Allegato 7 – Descrizione delle fasi della DPIA

Il processo di DPIA

La normativa in materia e le indicazioni del WP29 ((Working Party article 29 o WP29, previsto dall'art. 29 della direttiva europea 95/46)[1] non indicano un modello specifico da adottare, tuttavia fornisce i framework di DPIA realizzati dalle diverse autorità nazionali di controllo.

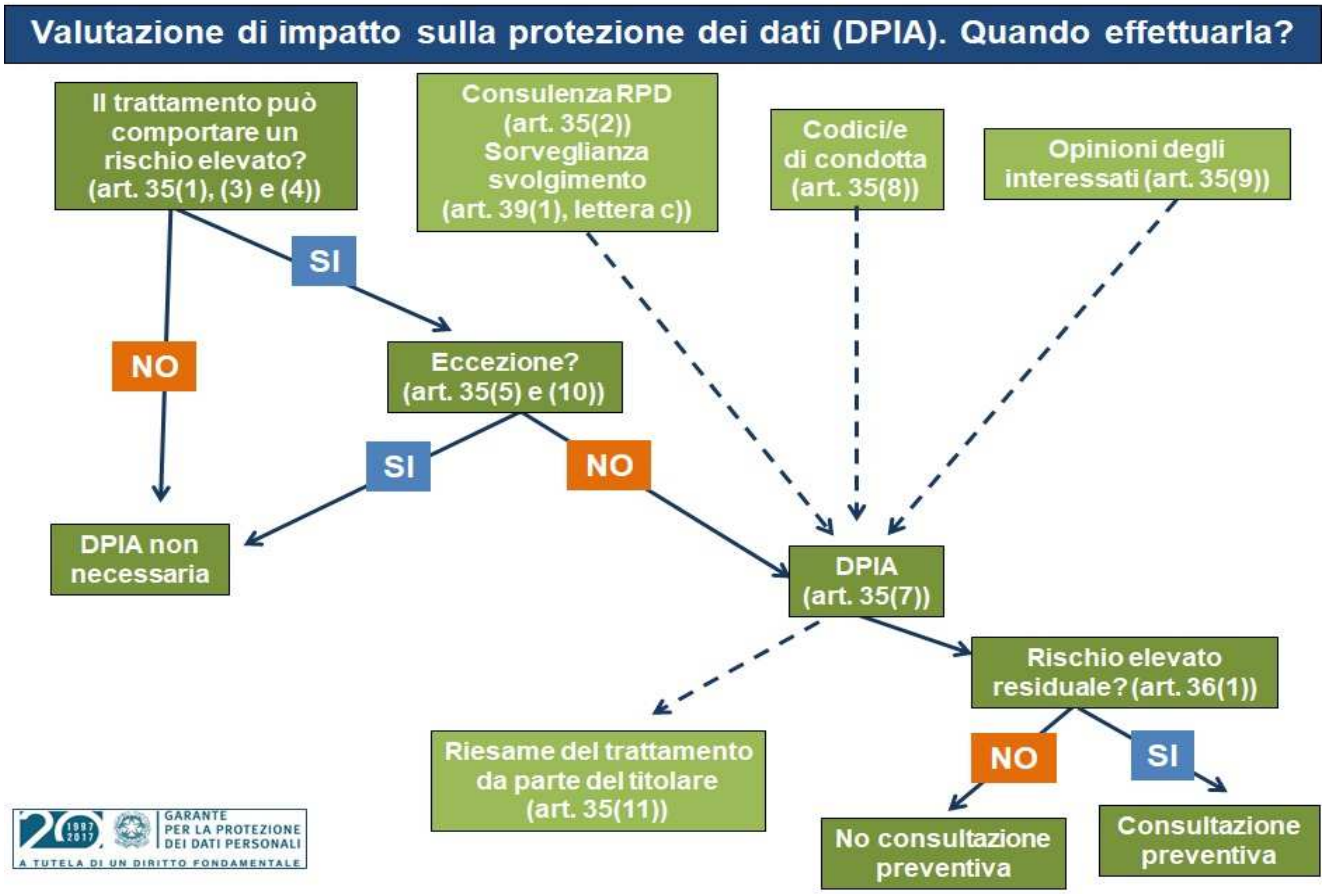
Autorità nazionale	Stato	Framework
CNIL - Commission Nationale de l'nformatique et des Libertés	Francia	https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-pia
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	Germania	https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf
Agencia española de protección de datos	Spagna	https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf
Information Commissioner's Office	UK	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

La ISO ha pubblicato una linea guida per effettuare un DPIA (ISO/IEC 29134), definendo un processo per la privacy impact assessment con una struttura ed i relativi contenuti del report del DPIA (a supporto del principio di accountability).
La DPIA consente di identificare le singole misure di sicurezza che è necessario adottare per contrastare le minacce rilevate. Tra i diversi modelli e strumenti disponibili dovrebbero essere anche richiamate le linee guida dell'Enisa.
Altresì per la valutazione del rischio privacy possono essere richiamati gli standard della ISO 31000 che vengono anche citati nel piano nazionale anticorruzione L. 190/2012.
Le riferite linee guida sono rilevanti perché fissano uno standard prestabilito per gli step da seguire nell'esecuzione del processo.

