POLITECNICO
MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET
digital innovation

Osservatorio Information Security & Privacy

Linea Guida
per la Data Protection Impact Assessment

Sommario

Indice delle Tabelle

Indice delle figure

Prefazione

Il "fenomeno GDPR" negli ultimi anni, ma soprattutto negli ultimi mesi, ha determinato un innalzamento dell'attenzione per il tema della data protection italiana, europea e globale. Il nuovo Regolamento europeo per la protezione dei dati personali oltre a colmare le possibili lacune che il progresso tecnologico ha generato nelle leggi attuali, è studiato e volto ad armonizzare le varie normative presenti in Europa in un'ottica di elasticità e di coerenza con un mondo sempre più digitale.

L'esigenza di risultare conformi al GDPR entro il 25 maggio 2018 è una delle maggiori preoccupazioni in chi nelle aziende oggi si occupa di affari legali e di compliance, anche e soprattutto a causa del forte inasprimento delle sanzioni amministrative (i massimali imposti dal GDPR ammontano a 10/20 mln di euro oppure al 2%/4% del fatturato annuo di gruppo).

Sono numerose le novità previste dal Regolamento UE n. 2016/679. Il testo, composto da 99 articoli, pone al centro la figura degli interessati, i quali vedono incrementata la rosa dei diritti esercitabili, la cui tutela viene garantita attraverso la realizzazione e la relativa implementazione dei vari adempimenti previsti (ad esempio il Registro dei Trattamenti, la predisposizione di varie procedure e policy, la realizzazione di analisi, ecc).

Risulta utile, infatti, la realizzazione di campagne di sensibilizzazione volte a condividere e spiegare l'approccio "by design" che il GDPR porta con sé. Una metodologia che impone di "pensare" e considerare le possibili implicazioni relative alla data protection sin dalla progettazione di un nuovo bene/servizio.

Uno dei principali concetti introdotti dal GDPR è quello di "accountability" che determina un deciso aumento della responsabilizzazione del Titolare del trattamento il quale deve mettere in atto (nonché riesaminare ed aggiornare) adeguate misure tecniche ed organizzative, per garantire ed essere in grado di dimostrare che le operazioni di trattamento vengano effettuate in conformità alla nuova disciplina.

Con riferimento a tutti quei trattamenti che possono comportare un rischio elevato per i diritti e le libertà degli interessati, per valutarne la proporzionalità nel trattamento e per garantire nonché dimostrare che le operazioni di trattamento siano conformi alle disposizioni del GDPR è stato previsto l'ausilio di una valutazione d'impatto sulla protezione dei dati personali, oggetto delle prossime pagine.

La pubblicazione di una valutazione d'impatto non è obbligatoria (ad eccezione dei trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati e le casistiche previste dall'articolo 35, co. III del Regolamento UE n. 2016/679). La decisione è sempre rimessa al Titolare e deve essere condotta prima dell'inizio dei trattamenti oggetto della stessa.

Le pagine che seguono illustrano in cosa consiste tale processo di valutazione e, in via generale, come condurla. Sarebbe assolutamente auspicabile lo sviluppo di una metodologia "settoriale", in grado di mettere a fuoco quesiti mirati di analisi per individuare rischi di protezione dei dati personali comuni e possibili soluzioni di settore.

Ci auguriamo che questo lavoro, per il quale ringrazio a nome di tutto il team degli Osservatori Luca Bechelli e tutti coloro che hanno dedicato il proprio prezioso tempo, possa risultare utile e facile da utilizzare.

Volevamo fornire uno strumento pratico. Speriamo di esserci riusciti.

Gabriele Faggioli
Responsabile Scientifico Osservatorio Information Security & Privacy
Presidente CLUSIT – Associazione Italiana per la Sicurezza Informatica

1 Introduzione

Il nuovo regolamento europeo sulla protezione dei dati personali richiede, all'art.35, l'esecuzione di una Data Protection Impact Assessment (DPIA, a volte indicata anche come PIA) sui dati delle persone fisiche trattati dall'azienda. È in particolare obbligatorio effettuarla quando il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La valutazione di impatto sulla protezione dei dati è un processo impiegato per descrivere un trattamento (o un insieme di trattamenti) di dati personali, per valutarne la necessità e la proporzionalità rispetto agli scopi e per determinare le misure necessarie a indirizzare i rischi per i diritti e le libertà delle persone fisiche, valutati in un'analisi preventiva. In tal senso, la DPIA è un modo strutturato ed efficace per rispondere agli obblighi normativi e ha lo scopo di:

- realizzare soluzioni nel rispetto delle prescrizioni del Regolamento in quanto è strumento di ausilio nel processo decisionale circa le misure relative al trattamento;
- dimostrare l'adozione di misure idonee per garantire la conformità alle prescrizioni del Regolamento.

Dunque, la DPIA è uno strumento rilevante per il principio di «accountability» in quanto aiuta il Titolare a dimostrare, mediante procedure interne, schemi di analisi, misure tecniche e organizzative, valutazioni quantitative, parametriche o statistiche, evidenze di monitoraggio di indicatori, revisione dei criteri e dei risultati ottenuti, la effettiva protezione dei dati e, in definitiva, la conformità al Regolamento.

Il GDPR stabilisce le caratteristiche minime (vedere §5.2.3) di una DPIA (cfr. art. 35.7, Considerando 84 e 90):

- «descrizione delle operazioni di trattamento previste e delle finalità del trattamento»;
- «una valutazione della necessità e della proporzionalità del trattamento»;
- «una valutazione dei rischi per i diritti e le libertà degli interessati»;
- «le misure previste per:
  - «indirizzare i rischi»;
  - «dimostrare la conformità al regolamento».

Cosa è la DPIA?

La Data Protection Impact Assessment è una procedura destinata a descrivere un trattamento, valutare la necessità e la proporzionalità del medesimo e contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei dati personali (valutandoli e determinando le misure per indirizzarli).

DPIA è uno strumento rilevante per il principio di «accountability» in quanto coadiuva il Titolare non solo a rispettare i requisiti del GDPR, ma anche a dimostrare di aver adottato misure appropriate per assicurare la compliance (cfr. articolo 24).

Laddove l'operazione di trattamento è dinamica e soggetta a cambiamenti in corso, la DPIA è un processo continuo non una tantum.

In termini di gestione dei rischi, una DPIA mira a «gestire i rischi» per i diritti e le libertà delle persone fisiche (es. diritto alla vita privata, diritti della libertà di espressione, libertà di pensiero, libertà di movimento, divieto di discriminazione, diritto alla libertà, alla coscienza e alla religione). La DPIA può affrontare le specificità di un particolare tipo di operazione di trattamento (es. particolari tipologie di dati, risorse aziendali, potenziali impatti, minacce, misure), ad esempio in un particolare settore economico o

produttivo, o quando si utilizzano particolari tecnologie o svolgono particolari trattamenti. L'azienda dovrà quindi porre in essere processi interni dell'Information Technology tali da garantire fin dalla fase di progettazione la protezione dei dati personali.

La responsabilità dell'esecuzione della DPIA è del Titolare ed in subordine del Responsabile del Trattamento. Ove sia presente il Data Protection Officer questi deve essere consultato.

È necessario comprendere i casi in cui un trattamento abbia caratteristiche tali da essere definito "sistematico" e "con significativo impatto sulla persona", che portano alla necessità di effettuare una DPIA. Rientrano certamente in questa casistica, senza esaurirla, dati relativi 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
- Sorveglianza sistematica di zone accessibili al pubblico

L'Autorità di Controllo redige un elenco di trattamenti per i quali la DPIA è obbligatoria. Tale elenco è pubblico e viene comunicato al Comitato Europeo per la Protezione dei Dati. L' Autorità di Controllo (di seguito anche «AdC») può redigere altresì una lista di trattamenti per i quali la DPIA non è richiesta.

La DPIA deve essere effettuata prima dell'inizio del trattamento. Secondo il WP29 i trattamenti che possono comportare un rischio elevato per i diritti e le libertà delle persone fisiche e per le quali può quindi essere necessario effettuare o rivalutare una DPIA includono le seguenti casistiche (almeno due, anche se il Titolare è chiamato a considerare la necessità di svolgere la DPIA anche in presenza di una sola)[1]:

- valutazione o assegnazione di punteggi
- realizzazione di valutazioni automatiche con effetti giuridici o comunque significativi
- monitoraggio sistematico degli interessati
- trattamento dati sensibili o di natura strettamente personale
- elaborazione di dati su larga scala
- combinazione o raffronto di più trattamenti a partire da dati di origine diversa
- dati relativi a soggetti vulnerabili
- uso di tecnologie innovative o nuove soluzioni tecnologiche e organizzative

[1] Fare riferimento a §9.1 per una descrizione dettagliata

- trattamenti che impediscono all'Interessato di esercitare un proprio diritto o l'uso di un servizio o l'attivazione di un contratto.

