di trattamento devono essere mantenuti aggiornati e devono tenere in opportuna considerazione i valori, gli obiettivi e le risorse della A.O., ma anche il contesto normativo di riferimento;
- la metodologia operativa deve essere mantenuta aggiornata in linea con le evoluzioni normative, tecnologiche e di contesto;
- per le diverse fasi del DPIA devono essere assegnati ruoli e responsabilità specifiche e deve essere garantito un forte commitment sul tema;
- le informazioni raccolte e/o elaborate durante il DPIA devono essere documentate in modo che queste siano agevolmente rintracciabili dalle persone autorizzate ed accessibili solo a queste ultime.
- nello svolgimento del DPIA occorre tenere in debito conto il rispetto di codici di condotta eventualmente approvati, di cui all'articolo 40 del GDPR, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati;
- il programma delle attività di DPIA deve essere formulato con frequenza almeno annuale e comunque rivisto ad ogni cambiamento avente impatti sul contesto o su valutazioni già effettuate;
- successive DPIA devono produrre risultati coerenti, validi e confrontabili fra loro.

3.CONDUZIONE DELL'ATTIVITÀ DI DPIA

Nei paragrafi successivi sono descritte, ad integrazione dei principi generali formulati, le linee guida da adottare per ognuna delle seguenti fasi del DPIA:

1) valutazione preliminare di necessità;
2) preparazione;
3) esecuzione;
4) eventuale consultazione del Garante per la Protezione dei Dati Personali.

3.1 VALUTAZIONE PRELIMINARE DI NECESSITÀ DEL DPIA

In base al Regolamento (art. 35), un DPIA è obbligatoria quando uno specifico trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
In particolare, il Regolamento UE 679/2016 prescrive la valutazione di impatto per i trattamenti che:

- prevedono una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- prevedono il trattamento, su larga scala, di categorie particolari di dati personali (art. 9 GDPR) o di dati relativi a condanne penali e a reati (art. 10 GDPR);
- prevedono la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Lo stesso Regolamento individua anche i seguenti casi per i quali non è invece obbligatorio eseguire una DPIA:

a) Il trattamento appartiene ad una o più fattispecie incluse in un elenco ufficiale di tipologie di trattamenti non soggetti al requisito di DPIA, ai sensi dell'art. 5 paragrafo 1 del GDPR, qualora pubblicato dall'autorità di controllo (Garante per la protezione dei dati personali);
b) Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare (art. 6, par. 1, lettera c) o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1 lettera e), inoltre il trattamento trova nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare è soggetto una base giuridica;
c) se il trattamento non determina un elevato rischio per i diritti e le libertà delle persone fisiche;
d) se la natura, l'ambito, il contesto e gli obiettivi del trattamento sono molto simili ad un trattamento per il quale è stata già svolta la DPIA. In tal caso, i risultati del DPIA possono essere utilizzati per trattamenti simili.

Tutto ciò premesso, per determinare la necessità di eseguire un DPIA, si devono adottare i seguenti criteri decisionali:

- Trattamenti che sottintendono un rischio elevato di violazione dei diritti e delle libertà delle persone fisiche (interessati);
- Trattamenti che non rientrano nei casi di sui ai precedenti punti a) e b) del precedente elenco;
- Trattamenti che rientrano in una o più delle casistiche riportate nella seguente tabella.

Valutazione di profilazione o scoring	Tutti quei trattamenti che prevedono la valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.