[1] Il WP29, col nuovo regolamento europeo, è stato sostituito dall'European Data Protection Board, o Comitato europeo per la protezione dei dati ed è il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati.

Descrizione delle fasi di processo

Il WP29 ha schematizzato efficacemente, nelle recenti linee guida2, i principi base della DPIA:



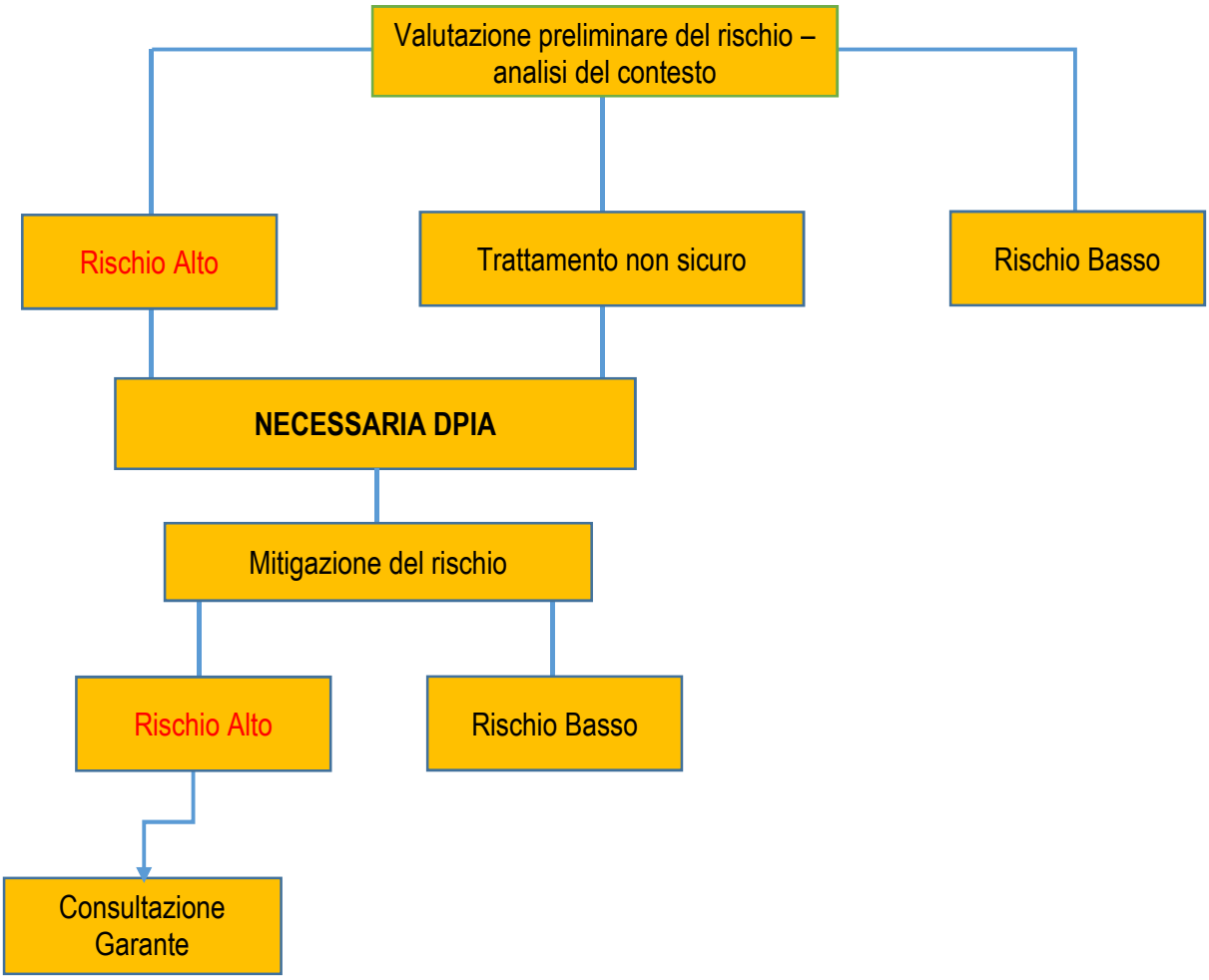
Le fasi di processo per realizzare una DPIA sono più specificatamente dettagliate nel corso dei paragrafi seguenti.

[2] Le "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato", realizzate ai fini del regolamento (UE) 2016/679, sono state adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017. Esse sono state stilate dal "Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali", è stato istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995. Le stesse linee guida possono essere consultate al link http://www.interlex.it/2testi/autorit/wp248dpia.pdf.