La DPIA dovrà contenere al minimo i seguenti aspetti:

- descrizione sistematica dei trattamenti
- valutazione necessità e proporzionalità dei trattamenti in relazione alla finalità
- valutazione rischi per i diritti e la libertà degli interessati
- misure approntate per mitigare i rischi

Nei casi in cui il trattamento effettuato presenti impatti elevati per le persone fisiche il Titolare è tenuto preventivamente a chiedere autorizzazione all'AdC, che è tenuta a rispondere entro 8 settimane, estensibili di ulteriori 6 previa comunicazione dell'AdC.

Nella sua comunicazione il Titolare dovrà comunicare almeno le seguenti informazioni:

- responsabilità del Titolare e Contitolare
- finalità e mezzi del trattamento
- misure e garanzie previste a protezione dei diritti e della libertà degli Interessati
- contatti del DPO, se presente
- DPIA effettuata
- altre informazioni eventualmente richieste

Nello sviluppo della DPIA è raccomandato fare riferimento a metodologie standard come [ISO] o le linee guida emesse dal WP29, come [Linee Guida WP29]. La pubblicazione di un DPIA non è un requisito legale del GDPR: la decisione è rimessa al Titolare.

Infine, il Titolare deve prevedere un processo periodico di revisione della DPIA. Infatti, nelle [Linee guida WP29], par.III D "Come si effettua una DPIA?" al punto a) è affermato che "la DPIA è un processo permanente, soprattutto se si ha a che fare con un trattamento dinamico e soggetto a continue trasformazioni. **Lo svolgimento della DPIA è un processo continuativo e non un'attività una tantum."**

È bene ricordare che:

La DPIA è una procedura di valutazione delle operazioni di trattamento previste sui dati personali che mira a impedire o a ridurre gli impatti in caso di violazione dei principi di protezione dei dati, ovvero a minimizzare il rischio

2 Regole di utilizzo del documento

Il documento non può essere oggetto di diffusione, riproduzione e pubblicazione, anche per via telematica (ad esempio tramite siti web, intranet aziendali, ecc.), e ne viene espressamente riconosciuta la piena proprietà del DIG – Dipartimento di Ingegneria Gestionale del Politecnico di Milano.

Fermo quanto sopra, le figure contenute nel documento possono essere utilizzate solo eccezionalmente e non massivamente e solo a condizione che venga sempre citato il Rapporto da cui sono tratte nonché il copyright © in capo al DIG – Dipartimento di Ingegneria Gestionale del Politecnico di Milano.

La violazione di tale divieto comporterà il diritto per il DIG di ottenere il risarcimento del danno da illecito utilizzo, ai sensi di legge.

3 Riferimenti

3.1 Riferimenti normativi

[196]	Codice in materia di protezione dei dati personali (d.lgs. 196/2003)
[GDPR]	Regolamento Europeo 679/2016 (nel seguito, più semplicemente "GDPR")
[Regolamento]	vedere [GDPR] (nel seguito, più semplicemente "Regolamento" o "Regolamento Europeo")
[Linee guida WP29]	Linee Guida WP 248 17/EN "Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri logici per stabilire se un trattamento 'possa presentare un rischio elevato' ai sensi del Regolamento 2016/679" del 4 aprile 2017, come emendata ed adottata il 4 ottobre 2017
[Linee Guida DPO]:	Linee Guida 16/EN WP243 del WP29 sul Responsabile della Protezione dei Dati
[Linee Guida Data Breach]	Guidelines on Personal data breach notification under Regulation 2016/679 – wp250 del WP29
[Opinion WP 203]	WP29 Opinion on Purpose limitation 13/EN WP 203
[Legge Delega]	Legge 25 ottobre 2017, n. 163 – Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016-2017

3.1.1 Specifici richiami normativi

Nel seguito, sono indicati i riferimenti al corpo normativo sopra definito, nel quale il lettore può approfondire le varie tematiche trattate nella presente linea guida.

Relativamente alla predisposizione e realizzazione della DPIA:

- Dal GDPR:
  - art. 28 comma 3, lettera f per il ruolo del Responsabile (o Responsabili) del Trattamento
  - art. 35 comma 1 (C84, C90, 95) per il ruolo del Titolare del Responsabile (o Responsabili) del Trattamento
  - art. 35 comma 2; art. 38 comma 1; art. 39 comma 1, lettera c e comma 2 per il ruolo del DPO
  - art. 35 comma 9 (C84, C90) per il ruolo degli interessati o loro rappresentanti
  - Considerando 97 per il ruolo di specialista

- Dalle [Linee Guida DPO]:
  - par 3.1 “Coinvolgimento del DPO in tutte le questioni riguardanti la protezione dei dati personali”
  - par 4.2 “Ruolo del DPO nella valutazione di impatto sulla protezione dei dati”
  - par 4.4 “Approccio basato sul rischio”

- Dalle [Linee Guida WP29]:
  - par.I “Introduzione” per il ruolo del Titolare
  - par.III D “Come si effettua una DPIA?” punto b) relativamente al ruolo del Titolare a degli altri ruoli che sarebbe opportuno coinvolgere

Ai fini della consultazione dell’Autorità di Controllo

- dal GDPR:
  - art. 36 comma 1, comma 2, comma 3 per il ruolo del Titolare del Responsabile (o Responsabili) del Trattamento
  - art. 39 comma 1 lettera d e lettera e per il ruolo del DPO

- Dalle [Linee Guida DPO]:
  - par 4.3 “Cooperazione con l’Autorità di Controllo e funzione di punto di contatto”

In riferimento alla revisione periodica della DPIA:

- dal GDPR
  - art. 35, sezione 11

3.2 Riferimenti bibliografici

[CNIL] PRIVACY IMPACT ASSESSMENT (PIA) – Tools (templates and knowledge bases) – https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf

[ISO] ISO/IEC 29134/2017 Information technology – Security techniques – Guidelines for privacy impact assessment

[ICO] Conducting DPIA – Code of Practice – Data Protection Act – ICO – https://ico.org.uk/media/for-organisations/documents/1595/DPIA-code-of-practice.pdf

[Q&A DP Reform] Questions and Answers – Data Protection reform 21 dic 2015 http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

[US SEC DPIA] DPIA GUIDE – U.S. Securities and Exchange Commission – https://www.sec.gov/about/privacy/DPIAguide.pdf

[US Justice DPIA] Guide to conducting DPIA – U.S. Department of Justice – 2012- http://www.it.ojp.gov/documents/d/Guide%20to%20Conducting%20Privacy%20Impact%20Assessments_compliant.pdf

[Pizzetti 2005] G. Pizzetti – Sette anni dati in Italia 2005 – 12 – Ed. G. Giappichelli

[Enisa Handbook] Handbook on Security of Personal Data Processing, Enisa, Dicembre 2017

3.3 Definizioni, sigle e acronimi

Considerando	Indicano la motivazione dell'articolato (cioè degli articoli) dell'atto
DPIA	Data Protection Impact Analysis
WP29	Denominato "Article 29 Working Party", o "Gruppo di Lavoro ex Art.29", è un organismo consultivo e indipendente istituito dall'art. 29 della direttiva 95/46, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione Europea
AdC	Autorità di Controllo
RPD	Responsabile della Protezione dei Dati personali
DPO	Data Protection Officer ovvero il RPD (nel documento, sarà utilizzato prevalentemente l'acronimo "DPO")
sSDLC	Secure Software Development Life Cycle

4 Contesto aziendale di riferimento

A chi compete svolgere la DPIA?

La DPIA spetta al Titolare, che può avvalersi del Data Protection Officer («DPO») e del Responsabile del trattamento, ove designati (cfr. art. 35.2), oltreché di alcuni esperti del settore (es. responsabile sicurezza sistemi informativi, responsabile IT).

Se il trattamento è eseguito interamente o parzialmente da un Responsabile, quest'ultimo dovrebbe assistere il Titolare nell'esecuzione della DPIA e fornire tutte le informazioni necessarie.

Se del caso, il Titolare «raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto» (cfr. art. 35.9).

Per descrivere il contesto aziendale di riferimento per il GDPR è necessario partire dalle indicazioni già presenti nel GDPR stesso e nelle [Linee guida WP29]. Il GDPR infatti fornisce un quadro generale relativo alle realtà in cui dovrà essere applicato che, riassumendo, può essere definito come: tutte le aziende **che, a prescindere dalle dimensioni (dalle piccole alle grandi, per fatturato, per numero di dipendenti, etc.), dal settore di appartenenza (sia pubblico che privato), dalla localizzazione geografica, trattano dati personali di persone fisiche.**

L'applicazione di una definizione così ampia e generica ci impone quindi di **definire un contesto aziendale di riferimento che possa essere considerato una rappresentazione stilizzata valida per ogni azienda**, compresa la "media", che costituisce il tessuto ed il fondamento dell'economia italiana.