Decisioni automatizzate	Tutti quei trattamenti che prevedono un processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente (trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che hanno effetti giuridici o che incidono in modo analogo significativamente su dette persone fisiche).
Monitoraggio sistematico	Tutti quei trattamenti utilizzati per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
Categorie particolari di dati personali e/o dati personali relativi a condanne penali e reati	Tutti quei trattamenti che si riferiscono a categorie particolari di dati personali o dati personali relativi a condanne penali o reati.
Trattamento di dati su larga scala	Tutti i trattamenti che gestiscono dati personali su larga scala, in relazione ai seguenti fattori: 1. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; 2. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; 3. la durata, ovvero la persistenza, dell'attività di trattamento; 4. la portata geografica dell'attività di trattamento.
Combinazioni o raffronto di insieme di dati	Tutti quei trattamenti nei quali è prevista la creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato.
Dati relativi a interessati vulnerabili	Tutti quei trattamenti in cui la tipologia delle informazioni trattate determina uno squilibrio fra interessato e titolare, nel senso della mancanza del potere, in capo al primo, di acconsentire o di opporsi al trattamento. Si inseriscono in questa categoria i dati dei minori, dei dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.).
Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	Tutti quei trattamenti che utilizzano tecnologie o tecniche innovative per la raccolta o l'utilizzo dei dati personali, dato che il livello di conoscenza tecnologica, in un dato momento storico, non è in grado valutare il livello di rischio connesso all'innovazione.
Trattamenti che impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto	Tutti quei trattamenti che impediscono agli interessati di esercitare un diritto, di avvalersi di un servizio o di un contratto, ossia tutti i trattamenti dai quali l'interessato non può esimersi qualora volesse accedere a detto servizio o concludere detto contratto.

Tabella 1 – Criteri per la valutazione di necessità del DPIA

Il titolare può comunque decidere di svolgere un DPIA anche per trattamenti che non soddisfano i suddetti criteri o che li soddisfano solo in parte, ma che da valutazioni preliminari potrebbero determinare rischi elevati.

Pertanto, al momento della definizione del Registro dei Trattamenti o del suo aggiornamento, il titolare valuta, per ogni trattamento, se le sue modalità di attuazione o i dati trattati soddisfano i suddetti criteri, e non si configurano eccezioni (individuate all'interno di elenchi che dovranno essere redatti dalle autorità di controllo degli Stati Membri), registrando la necessità di svolgere il DPIA in apposito campo del Registro.

I criteri per la valutazione di necessità del DPIA possono essere anche utilizzati per la definizione delle priorità di svolgimento delle valutazioni di impatto.

3.2 PREPARAZIONE DEL DPIA

Una volta individuata la necessità di effettuare una o più DPIA, occorre definire:

- l'ambito;

- le risorse (umane ed economiche) necessarie per lo svolgimento delle attività;
- il gruppo di lavoro, identificando i referenti interni ed esterni necessari, tenendo presente i ruoli e le responsabilità definite nel paragrafo 1.5;
- gli stakeholders (coloro che possono trattare dati personali o possono essere impattati dal trattamento: attori coinvolti), consultandoli ove ritenuto opportuno/necessario;
- le priorità per lo svolgimento dei DPIA, qualora il numero sia rilevante in relazione alle risorse disponibili;

Per quanto riguarda l'ambito, la valutazione può riguardare una singola operazione di trattamento dei dati oppure un insieme di trattamenti simili che presentano rischi elevati analoghi. Si può, ad esempio, ricorrere ad una singola DPIA per trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi oppure nel caso si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità.

Per quanto riguarda la pianificazione, coerentemente con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita, il DPIA deve essere effettuato prima possibile nella fase di progettazione del trattamento anche se alcune delle operazioni di trattamento non sono ancora note e, comunque, prima di avviare il trattamento.

Il DPIA deve, infatti, essere considerato come uno strumento atto a contribuire al processo decisionale in materia di trattamento, sia prima che nel corso dello stesso in special modo quando esso è dinamico ed è soggetto a variazioni continue.

3.3 PROCEDURA OPERATIVA PER LA ESECUZIONE DEL DPIA

La fase di esecuzione del DPIA deve seguire i seguenti passi principali:

- definizione del contesto;
- valutazione di necessità e proporzionalità del trattamento;
- valutazione dei rischi;
- definizione delle modalità di trattamento dei rischi;
- redazione e approvazione del rapporto di DPIA.

Durante l'esecuzione ci si può avvalere di strumenti automatici o semi-automatici purché siano conformi alle presenti linee guida.