Fase 1 - Valutare la necessità di condurre un'attività di DPIA

La fase 1 ha come obiettivo la necessità di stabilire se rispetto ad una determinata attività ricorra o meno la necessità di effettuare una Valutazione di Impatto, anche alla luce di quanto stabilito dal Garante per la Protezione dei dati personali[3].

Si tratta di effettuare una analisi del contesto e, come indicato nel flusso di processo, di condurre una prima analisi che consenta di identificare quali rischi possono manifestarsi nell'esecuzione di un trattamento o quali cause possono renderlo insicuro.



[3] Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018 [9058979]
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979

Tale valutazione dovrà essere condotta alla luce delle indicazioni metodologiche del GDPR, delle Linee guida WP29 e delle diverse metodologie che si possono adottare. L'art. 35, paragrafo 3, GDPR richiede la Valutazione d'Impatto sulla protezione dei dati nei seguenti casi:

- ✓ 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;
- ✓ il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'art. 10;
- ✓ la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il WP29, al fine di fornire un insieme più concreto di operazioni di elaborazione che richiedono una DPIA a causa del loro intrinseco alto rischio, suggerisce di considerare nove criteri.
La valutazione sulla necessità di condurre un'attività di DPIA può essere fatta utilizzando una check-list ed è sufficiente che siano soddisfatti due criteri per avviare, per quello specifico progetto di trattamento, una valutazione DPIA.

Criteri per valutare se effettuare una DPIA	Risposta
Sono previsti trattamenti valutativi o di scoring compresa la profilazione e attività predittive, con particolare riferimento a: 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?	
Sono effettuate decisioni automatizzate che producono significativi effetti giuridici o di analoga natura?	
Il trattamento comporterà un controllo sistematico degli interessati?	
Sono trattati dati sensibili o dati di natura estremamente personale?	
I dati saranno elaborati su larga scala?	
È prevista la combinazione o raffronto di insiemi di dati?	
Il trattamento di dati personali sono relativi a interessati vulnerabili?	
Sono previsti nel trattamento utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative?	
Il trattamento determinerà decisioni o azioni relative ai soggetti che avranno un significativo impatto su di loro?	
Sono trattati su larga scala dati riferiti a origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici, vita e/o orientamento sessuale, procedimenti giuridici e condanne?	
È prevista la sorveglianza sistematica di zone accessibili al pubblico?	

Fase 2 – Valutare la conformità del trattamento al GDPR

In questa fase si procede ad un'analisi della liceità, della necessità e della proporzionalità del trattamento rispetto alle finalità, con l'intenzione di rendere espliciti gli scopi di impiego dei dati perseguiti con il trattamento e le ragioni delle modalità adottate e gli interessi legittimi del Titolare. Le misure previste per conformarsi al GDPR (v. art. 35, paragrafo 7, lettera d) - considerando 90) e, nello specifico, anche al principio di liceità (art. 6) sono valutate attraverso i seguenti tre step:

1) Misure che contribuiscono alla proporzionalità e necessità del trattamento;
2) Misure che contribuiscono ai diritti delle persone interessate;
3) Liceità.

1. *Misure che contribuiscono alla proporzionalità e necessità del trattamento*

La proporzionalità e la necessità sono valutate rispetto all'art. 35 par. 7 lett. b) del GDPR.
Le seguenti tabelle si basano sulle indicazioni fornite nell'allegato 2 delle linee guida WP29[4] - Criteri per un accettabile DPIA.

Check list		
1	I dati personali saranno trattati in modo lecito e corretto?	
1.a	E' stato identificato lo scopo del trattamento?	
1.b	Come faranno gli interessati ad essere informati circa l'uso dei loro dati personali?	
1.c	Bisogna intervenire sulle informative privacy?	
1.d	E' stato stabilito come si effettuerà il trattamento?	
1.e	Se serve il consenso al trattamento dei dati personali come sarà raccolto?	
1.f	Se occorre il consenso come si procederà nel caso che sia rifiutato o ritirato?	
2	I dati saranno raccolti solo per scopi specifici e leciti e non saranno ulteriormente trattati in alcun modo che sia incompatibile con gli scopi originali?	
3	I dati personali sono adeguati, pertinenti e non eccedenti rispetto agli scopi raccolti?	
3a	Le informazioni impiegate sono sufficienti per gli scopi del trattamento?	
3b	Quali dati personali si potrebbe non usare senza compromettere le esigenze di trattamento?	
4	I dati sono esatti e sono costantemente aggiornati, ove necessario?	
4a	I sistemi sono in grado di modificare i dati quando necessario?	
4b	Come viene garantito che i dati personali ottenuti dagli interessati o da altre organizzazioni siano accurati?	
5	I dati personali trattati per una certa finalità non devono essere conservati per un periodo di tempo superiore a quello richiesto per raggiungere le finalità per cui i dati sono stati raccolti?	
5a	Qual è il periodo di conservazione adatto per l'elaborazione dei dati personali?	
6	I sistemi permettono di rispondere alle richieste di accesso da parte degli interessati?	
7	L'organizzazione adotta tecniche appropriate e idonee misure organizzative per contrastare trattamenti illeciti o non autorizzati e contro la perdita accidentale, la distruzione o il danneggiamento dei dati personali?	
7a	I nuovi sistemi sono sicuri contro rischi individuati?	
7b	**Che formazione e quali istruzioni sono necessarie per garantire che il personale opero in modo sicuro?**	
8	I dati personali non possono essere trasferiti a un paese al di fuori della UE, a meno che il Paese di destinazione assicuri un adeguato livello di protezione dei diritti e le libertà delle persone in relazione al trattamento dei dati personali?	
8a	L'attività richiede il trasferimento i dati al di fuori della UE?	
8b	Se i trasferimenti avvengono fuori area UE come si garantisce che i dati siano adeguatamente protetti?	