Ciò, al fine poi di definire su tale rappresentazione ruoli e responsabilità standard, che dovranno integrare le loro attività con i requisiti richiesti dal GDPR, proprio come era già in essere per il D.lgs. 196/2003.

4.1 Assunzioni

Si assume che la presente linea guida possa essere utilizzata nel settore privato sia da singole aziende che da gruppi industriali. Pertanto la definizione dei ruoli sarà scalabile a partire da "ruoli necessari", fino ad arrivare a "ruoli che sarebbe più opportuno coinvolgere".

Inoltre, la presente linea guida prenderà in considerazione 3 differenti sotto-processi:

1. Preparazione / Revisione di una nuova DPIA (Capitolo 6)
2. Consultazione dell'Autorità di Controllo (Capitolo 7)
3. Verifica delle DPIA esistenti. (Capitolo 8)

Nel Capitolo 5 sono fornite le indicazioni relative a come disegnare in generale la procedura della DPIA.

4.2 Requisiti normativi in relazione ai ruoli e responsabilità

La DPIA è uno degli strumenti che permette al Titolare di dimostrare non solo la propria responsabilizzazione (accountability), ma anche l'adozione di misure idonee a garantire il rispetto delle prescrizioni del GDPR. "In altri termini, la DPIA è una procedura che permette di realizzare e dimostrare la conformità con le norme" ([Linee guida WP29], par.I "Introduzione"). Pertanto la responsabilità del Titolare (accountability) è totale e riguarda tutte le fasi della procedura, dalla valutazione della necessità di una DPIA (o aggiornamento) all'eventuale comunicazione all'Autorità di Controllo.

In caso di gruppi societari

Particolare attenzione si dovrà prestare nel disegno del processo di DPIA nel caso di gruppi societari, come ad esempio in ambito industriale, nei quali si è stabilito uno stabilimento principale. In tali circostanze è fondamentale una chiara definizione all'interno del gruppo dei perimetri delle titolarità, delle contitolarità e delle responsabilità intra-gruppo nell'ambito dei trattamenti censiti.

Il Titolare del trattamento dei dati personali è, a norma dell'art. 4, comma 1, lettera f di [196], "la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza". Essendo di fatto per molte aziende una persona giuridica, le responsabilità in materia di trattamento di dati personali ricadono sulle figure che, in quanto poste al vertice dell'organizzazione, ne hanno anche la legale rappresentanza: ad esempio il Consiglio di Amministrazione, l'Amministratore Delegato o sull'Amministratore Unico. Pertanto, è opportuno che le responsabilità operative siano delegate a una funzione specifica, che chiameremo "Privacy Compliance Officer[2]", o al Legale Rappresentante.

Negli articoli 35, 36 e 39 del GDPR (rif.3.1.1) vengono citati come ruoli:

- il Responsabile (Responsabili) del Trattamento, da consultare e coinvolgere, se necessario e su richiesta;
- il DPO, se nominato;
- gli Interessati o i loro Rappresentanti, se del caso raccoglierne le opinioni.

L'opportunità da parte del Titolare e degli eventuali Responsabili di farsi assistere da una persona (o più persone) "che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati" è descritta nel Considerando 97 del GDPR.

[2] Noti bene il lettore che il Privacy Compliance Officer non è una figura individuata specificatamente dalla norma. Si utilizza questo artificio per indentificare la figura o le figure che, nell'organizzazione, vedranno concentrate le maggiori responsabilità, per conto del Titolare, nell'ambito della gestione della conformità al GDPR. Trattandosi di una figura che svolge ruoli operativi su diretto indirizzo del Titolare, questo ruolo non può essere assimilato, né essere in parziale sovrapposizione, con il DPO

Nelle [Linee guida WP29], par.III D "Come si effettua una DPIA?" al punto b) si possono trovare maggiori chiarimenti sugli obblighi:

- la conduzione della DPIA è di responsabilità del Titolare, che può chiedere la collaborazione del DPO e del Responsabile (o dei Responsabili) del Trattamento
- **"Spetta al Titolare garantire l'effettuazione della DPIA"** (art. 35, paragrafo 2)**.** La conduzione materiale della DPIA può essere affidata a un altro soggetto, interno o esterno all'organismo; tuttavia, la responsabilità ultima dell'adempimento ricade sul Titolare del trattamento."
- **"Il Titolare deve consultarsi con il responsabile della protezione dei dati"** (DPO), ove designato (art. 35, paragrafo 2). Tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il DPO è chiamato anche a monitorare lo svolgimento della DPIA (art. 39, comma 1, lettera c)). Indicazioni ulteriori sono presenti in [Linee Guida DPO]
- "Se il trattamento è svolto, in tutto o in parte, da un responsabile, **quest'ultimo deve assistere il Titolare nella conduzione della DPIA** fornendo ogni informazione necessaria conformemente con l'art. 28, paragrafo 3, lettera f)"
- **"Spetta al Titolare selezionare la metodologia, che comunque deve rispettare i criteri indicati nell'Allegato 2"** alle [Linee guida WP29]

e, a titolo di esempio, sul coinvolgimento di altri ruoli accessori, in particolare

- specifiche realtà aziendali se propongono di condurre una DPIA;
- "se del caso, esperti indipendenti provenienti da diversi ambiti disciplinari (legale, tecnologico, sicurezza, sociologico, etico, ecc.)";
- ove designato, il responsabile della sicurezza dei sistemi informativi (Chief Information Security Officer, CISO) e/o l'ufficio o la divisione IT.

In [Linee Guida DPO], par 4.2 "Ruolo del DPO nella valutazione di impatto sulla protezione dei dati", si asserisce che il DPO svolge un ruolo fondamentale e di grande utilità assistendo il Titolare nello svolgimento di tale DPIA. In ossequio al principio di "protezione dei dati fin dalla fase di progettazione" (o data protection by design), l'art. 35, secondo paragrafo, prevede in modo specifico che il Titolare "si consulta" con il DPO quando svolge una DPIA. A sua volta, l'art. 39, primo paragrafo, lettera c) affida al DPO il compito di "fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35".

È bene ricordare che:

La DPIA va eseguita quando si presenta un rischio elevato per i diritti e le libertà delle persone fisiche (ad es. discriminazione, furto d'identità …) o altro danno economico o sociale importante

Il WP29 raccomanda che il Titolare si consulti con il DPO, fra l'altro, sulle seguenti tematiche:

- 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 gli interessi delle persone interessate
- 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 conformi al GDPR.

4.3 Chi partecipa alla DPIA

In relazione alle caratteristiche specifiche, ogni azienda deve quindi, nel definire la propria procedura di DPIA, individuare i soggetti più appropriati che potranno svolgere un ruolo attivo o consultivo. A titolo esemplificativo, si riportano pertanto nel prospetto seguente tutte le figure che possono essere pertinenti. Nella colonna **"Esternalizzabile?"** si definisce se in un'azienda le aree elencate possono essere affidate a un outsourcer\fornitore esterno in linea teorica, senza tener conto delle sue dimensioni e complessità dei processi sottostanti:

Area di Riferimento	Descrizione dell'Area di Riferimento	Referenti / Soggetti	Esternalizzabile?
Proprietà dell'azienda	Soci dell'azienda.	Azionisti, Soci, etc.	NO
Management	Top Management dell'azienda, che ne definisce quindi strategie e modalità di implementazione ad alto livello di quest'ultime.	Presidente, CEO, Amministratore Delegato, Direttore Generale, Rappresentante Legale, etc.	SI (manager esterni che riportano alla proprietà, etc.).
Produzione/Erogazione	La parte vitale di ogni azienda, ossia l'area che si occupa di produrre/erogare prodotti/attività che sono il business dell'azienda.	Direttore di Produzione, etc.	NO (eventualmente solo sotto-processi).
Finanza/Amministrazione	Area responsabile delle attività di gestione e controllo finanziario/economico dell'azienda.	Direttore Finanziario, CFO, etc.	SI (commercialisti esterni, amministrazioni controllate, etc.).
Risorse Umane	Area responsabile delle attività di gestione del personale.	Responsabile Risorse Umane, CHRO, etc.	SI (uffici paghe, aziende di selezione, etc.).
Acquisti	Area responsabile di tutti gli approvvigionamenti/acquisti dell'azienda.	Responsabile Acquisti, CPO, etc.	SI (manager esterni che riportano alla proprietà, etc.).
Vendite/Marketing	Area responsabile della ricerca di nuovi clienti e/o business per l'azienda, e dal mantenimento di quanto già presente.	Direttore Commerciale, CSO, etc.	SI (agenzie di vendita esterne, etc.).
IT	Area responsabile della gestione dell'infrastruttura IT, ormai diventata asset fondamentale per qualsiasi business.	CTO, Responsabile IT, IT Manager, etc.	SI (consulenti esterni, aziende specializzate, etc.).
Segreteria	Ufficio che smista le telefonate dell'azienda, e che tendenzialmente si occupa dell'accoglienza dei clienti presso gli uffici dell'azienda.	Segretaria.	SI (aziende di multi-servizi, etc.).
Compliance/ Norme	Area che si occupa dell'implementazione e/o mantenimento di tutte quelli che sono le leggi e/o norme applicate/applicabili in azienda.	Compliance Manager, CCO, Responsabile Privacy, DPO, etc.	SI (consulenti esterni specializzati, etc.).
Legale	Area che si occupa della gestione di tutti quegli aspetti legali legati all'azienda.	Avvocato, etc.	SI (studi legali esterni, consulenti esterni, etc.).

