LINEE GUIDA PER LA CONDUZIONE DELLE ATTIVITÀ DI DATA PROTECTION IMPACT ASSESSMENT

LINEE GUIDA PER LA CONDUZIONE DELLE ATTIVITÀ DI DATA PROTECTION IMPACT ASSESSMENT

Sommario

CAPITOLO 1 Generalità 3

1.1 Finalità del documento 3

1.2 Ambito di applicazione 4

1.3 Documenti di riferimento 4

1.4 Acronimi e definizioni 5

1.5 Ruoli e responsabilità 8

CAPITOLO 2 Principi che indirizzano le attività di DPIA 9

CAPITOLO 3 Conduzione delle attività di DPIA 10

3.1 Valutazione preliminare di necessità della DPIA 10

3.2 Preparazione della DPIA 13

3.3 Procedura Operativa Per la Esecuzione del DPIA 14

3.3.1 Definizione del contesto.....14

3.3.2 Valutazione di necessità e proporzionalità del trattamento 15

3.3.3 Valutazione dei rischi.....16

3.3.3.1 Analisi degli impatti sui diritti e le libertà dell'interessato 17

3.3.3.2 Analisi delle minacce applicabili 19

3.3.3.3 Valutazione della probabilità di accadimento delle minacce 19

3.3.3.4 Valutazione del rischio effettivo 21

3.3.4 Definizione delle modalità di trattamento dei rischi 22

3.3.5 Redazione e approvazione del rapporto di DPIA.....23

3.4 Eventuale consultazione preventiva del Garante 24

CAPITOLO 4 Norme finali e di rinvio 25

CAPITOLO 1

GENERALITÀ

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, di seguito sinteticamente indicato come “Regolamento” o “GDPR”, relativamente agli obblighi dei Titolari (cfr. art 35), nell’ambito della gestione del rischio correlato al trattamento di dati personali.

La DPIA è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per ridurli.

La valutazione d'impatto sulla protezione dei dati è uno strumento importante di responsabilizzazione in quanto sostiene il titolare del trattamento non soltanto nel rispettare i requisiti del Regolamento, ma anche nel dimostrare che sono state adottate misure appropriate.

La mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa (articolo 35, paragrafi 1, 3 e 4), l'esecuzione in maniera errata di detta valutazione (articolo 35, paragrafi 2 e da 7 a 9) oppure la mancata consultazione del Garante per la protezione dei dati personali laddove richiesto (articolo 36, paragrafo 3, lettera e), possono comportare 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

Questo documento espone le linee guida per la conduzione delle attività di Data Protection Impact Assessment attuate dalla Struttura Sanitaria 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 a quei trattamenti della Struttura Sanitaria che il Titolare, confrontatosi con il DPO, ritiene dover sottoporre ad una DPIA e sono da ritenersi estese 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€ "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, Febbraio2018

[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 ProtectionOfficer./ 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	Infrastructureas 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 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 e supportato dal Responsabile della Protezione dei Dati (RDP/DPO) con il quale si consultano chiedendo, se necessario, un parere in merito al DPIA e di sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento.

In particolare, il Titolare si consulta con il RPD sulle seguenti tematiche[15]:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la 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 la 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 RPD, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.

In ogni caso, il RDP 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 UO della Struttura Sanitaria, ognuno per il proprio ambito di competenza in relazione al trattamento, incluse la UOC Privacy – Trasparenza e Integrità ,la UOC che si occupa della gestione dei sistemi IT e l'UOC che si occupa di apparecchiature elettromedicali ,supportano il titolare ed il RDP 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.

CAPITOLO 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 Struttura Sanitaria, ma anche il contesto normativo di riferimento;
- successive DPIA devono produrre risultati coerenti, validi e confrontabili fra loro;
- per le diverse fasi della DPIA devono essere assegnati ruoli e responsabilità specifiche e deve essere garantito un forte commitment sul tema;
- la metodologia operativa della DPIA deve essere mantenuta aggiornata in linea con le evoluzioni normative, tecnologiche e di contesto;
- 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;
- 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;
- le informazioni raccolte e/o elaborate durante la DPIA devono essere documentate in modo che queste siano agevolmente rintracciabili dalle persone autorizzate ed accessibili solo a queste ultime.

CAPITOLO 3

CONDUZIONE DELLE ATTIVITÀ DI DPIA

Nei paragrafi successivi sono descritte le linee guida da adottare per ognuna delle seguenti fasi della DPIA:

1. valutazione preliminare di necessità della DPIA;
2. preparazione della DPIA;
3. esecuzione della DPIA;
4. eventuale consultazione del Garante per la protezione dei dati personali.

3.1 VALUTAZIONE PRELIMINARE DI NECESSITÀ DELLA DPIA

In base al Regolamento (art. 35), una DPIA è obbligatoria quando il 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.