3.3.1 DEFINIZIONE DEL CONTESTO

La definizione del contesto consiste in una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, nonché degli strumenti a supporto, pertanto, occorre individuare:

- finalità del trattamento;
- categoria di interessati (evidenziando se trattasi di minori);
- se il trattamento soddisfa uno o più criteri tra quelli riportati in Tabella 1;
- responsabilità del trattamento (titolare del trattamento, contitolare del trattamento, RDP, eventuali referenti interni, eventuali Enti terzi/Responsabili del trattamento);
- gli asset (risorse e strumenti) a supporto del trattamento;
- le informazioni (categorie di dati personali) trattate ed il flusso informativo identificando le principali operazioni di trattamento svolte.

Nell'individuare gli asset a supporto, occorre censire e descrivere quelli afferenti alle seguenti principali categorie:

- organizzazione (strutture organizzative preposte al trattamento);
- asset IT on premise (applicativi/data base gestiti presso il Data Center aziendale o presso Data Center di fornitori);

- servizi in Cloud (distinguendo tra: Software as a Service – SaaS, Platform as a Service – PaaS, Infrastructure as a Service – IaaS);
- facility (Data Center, Uffici ove si effettuano le operazioni di trattamento, Archivi preposti alla conservazione di documentazione cartacea contenente dati personali, etc.);
- documentazione cartacea (tipologia di documentazione cartacea contenente dati personali oggetto di trattamento).

Nel descrivere le informazioni trattate, eventualmente aggregandole per categorie omogenee, occorre:

- descrivere la tipologia di dati personali (dati anagrafici, dati sanitari contenuti in referti medici, dati sanitari contenuti in cartella sanitaria, etc.);
- identificare se l'informazione è soggetta a trasferimento verso paesi terzi o organizzazioni internazionali, ed in tal caso identificare il paese terzo o l'organizzazione internazionale e le condizioni per il trasferimento;
- identificare se l'informazione è trattata all'interno del Fascicolo Sanitario Elettronico o Dossier Sanitario Elettronico, attraverso servizi web, app mediche e/o Referto on line;
- definire i termini di cancellazione dell'informazione;
- identificare i destinatari;
- identificare l'Unità Organizzativa preposta al trattamento dell'informazione.

Per quanto riguarda la tipologia di dati occorre specificare se trattasi di:

- categorie particolari di dati personali (art. 9 GDPR);
- dati personali relativi a condanne penali e reati (art. 10 GDPR);
- dati sanitari;
- dati biometrici;
- dati genetici;

Nello svolgimento di tale attività è necessario prendere come riferimento anche le informazioni contenute nel Registro dei Trattamenti aziendale.

3.3.2 VALUTAZIONE DI NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO

Un punto fondamentale del DPIA è la descrizione delle modalità adottate per garantire la necessità e la proporzionalità del trattamento in relazione alle finalità. Nello specifico, occorre:

- illustrare le motivazioni per cui le finalità del trattamento sono specifiche, esplicite e legittime;
- presentare le basi giuridiche del trattamento (ad esempio: consenso dell'interessato, esecuzione di misure precontrattuali, esecuzione di un contratto, adempimenti di obblighi legali del titolare, salvaguardia di interessi vitali, esercizio di un interesse pubblico, legittimo interesse del titolare);
- spiegare perché i dati raccolti sono necessari per le finalità del trattamento;
- descrivere quali sono le misure adottate per assicurare l'accuratezza dei dati;
- spiegare perché la durata dell'archiviazione è giustificata da requisiti legali e/o necessità di trattamento.

3.3.3 VALUTAZIONE DEI RISCHI

Definito il contesto e la valutazione di necessità e proporzionalità del trattamento occorre passare alla valutazione dei rischi. Un "rischio" è uno scenario che descrive un evento e le sue conseguenze. La valutazione dei rischi deve identificare gli "scenari di rischio" e, per ognuno di essi, stimare il "livello di rischio effettivo" per i diritti e le libertà dell'interessato connesso al trattamento in esame con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento.

I principali scenari di rischio da prendere in considerazione sono:

- perdita di riservatezza - accesso illegittimo ai dati personali;
- perdita di integrità - modifica non autorizzata dei dati personali;

- perdita di disponibilità - perdita, furto, cancellazione non autorizzata di dati personali.