Tabella 1: Aree di riferimento e relativi referenti

Tali soggetti possono partecipare alla DPIA, in relazione al trattamento in esame, con ruoli diversi. A tale scopo, sempre in riferimento ad una generica organizzazione, si definiscono i seguenti ruoli pertinenti per la DPIA, correlati alle precedenti aree:

ID Ruolo	Descrizione Ruolo	Descrizione Responsabilità	Area/e di riferimento	Note	Esternalizzabile?
R00	Titolare o suo Delegato	Accountable della procedura di DPIA	Management		NO
R01	Privacy Compliance Officer (PCO)	Ha la responsabilità di coordinare e verificare che tutti gli adempimenti in carico al Titolare siano effettuati. Ha la responsabilità di decidere se richiedere la Consultazione Preventiva e le azioni da fare in caso di esito negativo o di richiesta di modifiche.	Management, Compliance, Legale	Nel caso non sia nominato è il Legale Rappresentante. È uno Sponsor del progetto.	NO
R02	Project Manager (PM)	Segnalare al Titolare e al DPO il nuovo servizio, implementare la strategia, coordinare le attività necessarie alla DPIA e implementare le misure di sicurezza necessarie	Tutte le aree		SI
R03	Stakeholder	Fornire la loro opinione	Tutte le aree	Rappresentano gli Interessati o i loro Rappresentanti	SI
R04	Specialisti	Supportare il DPIA per le discipline di loro competenza e implementare le modifiche richieste	Tutte le aree	Esperti indipendenti provenienti da diversi ambiti disciplinari	SI
R05	Buyer	Negoziare gli strumenti contrattuali che fissino i ruoli e le responsabilità dei responsabili di trattamento	Acquisti		SI
R06	Legale / Contract Management (CM)	Definire gli strumenti contrattuali che fissino i ruoli e le responsabilità dei responsabili del trattamento	Legale, Compliance/Norme, Acquisti		SI
R07	DPO	Assistere il Titolare nella definizione della Strategia e nello svolgimento della DPIA, monitorarne lo svolgimento, verificare 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 conformi al GDPR. Assistere il Titolare nella richiesta di Consultazione Preventiva e fungere da interfaccia per l'Autorità di Controllo.	Management		SI
R08	Responsabili Trattamento dei Dati Personali (RTD)	Assistere il Titolare nel garantire il rispetto degli obblighi di DPIA, tenendo conto della natura del trattamento e delle informazioni a loro disposizione. Implementare le misure di sicurezza necessarie. Essere informati sull'esito della Consultazione Preventiva.	Terze parti (fornitori) o società diverse all'interno di un Gruppo Societario (laddove non individuate come conTitolari)		SI
R09	Responsabile Sicurezza dei Sistemi Informativi (CISO)	Supportare la DPIA con riguardo alle esigenze di sicurezza o operative. Implementare le misure di sicurezza necessarie. Essere informato sull'esito della Consultazione Preventiva.	Management, IT, Compliance / Norme		SI
R10	Responsabile di Funzione (RF) Owner del trattamento (OT)	In caso di un trattamento esistente segnalare al Titolare e al DPO la modifica con il cambiamento del profilo di rischio e collaborare per l'aggiornamento della DPIA	Tutte le aree		NO

Tabella 2: Mappa dei ruoli pertinenti per la DPIA

5 Disegnare la procedura di DPIA

5.1 Presupposti e interazioni della procedura di DPIA

Alla luce delle indicazioni del GDPR e delle [Linee Guida WP29], è fondamentale che i Titolari del trattamento abbiano ben chiari alcuni concetti basilari circa la procedura di DPIA, allo scopo di mettere la propria azienda in grado di effettuarla in piena aderenza con le prescrizioni della norma e con l'obiettivo di individuare la modalità migliore per la gestione dei dati personali all'interno della propria compagine.

Deve pertanto essere ben chiaro:

- in quali casi (QUANDO) la valutazione di impatto deve essere effettuata
- in che modo (COME) la valutazione di impatto deve essere implementata
- come sono formalizzate e quali Funzioni (CHI) hanno la responsabilità di prendere le decisioni relative alla necessità di:
    - effettuare/non effettuare una DPIA,
    - valutarne i risultati e le azioni conseguenti.

Per raggiungere i migliori risultati secondo le finalità del Regolamento e negli interessi dell'organizzazione, la procedura di DPIA dovrebbe quindi:

- contenere la **caratterizzazione delle operazioni di trattamento** previste, una valutazione del rischio, le misure di sicurezza, le garanzie e i controlli necessari alla protezione e alla sicurezza dei dati personali

- costituire uno strumento operativo, che aiuti le organizzazioni a individuare, analizzare e a ridurre con sistematicità i rischi per gli individui coinvolti da uno specifico trattamento

- essere parte integrante dell'approccio Privacy by Design, anzi aiuta ad assicurare che i **problemi potenziali siano identificati negli stadi iniziali** del progetto, quando la possibilità di indirizzarli è spesso più efficace e meno costosa

- avere un **ciclo ricorsivo** per attualizzare la valutazione fatta inizialmente a mano a mano che si procede con il progetto e vengono realizzate le misure pianificate ovvero evolvono le condizioni inizialmente definite

- **integrarsi con i processi di Demand e Project Management** definiti a livello aziendale; dunque è opportuno che ogni organizzazione ne sviluppi un proprio modello in base alle proprie consuetudini o necessità e lo correli con le pratiche operative di gestione dei progetti.

È bene ricordare che:

La DPIA si deve anche integrare con i processi di Demand e Project Management definiti a livello aziendale; dunque è opportuno che ogni organizzazione ne sviluppi un proprio modello in base alle proprie necessità e lo correli con le pratiche operative di gestione dei singoli progetti.

Inoltre, è opportuno che la procedura di DPIA sia integrata nel modo più omogeneo possibile con le attività e le prassi aziendali già in uso, in modo da evitare di costituire un collo di bottiglia, soprattutto nel primo periodo di adozione. In particolare, il fatto che la DPIA costituisca una procedura ricorsiva e strutturata in più fasi consente, in linea di principio, di ridurre il più possibile le attività preliminari tese a determinare i casi in cui la procedura debba essere svolta nella sua interezza (vedere in tal senso §6.1), spostando il maggiore effort solo ai casi (tendenzialmente in numero minore) in cui essa sia presumibilmente necessaria.

Infine, condurre una DPIA significa **lavorare in team** all'interno dell'organizzazione. Una DPIA è efficace quando coinvolge e consulta persone provenienti dai diversi settori dell'organizzazione in grado ciascuno di individuare differenti rischi di protezione dei dati personali e soluzioni basate sulla rispettiva area di interesse o di esperienza. Laddove opportuno si potranno prevedere contributi anche dalle funzioni operative che sono direttamente impattate dal nuovo servizio oggetto di DPIA, allo scopo di raccogliere riscontri da parte di chi ha una percezione pratica degli impatti.

5.2 Definizione della strategia

In relazione alle suddette caratteristiche, il disegno della procedura di DPIA, la scelta delle funzioni aziendali da coinvolgere, la definizione di ruoli e responsabilità, le modalità di attivazione ed i processi aziendali con cui la stessa procedura va a integrarsi (sia come procedura che "produce" informazioni, o che ne "consuma" da altri) ed altri elementi che ne caratterizzano il disegno, costituiscono gli elementi che contraddistinguono la DPIA non solo come procedura necessaria per la conformità ad un obbligo normativo, ma altresì come un nuovo strumento che può agevolare l'azienda nell'incremento della propria capacità di controllo.

Tale controllo indirizza i criteri di spesa, di standardizzazione delle pratiche di progettazione e implementazione, le misure di protezione, in modo coordinato e condiviso tra funzioni aziendali diverse, anche quelle che solitamente hanno difficoltà a interagire tra loro nell'ambito delle attività quotidiane.