In particolare, il Regolamento 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 tipologie incluse in un elenco ufficiale di tipologie di trattamenti non soggetti al requisito di DPIA ai sensi del paragrafo 1 del art. 5 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 del trattamento (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, tale diritto disciplina il trattamento specifico o l'insieme di trattamenti in questione, ed è già stato effettuato una DPIA nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

Tutto ciò premesso, per determinare la necessità di eseguire una DPIA, la Struttura Sanitaria deve 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 pocesso 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 ed 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 della DPIA

Il titolare può comunque decidere di svolgere una 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 la DPIA in apposito campo del Registro.
I criteri per la valutazione di necessità della DPIA possono essere anche utilizzati per la definizione delle priorità di svolgimento delle valutazioni di impatto.

3.2 PREPARAZIONE DELLA DPIA

Una volta individuata la necessità di effettuare una o più PDIA, occorre definire:
- l'ambito della DPIA;
- 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 0;
- 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 delle DPIA, qualora il numero sia rilevante in relazione alle risorse disponibili;

Per quanto riguarda l'ambito, una DPIA 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, la DPIA deve essere effettuata 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.
La DPIA deve infatti essere considerata come uno strumento atto a contribuire al processo decisionale in materia di trattamento, sia prima del trattamento, sia nel corso del trattamento, soprattutto quando esso è dinamico ed è soggetto a variazioni continue.

3.3 PROCEDURA OPERATIVA PER LA ESECUZIONE DEL DPIA

La fase di esecuzione della 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 piano di azione della DPIA.

Durante l'esecuzione della DPIA la Struttura Sanitaria può avvalersi di strumenti automatici o semiautomatici purché siano conformi alle presenti linee guida.

3.3.1 DEFINIZIONE DEL CONTESTO

La definizione del contesto deve consentire 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 della Struttura Sanitaria o presso Data Center di fornitori);

- servizi in Cloud (distinguendo tra: Software as a Service – SaaS, Platform as a Service – PaaS, Infrastructureas 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 predisposto della Struttura Sanitaria.

3.3.2 VALUTAZIONE DI NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO

Un punto fondamentale della DPIA è la descrizione delle modalità adottate per garantire la necessità e la proporzionalità del trattamento in relazione alle finalità. Nello specifico, occorre:
- illustrare perché 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 con alcuni adattamenti dallo standard ISO/IEC 27001:2017e dalla Norma DS/ISO/IEC 29134:2017 (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(P, G)

In tale ottica la valutazione del livello di rischio deve pertanto essere stimato in termini di:

- "impatto/gravità (**G**)" potenziale sull'interessato nel caso in cui si concretizzi ognuno degli scenari di rischio e relativa probabilità di accadimento dello scenario di impatto;
- "probabilità delle minacce (**P**)" che dipende principalmente dal livello di vulnerabilità delle risorse di supporto e dalle minacce in grado di sfruttarle.

A tal fine 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 definiteed alla

robustezza degli stessi;

- valutazione del rischio effettivo.

I principi dettagliati per lo svolgimento delle suddette attività sono descritti nei successivi paragrafi.

Al fine di valutare al meglio l'analisi delle minacce applicabili al contesto del trattamento, particolare attenzione deve essere applicata qualora il titolare del trattamento, affinché questo venga effettuato, 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 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. Le categorie di impatto devono includere le seguenti:
- 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 come applicabile al trattamento in esame, 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 applicabile 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 “asis” 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.

Nello specifico, sulla base dei requisiti derivanti dalla normativa e dai pronunciamenti del Garante per la protezione dei dati personali, dei requisiti derivanti da standard e *best practices* internazionali di sicurezza e privacy e dei riferimenti di cui al precedente punto 1.3, si identificano i controlli a sostegno della misura desiderata ed in funzione della esistenza o meno e del livello di robustezza di ognuno di essi, si determina in un range da 0 a 100l’efficienza (E) della misura in oggetto (100 = massima efficienza,) 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. 0);
- la probabilità di accadimento delle minacce (cfr. par. 0).

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.