[4] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979

2. *Misure che contribuiscono ai diritti delle persone interessate*

In questa fase è necessario definire i processi privacy (informative, consenso, opposizione al trattamento, accesso alle informazioni, correzione, cancellazione, ecc.) idonei a garantire l'esercizio dei diritti.

Check list		
1	Come sono fornite le informazioni alla persona interessata?	
2	Come l'interessato conosce ed esercita il diritto di accesso e alla portabilità?	
3	Come l'interessato conosce ed esercita il diritto di rettificare cancellare, opporsi, chiedere la limitazione del trattamento?	
4	Come sono resi noti i destinatari dei dati trattati?	
5	Come sono resi noti i responsabili del trattamento?	
6	Quali sono le garanzie sul trasferimento internazionale dei dati?	
7	Si è resa necessaria la consultazione preventiva del Garante?	

3. *Liceità*

La valutazione della liceità si fonda sull'art. 6 del GDPR. La seguente tabella consente di valutare se sono presenti le condizioni di liceità previste dall'art. 6.1.

CONDIZIONE DI LICEITÀ	**SE LA CONDIZIONE SI APPLICA, PERCHÉ?**	**SPECIFICARE / NOTE**
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità.		(come si acquisisce consenso e come si conserva)
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.		(quale, come, perché?)
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento.		(verifica obbligo di legge, quale, come perché)
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.		(quali, di chi, come)
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.		(quale, specificare)
f) il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.		(bilanciamento chi e come)

Fase 3 - Descrizione del trattamento

Si tratta di descrivere il ciclo di vita dell'informazione, in termini di raccolta, archiviazione, utilizzo e cancellazione. Tale fase ha lo scopo di evidenziare quale dato viene usato, per fare cosa e chi può accedervi. La descrizione dei flussi è fondamentale: solo una precisa comprensione dell'impiego dei dati consente di evidenziare i rischi ai quali essi sono esposti.

La comprensione del ciclo di vita delle informazioni può avvenire ricorrendo alle metodologie formulate dalla ISO, che propone il seguente workflow diagram, relativo al trattamento di dati personali.