Nel seguito, sono identificati gli aspetti che, più di altri, possono avere un rilievo nel disegno e nell'implementazione di una procedura di DPIA, a supporto della conformità e della gestione del patrimonio informativo aziendale.

5.2.1 Quando effettuare la DPIA

Il GDPR stabilisce che è necessario effettuare una DPIA in tutti i casi in cui le operazioni di trattamento presentano rischi elevati (Considerando 84) per i diritti e le libertà delle persone fisiche (es. discriminazione, furto d'identità) in virtù della loro natura, portata o finalità o quando possono procurare un danno economico o sociale importante.

È bene ricordare che:

tutti i dati personali sono soggetti alla protezione del GDPR, qualunque sia il formato o il supporto in cui sono registrati

L'oggetto della DPIA è costituito dal trattamento dei dati personali; solitamente si è portati a concentrare l'attenzione su quelli conservati/gestiti in formato elettronico, tuttavia non è escluso che possa ad avere ad oggetto, in tutto o in parte, il trattamento di dati in formato cartaceo. Le disposizioni del GDPR (comprese quelle sulla DPIA) riguardano infatti i dati personali in qualunque formato siano trattati, compreso quindi anche quello cartaceo.

Nel caso, le misure di sicurezza che la DPIA dovrà individuare saranno quelle più idonee a preservare il supporto cartaceo dai rischi sia di accesso non autorizzato che da perdita o distruzione. In generale le esigenze di protezione saranno quindi soddisfatte applicando le disposizioni sulla sicurezza fisica degli ambienti ove i documenti cartacei sono conservati, salvo eventuali ulteriori misure che potrebbero essere rese necessarie dalla specifica natura del trattamento o dalla condizione fisica degli ambienti in cui sono conservati.

La DPIA deve essere effettuata prima di procedere al trattamento (cfr. art. 35.1 e 35.10, Considerando 90 e 93) in coerenza con i principi di privacy by design e by default (cfr. art. 25 e Considerando 78) per determinare se il trattamento deve prevedere misure opportune in grado di mitigare i rischi. In tal senso, **la DPIA può essere una procedura "innescata" nell'ambito delle attività previste per l'adeguamento all'art.25**. Ciò consente di acquisire le necessarie conoscenze sulle misure, garanzie e meccanismi da prevedere per mitigare il rischio e assicurare la conformità del trattamento al Regolamento, prima che possano essere arrecati danni ai diritti ed alle libertà delle persone fisiche.

In accordo pertanto con l'obiettivo di assicurare i principi di privacy by design e by default (cfr. art. 25 e Considerando 78), può essere di utile determinare dei "check point" aziendali in grado di intercettare tutte quelle iniziative che possono far scattare l'esigenza di svolgere la procedura di DPIA, che possono essere riassunte nei seguenti casi:

- nuovi processi / attività aziendali per effetto dei quali sono introdotti dei nuovi trattamenti
- nuovi servizi informatici sviluppati in ambito progettuale, che insistono su trattamenti esistenti o che introducono essi stessi un nuovo trattamento
- cambiamenti significativi a livello organizzativo, con effetti su processi e relativi trattamenti
- variazioni significative a Trattamenti in essere
- cambiamenti rilevanti sui servizi informatici che supportano trattamenti esistenti.

In aziende strutturate, i processi più idonei per assicurare che per tutte le iniziative siano sottoposte a DPIA (quanto meno fino a determinarne la non necessità) sono tipicamente i processi di Demand e di controllo di gestione, in quanto già oggi costituiscono dei passaggi obbligati per la maggior parte delle attività progettuali aziendali. A questi possono essere aggiunte le iniziative rilevanti svolte dalle Risorse Umane e/o dall'Organizzazione, alle quali possono competere interventi trasversali sull'azienda che possono modificarne significativamente l'assetto.

Nella fase di transizione fino alla piena applicabilità del Regolamento, va ricordato che secondo le [Linee Guida WP29] non è assolutamente escluso che l'obbligo della DPIA possa riguardare anche i trattamenti già in corso prima del 25 maggio 2018. Questi pertanto andranno valutati caso per caso e si dovrà procedura alla DPIA in tutti i casi in cui sia presente un rischio elevato per i diritti e le libertà delle persone fisiche e per i quali siano intervenute variazioni dei rischi. I trattamenti tendono infatti a evolvere rapidamente e possono facilmente presentarsi nuove vulnerabilità.

È bene ricordare che:

il Regolamento non abroga il Codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003)

Non è invece necessario, sempre secondo il WP29, condurre una DPIA per quei trattamenti che siano stati già oggetto di verifica preliminare da parte di un'autorità di controllo o da un responsabile della protezione dei dati.

5.2.2 Approccio risk based

Il GDPR introduce un principio di proporzionalità delle misure da ritenere adeguate per garantire il trattamento conforme dei dati, cioè nel rispetto dei diritti degli interessati e della comunità.

La valutazione dell'adeguatezza va condotta sulla base di un processo che parte dai principi di protezione statuiti dal Regolamento (es. art. 5 e 6) e presuppone l'adozione di soluzioni incrementali in base a condizioni di rischio progressivo calcolato fin dalle fasi di progettazione del trattamento. Dunque la fase iniziale della progettazione diventa essenziale per stabilire i livelli di adeguatezza delle misure, in quanto è chiamata a verificare la proporzionalità delle misure rispetto agli scopi previsti dal trattamento.

Lo strumento per definire la progressione delle misure è essenzialmente il meccanismo di analisi del rischio. Fino ad oggi tale strumento è stato adottato in modo limitato dalle organizzazioni; le più virtuose, al massimo, ne hanno fatto un utilizzo sporadico, vuoi perché non ritenuto utile o necessario, vuoi perché il suo utilizzo sistematico prevede lo sviluppo di competenze aziendali specifiche e di un approccio organizzativo alle scelte maggiormente orientato, per l'appunto, ai rischi.

L'introduzione del processo di DPIA e di analisi del rischio richiesta dagli art.32 e 25 del GDPR crea una discontinuità con il passato e rende necessario un cambiamento. Naturalmente, la complessità ed il grado di efficacia delle valutazioni di rischio potranno variare da organizzazione a organizzazione, ma non sarà più possibile tornare ai precedenti approcci basati solo su "misure minime" o adempimenti predeterminati. Partendo da tale considerazione, i Titolari possono integrare l'approccio risk based come onere di conformità a garanzia del solo interessato, oppure cogliere l'occasione per introdurre lo strumento di analisi del rischio anche nella prospettiva della tutela del patrimonio informativo aziendale.

5.2.3 Il contenuto minimo in una DPIA

Nel capitolo successivo (§6) illustreremo le fasi in cui può articolarsi la procedura di DPIA, il cui contenuto minimo è comunque definito dalla norma e su cui è opportuno soffermarsi.

Pur non essendo previsto uno standard obbligatorio per la redazione della DPIA, la norma (art. 35 par. 7) ne definisce il contenuto minimo che deve comunque essere assicurato.

Partendo da questo, può essere utile, per chi si appresta ad effettuarne una, a seguire la seguente traccia articolata per punti, desunti dai criteri proposti dal WP29.

I titolari del trattamento possono utilizzarla per valutare se una DPIA o una metodologia per eseguire una DPIA sia o meno sufficientemente completa per la compliance al GDPR.

La DPIA dovrebbe quindi contenere:

1. la descrizione sistematica del trattamento (articolo 35, paragrafo 7, lettera a)):

2. la descrizione della natura, dell'ambito, del contesto e degli scopi del trattamento (Considerando 90);

3. i dati personali trattati, i destinatari e il periodo per il quale sono conservati;

4. una descrizione funzionale dell'operazione di trattamento;

5. la descrizione degli asset sui quali si basano i dati personali (es. hardware, software, reti, persone, documenti cartacei o canali di trasmissione cartacea);

6. la specificazione, se del caso, della conformità ai codici di condotta (articolo 35, paragrafo 8);

7. la valutazione della necessità e la proporzionalità del trattamento (articolo 35, paragrafo 7, lettera b)):

8. la descrizione delle misure previste per conformarsi al regolamento (articolo 35, paragrafo 7, lettera d) e Considerando 90), tenendo conto delle:

   - misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di: 1. scopo (i) specifico, esplicito e legittimo (articolo 5, paragrafo 1, lettera b)); 2. legittimità del trattamento (articolo 6); 3. adeguatezza, pertinenza e minimizzazione dei dati rispetto a quanto è necessario (articolo 5, paragrafo 1, lettera c)); 4. durata limitata di storicizzazione (articolo 5, paragrafo 1, lettera e));

   - misure relative ai diritti degli interessati: 1. informativa fornita agli interessati (articoli 12, 13 e 14); 2. diritto di accesso e portabilità (articoli 15 e 20); 3. diritto di rettifica, cancellazione, opposizione, limitazione del trattamento (articoli da 16 a 19 e 21); 4. destinatari; 5. Responsabile(i) (articolo 28); 6. misure di salvaguardia a tutela del trasferimento (i) internazionale (capitolo V); 7. consultazione preliminare (articolo 36).