Il livello di rischio è inteso come la probabilità che una minaccia possa sfruttare le vulnerabilità di un asset o di un gruppo di asset a supporto del trattamento e quindi causare un danno all'interessato.
Il criterio utilizzato per la conduzione dell'analisi dei rischi, derivato dallo standard ISO/IEC 27001/2017, dalla norma DS/ISO/IEC 29134 (Annex A) e dal documento "Privacy Impact Assessment" della Commission nationale de l'informatique et des libertés 2015, si basa sulla correlazione fra la gravità (**G**) di un rischio (definita in relazione all'ampiezza degli impatti potenziali sugli interessati, tenendo conto delle misure esistenti) e la probabilità (**P**) di accadimento dell'evento minaccia che provoca il danno (definita in relazione alle vulnerabilità dei supporti interessati e alla capacità delle fonti di rischio di sfruttarle, tenendo conto delle misure esistenti). A tal riguardo, si è definito l'indice o fattore di rischio R come funzione della probabilità di accadimento delle minacce e l'Indice di gravità del danno:

R = f (G, P).

La fase di valutazione del rischio deve prevedere le seguenti sotto-fasi:

- analisi degli impatti sui diritti e le libertà dell'interessato e della probabilità di accadimento degli scenari di impatto;
- analisi delle minacce applicabili al contesto di trattamento;
- definizione delle misure necessarie a contrastare le minacce identificate;
- valutazione della probabilità di accadimento delle minacce determinata secondo un criterio relazionale inversamente proporzionale al livello di efficienza delle misure identificate nel contrastarle, **efficienza determinata in funzione dell'applicabilità dei controlli a sostegno delle misure definite ed alla robustezza degli stessi**;
- valutazione del rischio effettivo.

Al fine di valutare al meglio l'analisi delle minacce applicabili al contesto del trattamento, particolare attenzione deve essere posta qualora il titolare del trattamento ricorra a responsabili del trattamento che, ai sensi dell'art. 28 del Regolamento (UE) 2016/679 (GDPR), devono presentare garanzie sufficienti in modo tale che il trattamento soddisfi i requisiti previsti dalla normativa vigente e garantisca la tutela dei diritti dell'interessato. Nello specifico il GDPR prevede che ogni responsabile e i suoi eventuali sub-responsabili per il trattamento dei dati - in relazione alle specifiche attività di trattamento svolte per conto del Titolare - per garantire, in conformità all'art. 32 del GDPR, un livello di sicurezza adeguato devono mettere in atto e mantenere in essere appropriate misure tecniche e organizzative, controlli interni e processi di sicurezza intesi a proteggere i dati da perdita accidentale, distruzione o alterazione, da accessi o da diffusione non autorizzati o da illegale distruzione.
Pertanto, atteso che tra i compiti del responsabile, ai sensi del citato art. 28 par. 3 lett. h), vi è quello di mettere a disposizione del Titolare tutte le informazioni per dimostrare il rispetto degli obblighi e delle disposizioni previste dal su citato Regolamento è necessario che, tra le suddette informazioni, vi sia il presupposto di una eventuale DPIA condotta dal Responsabile o, in alternativa, della disponibilità, nel caso di utilizzo di strumenti informatici o telematici, delle rispettive certificazioni di conformità al GDPR, validate dai preposti organismi e agenzie nazionali ed europei.

3.3.3.1 ANALISI DEGLI IMPATTI SUI DIRITTI E LE LIBERTÀ DELL'INTERESSATO

L'analisi degli impatti potenziali sui diritti e le libertà dell'interessato deve essere condotta considerando le seguenti dimensioni di analisi:

- scenario di perdita di riservatezza, integrità e disponibilità;
- categoria di impatto come di seguito:

- ✓ impatto fisico: tutti i danni fisici che gli interessati potrebbero subire a seguito di violazioni dei dati personali;
- ✓ impatto materiale: tutti i danni materiali che gli interessati potrebbero subire a seguito di violazioni dei dati personali;
- ✓ impatto psicologico: tutti i danni psicologici che gli interessati potrebbero subire a seguito di violazioni dei dati personali.