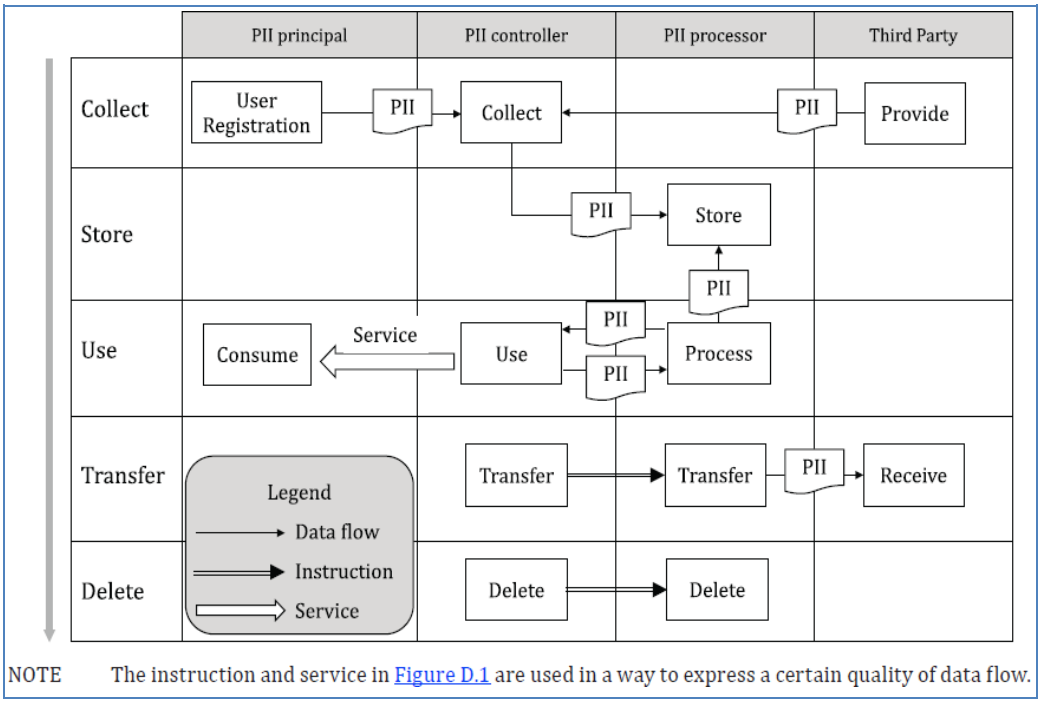


Figura 1 - Diagramma di flusso ISO/IEC 29134: 2017 per il Trattamento di Dati Personali

Per una lettura più agevole del diagramma, ecco una veloce guida dei termini usati nel grafico:

Termine	Definizione
PII	Dati Personali (Personally Identifiable Information)
PII principal	Interessato
PII controller	Titolare del trattamento
PII processor	Responsabile del trattamento
Third Party	Terze parti

Il grafico può senz'altro aiutare a determinare chi fa cosa e anche a identificare eventuali trasferimenti di dati. La descrizione del trattamento deve essere effettuata in modo conforme all'art. 35 paragrafo 7, lettera a).

La Natura/Tipologia dei Dati Personali trattati è fondamentale per determinare la valutazione degli impatti potenziali per i diritti e le libertà delle persone in caso di definizione del rischio per accesso illegittimo, modifica indesiderata e perdita o indisponibilità dei dati personali.

Definiti i dati e il contesto coinvolto nel trattamento è possibile descrivere i flussi dei dati personali. Si suggerisce di utilizzare la forma grafica dei flow chart, che si presta a valutazioni d'insieme.

Tabella di esempio di categorie di interessati:

Categorie di interessati	Risposta si/no
Dipendenti	
Docenti	
Assegnisti	
Dottorandi	
Studenti	
Aspiranti collaboratori	
Studenti 150 ore	
Fornitori	
Clienti	
Collaboratori esterni	
Minori	
Altri soggetti da identificare nel caso di contratti di ricerca.	
Stakeholder (partecipanti ai corsi ecc.)	

Tabella di esempio di check list per l'identificazione dei dati personali trattati:

Dati personali trattati		
Natura del dato trattato	**Tipologia**	**Si/no**
Dati Comuni	Anagrafici	
	Foto	
	Video	
Dati Salute	Stato di salute	
	Sorveglianza sanitaria	
	Dati diagnostici	
Dati genetici	Dati genetici	
Dati biometrici	Firma grafometrica	
Dati particolari	Retribuzione	
	Giudizi di idoneità a mansioni specifiche	
	Esposizione a particolari rischi	
Dati giudiziari	Provvedimenti giudiziari	
	Sentenze di condanna	

L'identificazione dei dati personali trattati ha un ruolo centrale per fissare la valutazione degli impatti potenziali sui diritti e le libertà delle persone, per le ipotesi di accesso illegittimo (R), modifica indesiderata (I) e perdita o indisponibilità dei dati personali (D).

Occorre anche rilevare gli strumenti che sono usati per il trattamento dei dati personali. Nella tabella si propone un esempio di quelli che possono essere gli asset coinvolti in un trattamento di dati personali tenuto conto delle norme ISO e del WP art. 29.

Strumenti	Esempio non esaustivo
Hardware e software dell'interessato	Smartphone, tablet, pc
Hardware del Titolare	Computer, apparati di comunicazione, usb drive, hard drive
Software del Titolare	Sistemi operativi, di messaggistica, database, applicativi
Rete	Rete
Siti (fisico o virtuale dove si svolge il trattamento)	Ufficio, sala, server, archivio
Persone	User, amministratore, ecc.
Documenti cartacei	Stampe, fotocopie, ecc.
Canali di trasmissione di documenti cartacei	Posta, corriere, ecc.

Fase 4 – Valutazione dei rischi

In questa fase vanno identificati quali potenziali minacce possono riguardare gli interessati. Il processo di valutazione dei rischi deve tener conto di tutte le entità coinvolte.
Possiamo individuare minacce legate a:

- ✓ Contesto;
- ✓ Strumenti;
- ✓ comportamento umano.

L'analisi dei rischi richiede la corretta identificazione delle minacce che possono aver successo sui dati coinvolti nel trattamento.
La valutazione dei rischi stabilisce il valore delle attività di informazione, identifica le minacce applicabili e le vulnerabilità che esistono (o possono esistere), identifica i controlli esistenti e il loro effetto sul rischio identificato, determina le potenziali conseguenze.