9. la descrizione del modo in cui sono gestiti i rischi per i diritti e le libertà degli interessati (articolo 35, paragrafo 7, lettera c));

10. la descrizione dell'origine, della natura, della particolarità e della gravità dei rischi (cfr. Considerando 84), considerati dalla prospettiva dei soggetti interessati (accesso illegittimo, modifica non richiesta e sottrazione dei dati). In particolare:

    - si considerano le fonti di rischio (Considerando 90);

    - sono identificati i potenziali impatti sui diritti e le libertà degli interessati in caso di accesso illegittimo, modifica indesiderata e sottrazione dei dati;

- si identificano le minacce che potrebbero portare ad un accesso illegittimo, ad una modifica indesiderata e sottrazione dei dati;
- sono valutate probabilità e gravità (Considerando 90);

11. la determinazione delle misure previste per il trattamento di tali rischi (articolo 35, paragrafo 7, lettera d) e Considerando 90);
12. la descrizione del modo in cui sono coinvolte le parti interessate:
13. il parere del DPO (articolo 35, paragrafo 2);
14. le opinioni eventualmente raccolte dagli interessati o dei loro rappresentanti (art. 35, paragrafo 9).

5.2.4 Integrare la DPIA con gli altri processi aziendali

Le fasi della DPIA tendono ad integrarsi inevitabilmente con quelle dei processi di Demand Management e di Project Management già consolidate all'interno dell'organizzazione. I rilievi emersi dalla DPIA vanno quindi a convergere all'interno delle fasi di definizione e sviluppo di un progetto, e viceversa.

Più in generale, l'analisi effettuata ai fini della DPIA interagisce con tutti i processi aziendali, non esclusi ovviamente quegli stessi resi obbligatori dagli adempimenti del GDPR

Quella proposta di seguito è quindi la descrizione dei processi aziendali, le quali evidenze o risultati possono rappresentare un input/output per la conduzione della DPIA.

In particolare, nella figura seguente, sono evidenziati i punti di contatto tra i vari processi e la DPIA.

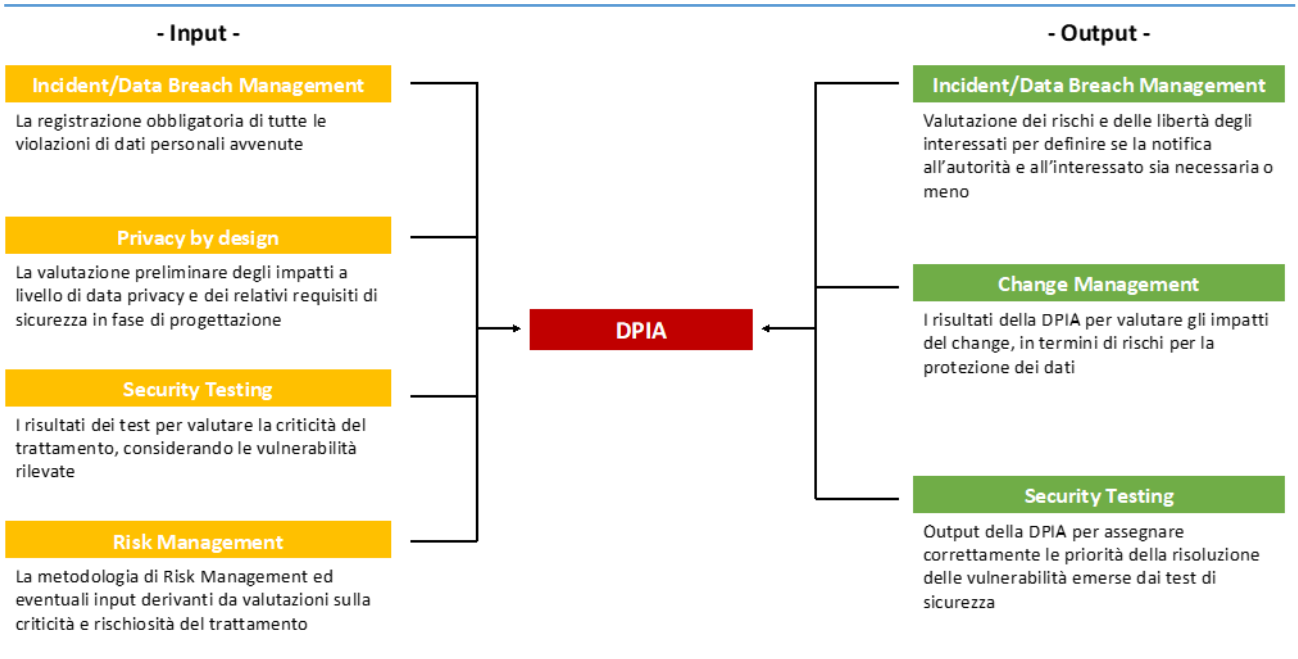

Figura 1: Relazioni tra la DPIA e altri processi dell'organizzazione

5.2.4.1 *Incident/Data Breach Management*

Per incidente di sicurezza delle informazioni si intende un singolo evento o una serie di eventi di sicurezza indesiderati o inaspettati, che hanno una significativa probabilità di compromettere il business e minacciare la sicurezza delle informazioni (ISO/IEC 27000:2014).

Ai fini ISO/IEC 27035:2011 si intende un evento o più eventi di sicurezza delle informazioni indesiderati o inattesi che hanno una significativa probabilità di compromettere le operazioni di business e minacciare la sicurezza delle informazioni.

Secondo la Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 «recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione», nota anche come «Network and Information Security Directive» («NIS») si intende ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi (art. 4).

All'interno di ogni organizzazione deve essere definito un processo per gestire l'incidente e ripristinare le normali operazioni di servizio, nel più breve tempo possibile.

Con l'introduzione del GDPR, ed in particolare con l'introduzione dell'articolo 33, le violazioni di sicurezza sui dati personali[3] (cosiddetti "Data Breach") devono essere gestiti in maniera differente rispetto agli incidenti di sicurezza.

***Input**: proprio il processo di Data Breach management, che richiede la registrazione obbligatoria di tutte le violazioni di dati personali avvenute per garantire la verifica da parte dell'Autorità di Controllo, può costituire un input per la DPIA. Il Titolare, a seguito di Data Breach, deve riesaminare le misure tecniche ed organizzative che non sono state adeguate per garantire il rispetto del GDPR, rivalutare gli impatti sulla Data Protection ed aggiornare le misure di sicurezza, garantendo un livello di sicurezza adeguato al rischio. In aggiunta, lo stesso processo di gestione del Data Breach richiede una valutazione dei rischi e delle libertà degli interessati (e quindi una DPIA), per definire se la notifica all'autorità e all'Interessato sia necessaria o meno. Infatti i processi di notifica e comunicazione, seppure richiedono adempimenti specifici, non possono essere letti ed interpretati correttamente senza considerare la loro correlazione con la DPIA.*

***Output**: la DPIA può rappresentare anche un output per gli incidenti di sicurezza, in quanto la stessa comunicazione può essere fatta solo se sono disponibili le informazioni necessarie, aspetto possibile solo se precedentemente è stato strutturato un sistema di report dell'incidente, è stata fatta una ricognizione adeguata dell'organizzazione del Titolare e sono state condotte le Valutazioni di impatto sui dati personali. L'esito della conduzione della DPIA, quindi, rappresenta anche uno strumento per la classificazione dell'incidente di sicurezza che ha coinvolto i dati personali, in quanto è stata eseguita proprio perché si è considerato un rischio elevato per i diritti e le libertà delle persone fisiche.*

[3] Per violazione dei dati personali (data breach) si intende una «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» da aziende o pubbliche amministrazioni.

5.2.4.2 Privacy By Design

Fino ad oggi le analisi di rischio richieste dalle normative settoriali precedenti al GDPR erano limitate (o così perlomeno erano state recepite dalla prevalenza delle organizzazioni interessate) alla valutazione dei soli impatti sui processi e sui prodotti in esercizio.

Il GDPR ha invece reso introdotto il principio (art. 25) secondo cui l'analisi del rischio deve essere compiuta a partire dalle fasi di progettazione di un prodotto o servizio pensando ai possibili impatti che questo avrà quando sarà in esercizio.

È bene ricordare che:

con il Regolamento la protezione dei dati personali va assicurata fin dalla progettazione

Ogni organizzazione, per garantire la sicurezza dei propri sistemi informativi, dovrebbe dunque avere definito un processo di sSDLC (Secure Software Development Life Cycle)[4].