Per ogni scenario e per ogni categoria d'impatto occorre identificare un "livello di impatto (**G**)", espresso secondo una scala di valutazione qualitativa discreta (N.A.= Non Applicabile, 1=Trascurabile, 2=Limitato, 3=Significativo, 4=Massimo), descritta nella seguente tabella.

LIVELLI DI IMPATTO PER CATEGORIA				
Livello		**Impatto fisico**	**Impatto materiale**	**Impatto psicologico**
N.A.	**Non Applicabile**	Gli interessati non subirebbero alcun impatto.	Gli interessati non subirebbero alcun impatto.	Gli interessati non subirebbero alcun impatto.
1	**Trascurabile**	Gli interessati potrebbero incontrare qualche inconveniente fisico, superabile senza difficoltà (ad es. mal di testa).	Gli interessati potrebbero incontrare qualche inconveniente materiale, superabile senza difficoltà (ad esempio perdita di tempo).	Gli interessati potrebbero incontrare qualche inconveniente psicologico, superabile senza difficoltà (ad esempio semplice fastidio).
2	**Limitato**	Gli interessati potrebbero sperimentare inconvenienti fisici superabili nonostante alcune difficoltà (ad es. malattia lieve).	Gli interessati potrebbero avere inconvenienti materiali, superabili nonostante alcune difficoltà (ad esempio: costi aggiuntivi o mancato accesso ad un servizio).	Gli interessati potrebbero avere inconvenienti psicologici, superabili nonostante alcune difficoltà (ad esempio disturbo psicologico minore ma oggettivo, intimidazione sui social network).
3	**Significativo**	Gli interessati potrebbero subire conseguenze fisiche significative, che dovrebbero essere in grado di superare, ma con notevoli difficoltà (ad esempio malattia a lungo termine).	Gli interessati potrebbero subire conseguenze materiali significative, che dovrebbero essere in grado di superare, ma con notevoli difficoltà (ad esempio perdita di opportunità non ricorrenti).	Gli interessati potrebbero subire conseguenze psicologiche significative, che dovrebbero essere in grado di superare, ma con notevoli difficoltà (ad esempio significativo disturbo psicologico, esposizione a ricatti, cyberbullismo)
4	**Massimo**	Gli interessati potrebbero sperimentare gravi conseguenze fisiche, anche irrimediabili, che potrebbero non superare (ad esempio malattie permanenti o decesso).	Gli interessati potrebbero subire gravi conseguenze materiali, anche irrimediabili, che potrebbero non superare (ad esempio indebitamento ingente, impossibilità di lavorare)	Gli interessati potrebbero subire gravi conseguenze psicologiche, anche irrimediabili, che potrebbero non superare (ad esempio perdita di legami familiari, disturbo psicologico permanente o a lungo termine).

Figura 1 – Livelli di impatto per categoria

3.3.3.2 ANALISI DELLE MINACCE APPLICABILI

L'analisi delle minacce deve essere basata su un "catalogo di minacce" derivanti da standard e best practices di riferimento, ognuna delle quali è caratterizzata da:

- uno o più scenari di rischio che la minaccia può determinare (accesso illegittimo ai dati, modifica non autorizzata dei dati, perdita dei dati);
- la tipologia di asset sulla quale può agire;
- uno o più agenti di minaccia che possono attuarla (fonti umane interne/esterne o fonti non umane).

Tra queste minacce occorre identificare quelle applicabili allo specifico trattamento in esame.

3.3.3.3 VALUTAZIONE DELLA PROBABILITÀ DI ACCADIMENTO DELLE MINACCE

Per ogni minaccia identificata occorre valutare la probabilità (**P**) di accadimento espressa su una scala di valutazione qualitativa discreta di 4 livelli (Trascurabile, Limitata, Significativa, Massima) prendendo in considerazione i tre scenari di rischio relativi alla perdita di riservatezza, integrità e disponibilità.

A tal fine, la probabilità viene derivata secondo un principio inversamente proporzionale al livello di efficienza delle misure predisposte per contrastarle e quindi dal livello di attuazione dei controlli posti in essere a protezione del trattamento relativamente ai seguenti ambiti:

- requisiti del Regolamento;
- requisiti derivanti dalla normativa e dai pronunciamenti del Garante per la protezione dei dati personali;
- requisiti derivanti da standard e best practices internazionali di sicurezza e privacy.