Si possono prendere in considerazione le classi di rischio in relazione all'effetto della minaccia sulle caratteristiche del dato personale. Le minacce che possono insidiare le tre caratteristiche fondamentali dei dati personali sono: Riservatezza (R); Integrità (I); Disponibilità (D).

Definizione	Tipologia di violazione	Effetti
Riservatezza	Accesso illegittimo	Divulgazione/accesso non autorizzato
Integrità	Modifica indesiderata	Modifica
Disponibilità	Ccomparsa dei dati (compresa l'indisponibilità momentanea dei dati)	Distruzione / Perdita

Check list di analisi del rischio

Accesso illegittimo dei dati (vs. Riservatezza)		
1	Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	
2	Quali sono le principali minacce che potrebbero concretizzare il rischio?	
3	Quali sono le fonti di rischio?	
4	Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	
5	Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	
6	Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	

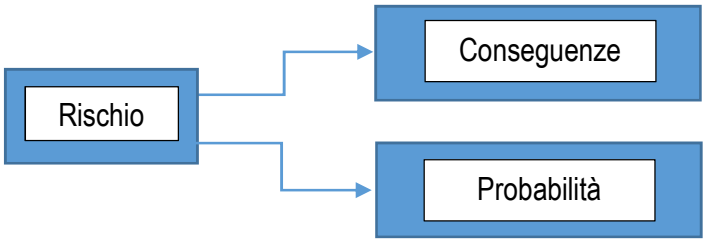
Modifiche indesiderate dei dati (vs Integrità)		
1	Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?	
2	Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?	
3	Quali sono le fonti di rischio?	
4	Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	
5	Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?	
6	Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?	

Perdita dei dati (vs Disponibilità)		
1	Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?	
2	Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?	
3	Quali sono le fonti di rischio?	
4	Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	
5	Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	
6	Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	

Fase 5 – Analisi del rischio

È la fase destinata ad identificare le azioni da intraprendere per contrastare i rischi, tenendo conto che la DPIA ha come obiettivo la riduzione del rischio o di portarlo ad un livello accettabile.

Per Rischio possiamo intendere la realizzazione di potenziali conseguenze negative e/o non desiderate di un evento. Possiamo definire il Rischio **(R)** come la combinazione della probabilità **(P)** e delle conseguenze (impatto) **(C)** del verificarsi di un particolare evento pericoloso.
La quantificazione dei rischi può quindi essere espressa adottando una funzione del tipo: **R=f (C,P)**, dove R rappresenta il rischio, C la gravità delle conseguenze e P la probabilità o la frequenza con cui si verificano le conseguenze.



Si consiglia di considerare, nella valutazione del Rischio, anche quello residuo dopo aver applicato le misure di attenuazione/rimozione dei rischi individuati.
Definire una funzione di rischio (f) significa costruire un modello di esposizione dei Trattamenti a determinati pericoli, modello che mette in relazione l'entità del danno atteso (Impatto) con la probabilità che tale danno si verifichi (P).

Una formulazione analitica della funzione di rischio richiederebbe l'utilizzo di un modello matematico estremamente dettagliato. Dal punto di vista pratico si può procedere con una metodologia semplificata, almeno all'inizio, riservandosi un eventuale approfondimento successivo.

Per la valutazione dell'entità del danno (ossia dell'impatto IMP) sul singolo dato personale trattato (dato della persona "n" = DATn) si può assumere il valore massimo di danno che verrebbe inflitto se si perdesse una qualunque delle caratteristiche RID sopra citate.
Indicando con **Rn** il danno dovuto ad accesso non autorizzato al dato della persona enne-sima, con **In** il danno dovuto a alterazione accidentale e con **Dn** il danno dovuto ad indisponibilità, l'impatto è quindi pari a:

IMP(DATn) = massimo_valore_tra [Rn, In, Dn]

Poiché il trattamento si riferisce ai dati di tutte le persone interessate, dalla prima (indicata con "1") all'ultima (indicata con "z") come entità del danno riferito al trattamento nel suo complesso può essere preso il valore massimo tra tutti gli impatti che si riferiscono all'intero insieme dei dati, partendo da DAT1 e arrivando a DATz. Pertanto:

IMP(T) = massimo_valore_tra [IMP(Dat1), IMP(Dat2)…IMP(DATn)…IMP(DATz)]

Per semplificare le successive operazioni si suggerisce di adottare per la valutazione dell'impatto un approccio qualitativo rappresentato dalla ISO/IEC 29134:2017.

Risulta conveniente concentrare l'attenzione su possibili scenari di impatto, considerando le potenziali ricadute negative sui diritti e le libertà delle persone i cui dati personali sono trattati.