> *Input:* il processo di Privacy by Design dovrebbe fornire come input alla DPIA – sulla base di una serie di informazioni (come tipologia di dato trattato, caratteristiche infrastrutturali, etc…) una valutazione preliminare degli impatti a livello di data privacy e dei relativi requisiti di sicurezza in fase di progettazione. Tale valutazione dovrà essere poi monitorata nel tempo, in fase di implementazione e testing, attraverso il classico processo sSDLC. Nella fase preliminare di raccolta delle informazioni si dovrà procedere anche all'identificazione della rischiosità del trattamento attraverso l'esecuzione della DPIA. Le attività definite per la *privacy by design* possono costituire quindi il punto di avvio della procedura di DPIA.

5.2.4.3 Change Management

Ogni cambiamento (ad es. aggiornamento, integrazione) che coinvolge i sistemi informatici, dovrebbe seguire una procedura di Change Management ben strutturata, per evitare impatti non previsti sull'operatività e sulla disponibilità, confidenzialità ed integrità delle informazioni appartenenti all'organizzazione.

> *Output:* il processo di Change Management dovrebbe essere integrato con il processo di privacy by design e DPIA, per la valutazione preventiva di eventuali change (tecnologici od organizzativi), che potrebbero avere impatti in termini di rischi per l'individuo. Per far questo è importante che all'interno di un processo strutturato di Change Management venga previsto un ulteriore step di approvazione, a seguito di una conduzione della DPIA per valutare gli impatti del change, in termini di rischi per la protezione dei dati.

[4] Per **sSDLC** si intende un ciclo di vita sicuro del software atto a considerare ed implementare opportune attività di sicurezza nel corso di tutte le sue fasi: analisi, progettazione, sviluppo, test e manutenzione.

5.2.4.4 *Security testing*

Le organizzazioni dovrebbero pianificare regolarmente una campagna di test di sicurezza (Penetration Test, Code Review) sui propri sistemi informativi, per rilevare proattivamente le vulnerabilità di sicurezza, che potrebbero rappresentare un rischio per i dati aziendali.

> *Input:* i risultati dei test effettuati su sistemi che trattano dati personali, possono costituire un input per la DPIA, in quanto devono essere considerati per valutare il livello di rischio per la tipologia di trattamento in questione. Nel caso di trattamenti ad alto rischio dovrà essere monitorata nel tempo l'efficacia ed applicazione delle misure di sicurezza adeguate anche attraverso i test di sicurezza.
>
> *Output:* relativamente alla gestione delle vulnerabilità emerse nel processo di security testing si dovrà eventualmente tenere in considerazione l'output della DPIA, per rivedere ed assegnare correttamente le priorità nella risoluzione delle stesse.

5.2.4.5 *Risk Management*

Il Considerando 90 del GDPR evidenzia degli elementi di sovrapposizione tra la DPIA ed altre componenti di gestione del rischio. La DPIA ha infatti l'obiettivo di gestire i rischi del trattamento per i diritti e le libertà delle persone fisiche, tenendo in considerazione il contesto, la valutazione dei rischi (in particolare probabilità ed impatto del rischio) e azioni di mitigazione del rischio. Attività che sono caratteristiche del processo di Risk Management di ogni organizzazione.

> *Input:* per questo motivo è importante che la DPIA DPIA possa contare su di una metodologia di Risk Management connessi ai trattamenti oltre agli input derivanti da valutazioni sulla criticità e rischiosità del trattamento in ambito ad esempio di normative o standard di settore (quali ad esempio la 231, 285, SOX, etc). Propedeutico per l'associazione dei rischi ai trattamenti è il dotarsi di una libreria di minacce *ad hoc*, tenendo conto dell'evoluzione tecnologica, dell'ambito di violazione – rispetto alla triade CIA o RID (Riservatezza, Integrità, Disponibilità) – e degli *asset*, andando oltre il concetto di rischio informatico al quale siamo abituati (legato all'*asset* e non al trattamento).

5.2.5 Integrare la DPIA con gli altri adempimenti del GDPR

Al termine di questa disanima sarà chiaro al lettore che tutti gli adempimenti disciplinati nel Regolamento che si basano sulla verifica del livello di rischio esistente o sulla adeguatezza delle misure predisposte per attenuarlo (ad esempio, quanto previsto dall'art.25) potranno avvalersi della analisi compiuta per la DPIA. Così come pure le verifiche e le valutazioni compiute per altri processi e altri adempimenti potranno essere riutilizzati per la DPIA.

È bene ricordare che:

Molti degli adempimenti del GDPR implicano una valutazione del rischio e delle misure atte a contrastarlo

È pertanto utile avere una mappa dei collegamenti tra la DPIA e gli altri adempimenti che valutano il rischio e le misure idonee a contrastarlo. L'organizzazione dovrà infatti avere cura di verificare che le decisioni

assunte nei vari processi e basate la valutazione del rischio e sulla valutazione dell'adeguatezza delle misure siano tra loro coerenti o quanto meno non contraddittorie.

5.2.5.1 Tenuta del Registro dei Trattamenti

La tenuta del Registro dei Trattamenti non è obbligatoria per le imprese o organizzazioni con meno di 250 dipendenti, a meno (tra le altre condizioni) che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'Interessato (art. 30 par. 5).
Il fatto stesso che l'impresa abbia ritenuto necessario effettuare una DPIA rende opportuno quindi considerare l'eventuale adozione del Registro, laddove l'organizzazione abbia precedentemente scelto altrimenti.
Peraltro, mentre la DPIA è richiesta in presenza di rischio "elevato", per l'obbligo di tenere il Registro dei Trattamenti basta che sia ravvisabile un qualunque rischio. Inoltre non ha rilevanza che le misure adottate ed individuate nella DPIA siano sufficienti per attenuarlo: il fatto stesso che in astratto ci sia un rischio rende potenzialmente necessario tenere un Registro dei Trattamenti.
Il Registro dei Trattamenti conterrà anche, ove possibile (GDPR, art. 30 par. 1 lett. g) una descrizione generale delle misure di sicurezza tecniche e organizzative adottate. Tale descrizione dovrà essere coerente con le misure individuate nell'ambito della DPIA.

5.2.5.2 La scelta delle misure tecniche e organizzative adeguate

La valutazione del rischio e l'individuazione delle misure di sicurezza ai fini della DPIA si intersecano, anche dal punto di vista temporale, con l'individuazione delle misure tecniche ed organizzative adeguate che l'art. 25 par. 1 chiede venga effettuata, oltre che al momento del trattamento, "al momento di determinare i mezzi di trattamento". Anche la DPIA deve infatti essere effettuata "prima di procedere al trattamento". Entrambi gli adempimenti tendono pertanto a convergere durante la progettazione (nella fase cioè logicamente antecedente all'inizio del trattamento).

La sovrapposizione tra la valutazione di rischio della DPIA e la conseguente definizione delle misure di sicurezza rispetto alla valutazione ex art. 25 par. 1 finalizzata ad individuare le misure tecniche ed organizzative adeguate non è totale.

Anzitutto la valutazione ex art. 25 riguarda tutti i trattamenti, mentre la valutazione ai fini della DPIA riguarda solamente i trattamenti che presentino un rischio elevato per i diritti e le libertà delle persone fisiche. L'ambito della valutazione ex art. 25 è quindi sensibilmente più ampio rispetto alla valutazione finalizzata alla DPIA.

Inoltre, la valutazione finalizzata alla individuazione delle misure tecniche ed organizzative adeguate ex art. 25 non dà luogo ad una comunicazione verso terzi (posto comunque il requisito di accountability che implica di dover documentare, e saper dimostrare l'adeguatezza, delle scelte adottate). Ciò tuttavia non toglie, evidentemente, che ai fini della redazione della DPIA vadano naturalmente a convergere le valutazioni e le scelte già effettuate ai sensi dell'art. 25 par 1. È anzi auspicabile che lo sia, in quanto le misure dalla DPIA dovranno essere ovviamente coerenti con quelle individuate nel corso della progettazione e della individuazione dei mezzi di trattamento. Inoltre, la valutazione del rischio condotta nell'ambito della DPIA sarà influenzata dalla considerazione delle misure tecniche e organizzative già adottate dall'organizzazione con riferimento ai trattamenti già esistenti a norma dell'art. 32, nonché le misure adottate per impostazione predefinita (privacy by default).

In particolare, la valutazione dell'adeguatezza del livello di sicurezza richiesta dall'art. 32 può portare alla necessità di effettuare un riesame della DPIA (art. 25 par 11) qualora siano insorte variazioni del rischio

rappresentato dalle attività relative al trattamento. Pertanto, il Titolare del trattamento rileverà le variazioni del rischio intervenute in primo luogo nell'ambito della valutazione che deve assicurare allo scopo di mantenere le misure tecniche e organizzative adeguate rispetto al livello di sicurezza richiesto (art. 32). Qualora tali variazioni riguardino i trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche per i quali sia già stata effettuata una DPIA, il Titolare dovrà altresì considerare l'esigenza di procedere altresì ad un riesame della DPIA.