Nello specifico per ogni minaccia identificata sono individuate le misure ritenute necessarie a contrastarla e per ogni misura l'insieme dei controlli che la costituiscono.

Ciò richiede che i controlli siano strutturati in "classi funzionali", ciascuna delle quali individua funzionalità omogenee di sicurezza e privacy in grado di contrastare le minacce applicabili, ovvero la misura che esse configurano. Ogni controllo inoltre deve essere caratterizzato da un livello di robustezza su una scala ordinale a tre valori; il livello ordinale e, quindi, cardinale di implementazione "as is" dei controlli deve essere valutato, sia tramite intervista che autovalutazione, utilizzando la seguente nomenclatura convenzionale:

- "Si": il controllo è coperto da una o più contromisure pienamente e correttamente applicate (100%);
- "Parziale": una o più contromisure coprono solo parzialmente il controllo espresso (più del 50% ma non ancora il 100%);
- "No": il controllo non è coperto da alcuna contromisura oppure è solo parzialmente implementato (<50%);
- "N.A.": il controllo non è applicabile al contesto di riferimento.

Come già detto la probabilità di accadimento di una minaccia è inversamente proporzionale alla efficienza delle misure predisposte a contrastarla e quindi alla copertura e alla robustezza dell'insieme dei controlli a sostegno delle suddette misure.

In funzione della esistenza o meno dei controlli e del livello di robustezza di ognuno di essi, si determina in un range da 0 a 100 l'efficienza (E) della misura in oggetto (100 = massima **e**fficienza**)** e di conseguenza la probabilità (P) di accadimento della minaccia in un range da 0 a 100: P= (100 – E; 0 = probabilità nulla).

La scala di valutazione qualitativa discreta secondo 4 livelli della probabilità di accadimento delle minacce si ottiene rapportando i valori percentuali secondo il seguente criterio:

0-25% = 1 Trascurabile; 25-50% = 2 Limitata; 26-75% = 3 Significativa; 75-100% = Massima.

3.3.3.4 VALUTAZIONE DEL RISCHIO EFFETTIVO

Il rischio effettivo per i diritti e le libertà degli interessati connesso al trattamento in esame deve essere valutato per ogni scenario di rischio e per ogni minaccia, in base a:

- I valori di impatto rilevati, pesati con la probabilità degli scenari di impatto (cfr. par. 3.3.3.1);
- La probabilità di accadimento delle minacce (cfr. par. 3.3.3.3).

I livelli di rischio rilevati devono essere espressi secondo una scala di valutazione qualitativa discreta a 4 livelli (1=Trascurabile, 2=Limitato, 3=Significativo, 4=Massimo), applicando i criteri espressi dalla matrice di rischio rappresentata nella figura seguente.