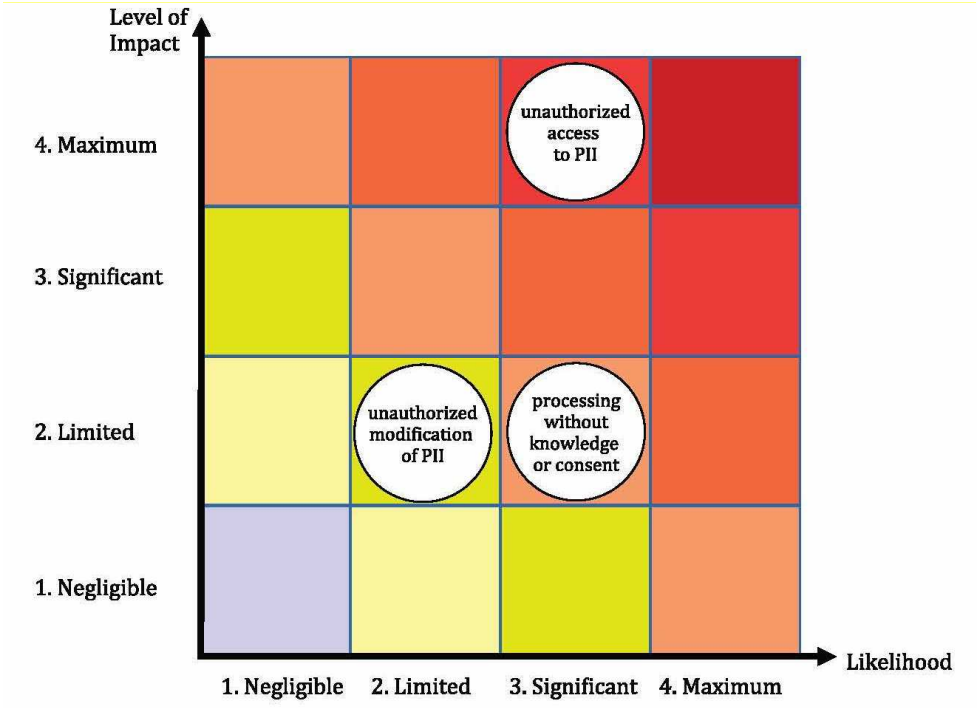
Nella tabella si indicano quelli che sono gli scenari di impatto più rilevanti che poi devono essere calati nel contesto specifico di dove si esegue la DPIA.

Scenario di Impatto	Descrizione
Danno Reputazionale (DR)	Trattamenti di dati personali invasivi della privacy o violazione di dati personali (c.d. «data breach») comportano la delegittimazione da parte degli stakeholder, degli interessati e compromettono la reputazione dell'ente.
Violazioni di Norme di legge (VN)	Trattamenti di dati personali effettuati in modo illecito o violazione di dati personali (c.d. «data breach») comportano sanzioni civili/amministrative/penali o il pagamento di penali contrattuali.
Richieste di Risarcimento (RR)	Trattamenti di dati personali effettuati in modo illecito o di violazione di dati personali (c.d. «data breach») comportano richieste di risarcimento da parte degli interessati.

Secondo tale approccio la valutazione sia dell'IMPATTO che della PROBABILITA' di verificarsi dell'evento dannoso sono sviluppate tramite una metodologia qualitativa usando le sotto elencate definizioni:

Livello di Probabilità di successo della minaccia			
1	2	3	4
Trascurabile	**Limitato**	**Significativo**	**Massimo**
L'esecuzione di una minaccia sfruttando le proprietà delle risorse di supporto non sembra possibile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei archiviati in una stanza protetta da un lettore di badge e un codice di accesso).	L'esecuzione di una minaccia sfruttando le proprietà delle risorse di supporto sembra essere difficile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei archiviati in una stanza protetta da un lettore di badge).	L'esecuzione di una minaccia sfruttando le proprietà delle risorse di supporto sembra essere possibile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei conservati negli uffici a cui non è possibile accedere senza aver prima effettuato il check-in alla reception).	L'esecuzione di una minaccia sfruttando le proprietà delle risorse di supporto sembra essere estremamente facile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei conservati in una lobby).

Il Rischio del trattamento si determina quindi in funzione della probabilità di successo della minaccia e dell'impatto. Ecco la Privacy Risk Map, secondo la ISO 29134:



Il relativo Livello di Rischio del Trattamento può essere qualitativamente espresso usando la scala sopra indicata. Normalmente le organizzazioni preferiscono, come scelta strategica, quello che viene definito rischio accettabile (RA).
Ciò consente di sviluppare un piano di interventi, dando la priorità a quelli relativi ad eventi che presentino un livello di rischio stimato R > RA.