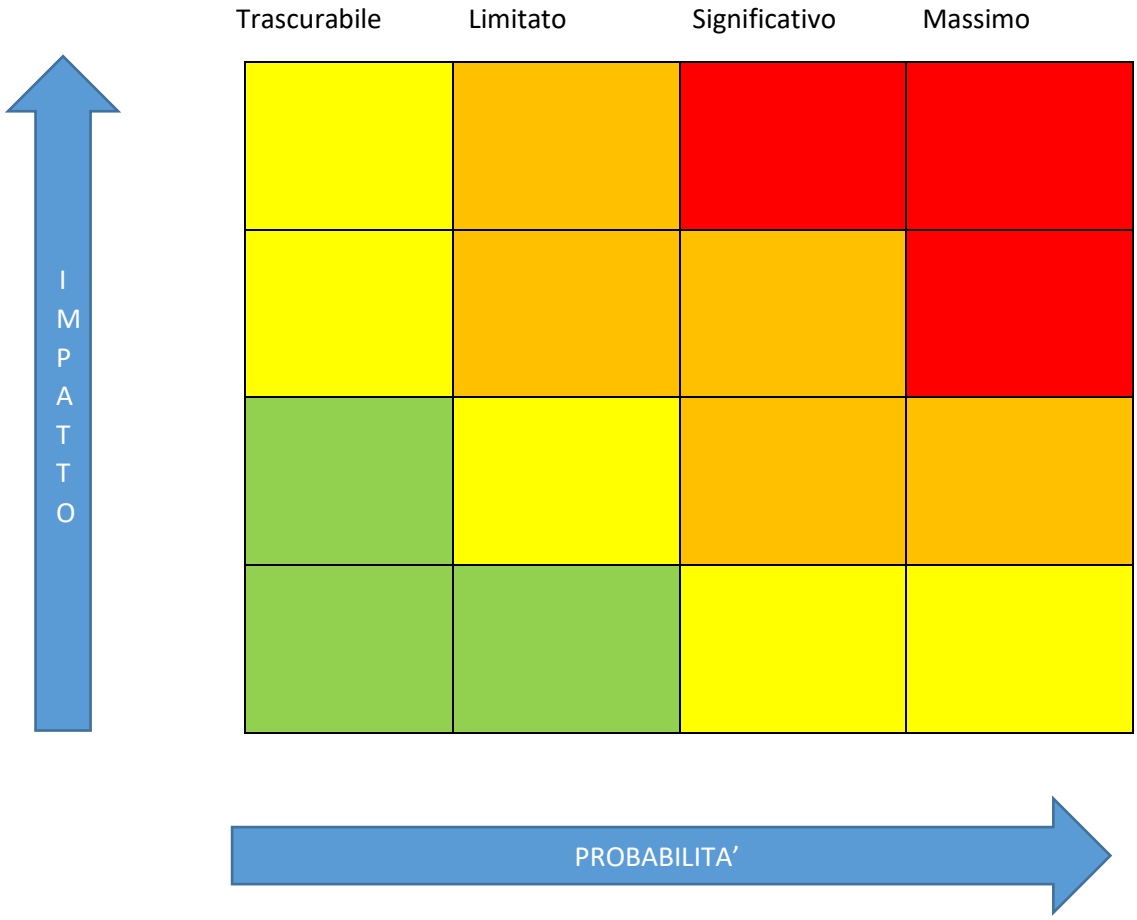

Figura 2- Matrice livello di rischio

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 della Struttura Sanitaria.

Tale strategia 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 essi 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 della DPIA, i piani di sicurezza/azione temporali e strutturali relativi alla pianificazione degli 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 vanno poi 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 gestire il rischio 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 Struttura Sanitaria, nella 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 i costi di una eventuale riduzione, rispetto ai benefici per l'interessato e quindi valutare l'opportunità di ridurre tale rischio.

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.

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/PIANO DI AZIONE

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

- la descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
- la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- i risultati della valutazione dei rischi per i diritti e le libertà degli interessati in linea con l'art. 5 par. 1 del Regolamento;
- le misure previste per affrontare i rischi e dimostrare la conformità al Regolamento;
- la descrizione della strategia di gestione del rischio che si intende adottare.

Il documento deve essere approvato dal titolare e riportare i nominativi di chi ha contribuito alla redazione ed alla revisione del documento (RDP, 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 del DPIA, nella conclusione del DPIA o addirittura soltanto in una dichiarazione nella quale si afferma che la DPIA è stata condotta.

3.4 EVENTUALE CONSULTAZIONE PREVENTIVA DEL GARANTE

In linea con le prescrizioni del Regolamento (cfr. art. 35), il titolare, prima di procedere al trattamento, deve Consultare il Garante per la protezione dei dati personali qualora la DPIA indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio (rischio residuo elevato).

In caso di consultazione, il titolare del trattamento deve comunicare al Garante le seguenti informazioni:

- ove applicabile, 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 del Trattamento non abbia identificato o attenuato sufficientemente il rischio, fornisce, entro un termine prestabilito, dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento.

A fronte di tale parere, il titolare deve pianificare tutte le attività necessarie a recepire quanto segnalato dal Garante.

CAPITOLO 4

NORME FINALI E DI RINVIO

4.1 DISPOSIZIONI FINALI

La presente procedura è stata adottata dal Titolare del trattamento.

Suddetta procedura entra in vigore il giorno successivo alla sua approvazione. Il suo contenuto è soggetto ad aggiornamento periodico.

La sua pubblicizzazione, secondo norma, avverrà attraverso il sito aziendale.

attraverso il sito aziendale.

È fatto obbligo a chiunque spetti di osservarlo.

4.2 NORMA DI RINVIO

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.