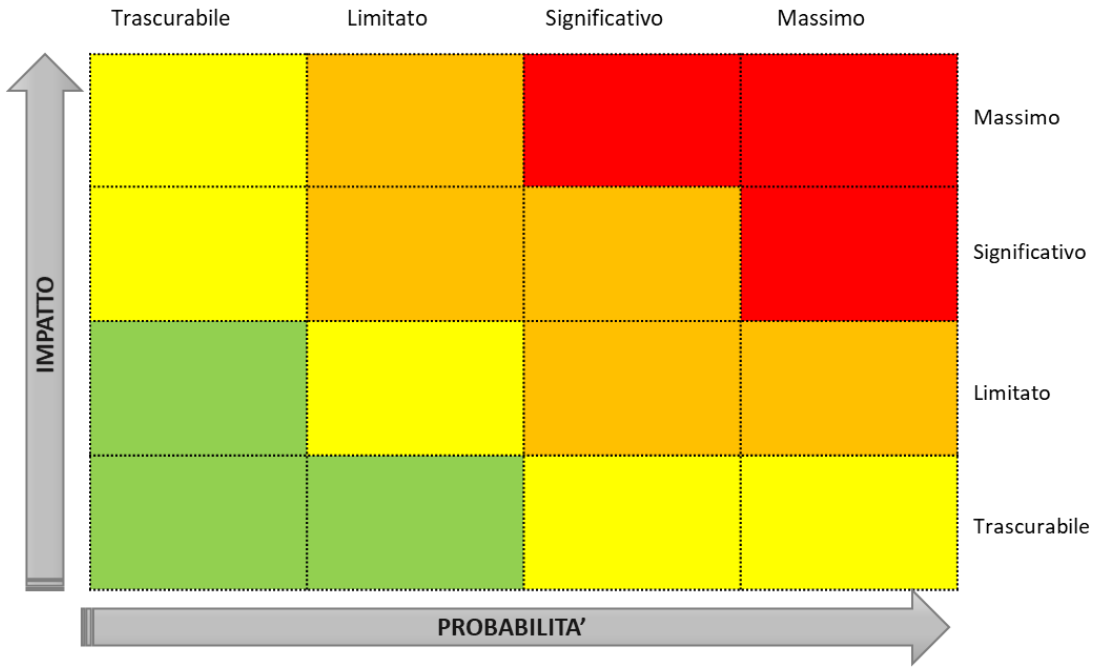

Figura 2 – Matrice livello di rischio

3.3.4 DEFINIZIONE DELLE MODALITÀ DI TRATTAMENTO DEI RISCHI

A conclusione delle attività fin qui descritte ed analizzate occorre definire ed individuare la strategia di gestione del rischio per i diritti e le libertà degli interessati.
Essa scaturisce dalla identificazione degli asset tecnici, organizzativi e logistici che presentano criticità elevate e, pertanto, controlli non adeguati a contrastare le eventuali minacce per il trattamento dei dati a cui sono rivolti. Tali asset, o meglio i relativi controlli a sostegno, vanno formalmente catalogati in documenti di analisi sulla base dei quali dovranno essere successivamente formulati, quali parte integrante della documentazione a corredo del DPIA, i piani di sicurezza/azione temporali e strutturali relativi agli interventi da mettere in atto per la implementazione o il potenziamento delle misure necessarie a raggiungere i livelli di sicurezza prefissati. Tali piani di azione sono sottoposti all'attenzione del Titolare che, valutato il livello di rischio effettivo, identifica quale tra le seguenti opzioni per il trattamento del rischio ritiene di adottare:

- Evitare il rischio, rinunciando, ad esempio, alle attività che lo generano;
- Condividere il rischio con un'altra parte in grado di gestirlo in modo più efficace, come ad esempio assicuratori e fornitori;
- Ridurre il rischio ad un livello ritenuto accettabile, attraverso l'implementazione delle contromisure necessarie al raggiungimento di tale soglia;
- Accettare il rischio se non si ritiene opportuna alcuna delle precedenti opzioni.

In tal senso, la A.O., in persona del titolare, adotta, in funzione del livello di rischio effettivo riscontrato, l'approccio sintetizzato nella seguente tabella:

Livello di rischio effettivo		Strategia di trattamento del rischio			
		Evitare	Condividere	Ridurre	Accettare
4	Massimo	x	x	x	
3	Significativo	x	x	x	
2	Limitato			x	x
1	Trascurabile				x

Come si evince dalla tabella, la soglia di accettabilità del rischio è stabilita ad un livello di rischio "Limitato", conseguentemente tutti gli altri casi, richiedono un trattamento al fine di ridurlo, trasferirlo o evitarlo. In ogni caso, anche quando il livello di rischio effettivo risulta limitato, la Struttura Sanitaria deve valutare l'opportunità, in termini di costi, di ridurre lo stesso.
In generale, nel caso in cui si optasse per il trattamento di riduzione, il rischio di riferimento sarà quello ritenuto accettabile dal titolare.
Quando il livello di rischio risulta essere Massimo o Significativo, è consigliabile prendere in considerazione:

- L'opzione evitare, in caso di gravi violazioni di legge o di pericolo per le incolumità delle persone;
- L'opzione condividere, quando scartata l'opzione precedente, il costo di tale condivisione (in termini di tempi e costi) è minore di quello associato all'implementazione delle contromisure di sicurezza per la riduzione del rischio;
- L'opzione ridurre, anche congiuntamente a quella di condividere, quando il titolare ritiene opportuno l'implementazione delle contromisure necessarie al raggiungimento di un livello di soglia ritenuto accettabile.