È in questa Fase che si decide se i livelli di rischio residuo risultano accettabili o richiedono un intervento. Le possibili modalità di gestione dei Rischi sono tradizionalmente quattro:

- **ACCETTARE**: decidere di accettare il rischio, a fronte di una valutazione costi/benefici;
- **RIDURRE**: mitigare il rischio, ovvero ridurre il rischio ad un livello accettabile per il business, attraverso l'adozione di contromisure sostenibili;
- **TRASFERIRE**: trasferire il rischio ad altre parti (ad es. fornitori, outsourcer, società di assicurazione, cliente, ecc.);
- **RIMUOVERE**: evitare il rischio, rinunciando, ad esempio, ad effettuare il trattamento in esame.

Qualora il rischio residuo sia ritenuto elevato, il Titolare del trattamento, prima di procedere al trattamento, consulterà l'autorità di controllo (la c.d. Consultazione preventiva, art. 36, paragrafo 1).
La metodologia di cui al presente paragrafo può/deve essere usata per l'analisi di rischio relativa ai trattamenti dati già consolidati nell'organizzazione (v. la mappa di cui al paragrafo 4 del Piano).

Fase 6 – Il piano di azione

Il piano di azione, che costituisce chiaramente un sostegno all'accountability, consente di definire un piano condiviso delle misure da adottare, delle responsabilità di esecuzione e di verifica, di assunzione da parte del Titolare, della consapevolezza del Rischio residuo.
Si tratta di rilevare le misure idonee per ridurre probabilità e impatto. I controlli che il Titolare deve valutare per mitigare i rischi sul trattamento possono riguardare le misure descritte di seguito.

Misure e controlli di tipo organizzativo
Tali misure sono a loro volta raggruppabili in:

- **Organizzazione e governance**: specifici ruoli e responsabilità all'interno dell'organizzazione, controlli interni di supervisione, definizione dei ruoli per la gestione dei progetti, regole di interazione e le rispettive responsabilità in caso di contitolarità di un trattamento;
- **Processi**: procedure e policy interne, modelli di gestione dei rischi, gestione degli incidenti, delle modifiche e delle notifiche alle Autorità, contratti per proteggere le informazioni trattate in ambiti esternalizzati, accordi che rendano evidente quali informazioni debbano essere condivise, come e con chi;
- **Formazione e consapevolezza**: formazione adeguata del personale e consapevolezza dei potenziali rischi, selezione degli incaricati in base a qualifiche e competenze dimostrabili, guide operative per il personale su come usare i nuovi sistemi e su come condividere i dati quando necessario, materiale informativo per gli utenti, misure che consentano agli interessati di accedere alle proprie informazioni e al tempo stesso che rendano gli interessati consapevoli di come sono protette le proprie informazioni, di prevedere canali con cui gli utenti possano contattare l'organizzazione in caso di necessità di assistenza e con cui le organizzazioni possano rispondere alle richieste di accesso da parte degli interessati.

Misure e controlli di tipo tecnologico
Si tratta ad esempio di misure di:
- **Anonimizzazione**: rimozione o mascheratura delle informazioni personali quando non necessarie.
- **Pseudonimizzazione**: sostituzione dei riferimenti personali con identificatori finti e garanzia che le informazioni aggiuntive per l'attribuzione dei dati personali ad uno specifico Interessato siano conservate in metadati separati (Considerando 28).
- **Cifratura dei dati, dei messaggi o degli archivi**: soluzioni atte a rendere incomprensibili i dati acceduti, tranne ai soli autorizzati che possiedono la chiave di decifratura.

Misure e controlli sui dati e sugli archivi
Si tratta di misure e controlli di sicurezza fisica come, ad esempio, quelli sui supporti cartacei, sugli accessi fisici, sulla sicurezza degli impianti, dell'hardware e dei macchinari, della protezione da fonti di rischio non umane ecc.

Esempio di Piano di miglioramento					
Minaccia	**Azione di mitigazione del Rischio (Entro il…)**	**Costo (in €)**	**Risultato Atteso [il rischio sarà eliminato, ridotto o accettato?]**	**Valutazione dell'Efficacia [relativa all'impatto finale sugli interessati dopo l'implementazione della soluzione]**	**Resp.**
Azioni non autorizzate	Inserire nel perimetro della 27001 (data)	2.000	Ridotto a Trascurabile	Audit IT (data)	IT
Errori accidentali	Formazione addetti (data)	10.000	Ridotto a Trascurabile	Audit HR (data)	HR
Non Conformità con Requisiti	Riesame contratto Fornitore esterno (data)	900	Ridotto a Trascurabile	Audit Acquisti; Audit Fornitore (date)	Acquisti

Fase 7 – Monitorare il trattamento

I Rischi Privacy sono valutati e monitorati nell'ambito di gestione dei rischi dell'Ateneo.
Il modello di gestione della privacy adottato dalla Sapienza è sottoposto a costante monitoraggio da parte dell'Amministrazione, allo scopo di intervenire rapidamente, anche su proposta del RPD, sull'assetto organizzativo in caso di modifiche normative o a seguito dell'evoluzione tecnologica o della necessità di introdurre nuove e più efficaci politiche di gestione dei dati personali.