Se la strategia di trattamento approvata prevede la riduzione, occorre valutare il livello di rischio residuo che si raggiungerà a valle della applicazione della strategia scelta ed i requisiti da attuare per il suo conseguimento, che saranno successivamente dettagliati all'interno di specifici piani di sicurezza. In base al livello di rischio residuo ed ai tempi previsti per il suo raggiungimento, il titolare valuta la necessità di consultare il Garante (paragrafo 3.4).
In ogni caso, a prescindere dal livello di rischio effettivo valutato, occorre definire una strategia di trattamento mirata a soddisfare tutti i requisiti normativi, non coperti o parzialmente coperti.

3.3.5 REDAZIONE E APPROVAZIONE DEL RAPPORTO DI DPIA

Tutto quanto fin qui indicato deve essere racchiuso in un rapporto generale del DPIA con relativo piano di sicurezza che ne costituisce parte integrante; tale rapporto deve contenere almeno i seguenti argomenti (art. 37 paragrafo 7 GDPR):

- Descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
- Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- Risultati della valutazione dei rischi per i diritti e le libertà degli interessati;
- Misure previste per affrontare i rischi e dimostrare la conformità al Regolamento.

Il documento deve essere approvato dal titolare e riportare i nominativi di chi ha contribuito alla redazione ed alla revisione del documento (DPO, responsabili del trattamento, etc.).
Il titolare può prendere in considerazione, in taluni casi, la pubblicazione di alcune parti del rapporto di DPIA. Il documento pubblicato non deve, comunque, contenere l'intera valutazione, soprattutto qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza o divulgare informazioni riservate. In queste circostanze, la versione pubblicata può consistere soltanto in una sintesi delle principali

risultanze della DPIA, nella conclusione o addirittura soltanto in una dichiarazione nella quale si afferma che la DPIA è stato condotta.

3.4 EVENTUALE CONSULTAZIONE PREVENTIVA DEL GARANTE

In linea con le prescrizioni del Regolamento (cfr. art. 35), prima di procedere al trattamento, il Titolare deve consultare il Garante per la protezione dei dati personali qualora il DPIA indichi che il trattamento potrebbe presentare un rischio elevato in assenza di misure adeguate (rischio residuo elevato).
In tal caso occorre comunicare al Garante le seguenti informazioni:

- Le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento;
- Le finalità e i mezzi del trattamento previsto;
- Le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del Regolamento;
- I dati di contatto del responsabile della protezione dei dati;
- La valutazione d'impatto sulla protezione dei dati;
- Ogni altra informazione richiesta dal Garante.

Il Garante, se ritiene che il trattamento violi il Regolamento, in particolare qualora il titolare non abbia identificato o attenuato sufficientemente il rischio, fornisce, entro un termine prestabilito dal ricevimento della richiesta di consultazione, un parere scritto al titolare e, ove necessario, al responsabile del trattamento.
A fronte di tale parere, il titolare deve pianificare tutte le attività necessarie a recepire quanto segnalato dal Garante.

4.NORME FINALI E DI RINVIO

La presente procedura è stata adottata dal Titolare del trattamento, su proposta della U.O.S.I.D Controllo Interno, d'intesa con il DPO. Essa entra in vigore il giorno successivo alla sua approvazione. Il suo contenuto è soggetto ad aggiornamento periodico.

Tutte le Unità Operative sono invitate a coinvolgere la UOSID Controllo Interno e Tutela della Privacy e/o il DPO su eventuali nuove iniziative promosse all'interno della Azienda che prevedano l'utilizzo di nuove tecnologie e che possano determinare un trattamento rilevante di dati personali al fine di valutare adeguatamente e congiuntamente se sia richiesta o meno l'attivazione del procedimento di DPIA.

Per quanto non espressamente previsto dal presente regolamento, si applicano le disposizioni di legge e i provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali che regolamentano la materia in oggetto.