Con riferimento invece al principio privacy by default, i criteri che l'art. 25.2 richiede vengano adottati per impostazione predefinita valgono anche ai fini della valutazione della necessità e proporzionalità dei trattamenti in relazione delle finalità, che l'art. 35.7, lett. b) richiede sia contenuta nella DPIA. Quest'ultima pertanto dovrà ispirarsi alla esigenza di limitare il trattamento ai soli dati necessari per le specifiche finalità del trattamento, sia con riferimento alla quantità dei dati raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità.

L'eventuale adesione a codici di condotta (art. 40) può costituire inoltre un utile riferimento per la conduzione della DPIA, qualora per esempio il codice abbia individuato delle possibili misure o procedure a cui conformarsi per garantire la sicurezza del trattamento. La scelta delle misure tecniche e organizzative potrà tenere conto anche delle misure suggerite in [Enisa Handbook].

5.2.5.3 La revisione delle misure tecniche e organizzative (art. 32)

Da quanto scritto, le risultanze della DPIA potranno quindi essere utili per una eventuale revisione delle misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio (art. 32).
Il Titolare del trattamento e il responsabile del trattamento sono infatti tenuti a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. La DPIA effettuata con riferimento ad un nuovo trattamento potrebbe comportare l'esigenza non solo di approntare misure adeguate con riferimento a quello specifico trattamento, ma altresì di rivedere le misure nel complesso preesistenti nell'organizzazione.
Il Considerando 83 precisa che in tale contesto occorre tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale. Si tratta di eventi potenziali di cui la DPIA deve tenere conto e la cui persistenza, nonostante le misure di sicurezza adottate, rende obbligatoria la Consultazione Preventiva dell'Autorità di Controllo.

5.2.5.4 La scelta del responsabile del trattamento

È opportuno che il Titolare includa, nell'ambito delle analisi condotte durante la DPIA, i criteri di selezione e valutazione dei Responsabili del trattamento da incaricare (art. 28 par. 1) per l'erogazione dei servizi connessi con il trattamento stesso. La norma infatti richiede che il responsabile del trattamento presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, da valutare soprattutto sotto il profilo di conoscenza specialistica, affidabilità e risorse (Considerando 81).

Per valutare se per il trattamento in questione il responsabile presenti garanzie sufficienti occorrerà pertanto fare riferimento alla valutazione del rischio contenuta nella DPIA ed alle misure ivi individuate, e valutare quindi se il responsabile del trattamento abbia i requisiti di conoscenze, affidabilità e risorse sufficienti per assicurare queste ultime.

5.3 Ruoli e responsabilità

La attività di definizione della strategia di implementazione della DPIA descritte sono state raggruppate in tre macro attività:

Macro-attività	Paragrafi di riferimento
Definire la strategia per la conduzione di un DPIA	5.2.1 Quando effettuarla 5.2.2 Approccio risk based 5.2.3 Il contenuto minimo di una DPIA
Implementare la strategia: Integrazione con altri adempimenti	5.2.5 Integrare la DPIA con gli altri adempimenti del GDPR
Implementare la strategia: integrazione con i processi aziendali	5.2.4 Integrare la DPIA con gli altri processi aziendali

Tabella 3: Macro-Attività – Definizione della Strategia

Si riporta di seguito a titolo di esempio una possibile attribuzione di responsabilità all'interno del contesto aziendale di riferimento (§4):

	R01 PCO	R04 Specialista	R06 Legal/CM	R07 DPO	R08 RTD	R09 CISO	R10 RF/OT
Definire strategia	A/R		C	C		C	
Integrazione con altri adempimenti	A/R		C	C	R	C	C
Integrazione con i processi aziendali	A			C	R	R	R

Tabella 4: Definizione della Strategia – Esempio di matrice RACI

Legenda:

- **Responsible (R)**: esegue e/o assegna l'attività;
- **Accountable (A)**: ha la responsabilità sul risultato dell'attività (univocamente assegnato);
- **Consulted (C)** collabora nell'esecuzione dell'attività;
- **Informed (I)**: è informato dell'esecuzione dell'attività

6 Disegno e descrizione della procedura di DPIA

Una volta definiti gli aspetti significativi di cui tenere conto (vedere a tal proposito la "Definizione della Strategia" in §5.2), è possibile procedere a definire nel dettaglio la procedura di DPIA e gli aspetti metodologici di valutazione. Il presente capitolo ed i seguenti §7 e §8, contengono la descrizione di un possibile flusso di attività, con relativa mappatura di ruoli e responsabilità, mentre per la metodologia è possibile fare riferimento al capitolo §9.

È bene ricordare che:

La DPIA costituisce uno studio utile per una azienda soprattutto quando affronta le specificità di un nuovo tipo di trattamento o particolari tipologie di dati, nuovi impatti potenziali, nuove minacce, nuove soluzioni. Ciò significa che la DPIA dovrebbe affrontare le questioni che sorgono in un particolare settore economico, o quando si utilizzano particolari tecnologie o si svolgono particolari trattamenti. In tal senso, sarebbe auspicabile lo sviluppo di metodologie settoriali di valutazioni d'impatto in grado di mettere a fuoco quesiti mirati di analisi per individuare nuovi rischi di protezione dei dati e per far evolvere e condividere la conoscenza di contromisure appropriate.

In generale, dovendo schematizzarne la struttura, la procedura di DPIA si può scomporre nelle seguenti fasi:

1. **Valutazione preliminare:** scopo dell'attività è, ai fini della conformità, determinare la necessità o meno di condurre una DPIA sul nuovo trattamento o su una modifica significativa di un trattamento in essere.
2. **Esecuzione DPIA:** in questa fase l'organizzazione deve sviluppare le valutazioni di rischio inerente per ciascuna categoria di rischio cui i trattamenti sono concettualmente soggetti. L'attività può essere strutturata come segue:
    a. **Analisi dei rischi sui trattamenti:** valutazione dei rischi sui diritti e sulle libertà degli interessati in termini di probabilità delle cause e di gravità degli effetti, tenuto conto anche della presenza di eventuali codici di condotta quando disponibili e pertinenti (GDPR, art. 35.8, Considerando 98).

    b. Identificazione misure e calcolo del rischio residuo: definizione delle misure di mitigazione dei rischi in termini di:
        i. soluzioni di sicurezza, tecniche, procedurali o organizzative
        ii. adozione di meccanismi o criteri di valutazione e di monitoraggio
        iii. garanzie sull'affidabilità e sull'adeguatezza delle misure.

3. **Finalizzazione e decisione finale:** valutare se le misure individuate sono idonee a mitigare i rischi ad un livello accettabile, stimando in tal senso un rischio residuo, nonché documentare i risultati di tutte le attività svolte durante la DPIA ed i razionali che determinano la scelta se procedere o meno alla Consultazione Preventiva
4. **Consultazione Preventiva:** consultare l'Autorità di Controllo qualora non sia stato possibile ridurre il rischio residuo a un livello accettabile. L'attività include il recepimento dell'eventuale risposta e l'attuazione degli eventuali interventi necessari per aderire al parere fornito dall'Autorità.

FASE		Quando
1	Valutazione preliminare	Ogni qualvolta viene pianificata un'iniziativa o un progetto. Da attivare fin dall'inizio della progettazione
2	Esecuzione DPIA	Prima dell'inizio del trattamento dei dati
2.a	Analisi dei rischi sui trattamenti	
2.b	Identificazione misure e calcolo del rischio residuo	
3	Finalizzazione e decisione finale	
4	Consultazione Preventiva	Se necessario, prima dell'inizio del trattamento dei dati

Tabella 5: Fasi della DPIA

Tali fasi, devono poi essere contestualizzate per l'esecuzione della procedura nei due seguenti casi:

- Caso A – Nuovo servizio sviluppato in ambito progettuale per il quale sia necessaria una DPIA
- Caso B – Nuovo trattamento per il quale sia necessaria una DPIA o revisione per un trattamento esistente

Nel seguito, nella descrizione delle attività saranno evidenziate le specificità previste nei due casi (nuovo servizio sviluppato in ambito progettuale, nuovo trattamento o revisione per un trattamento esistente), ad esclusione della descrizione delle attività di revisione periodica (per cui si rimanda al capitolo 8) e di esecuzione della fase di Consultazione Preventiva (vedere capitolo 7).

È bene ricordare che:

La DPIA è un processo codificato e strutturato in fasi, dunque è uno strumento operativo che aiuta le organizzazioni ad analizzare con sistematicità, a individuare e a ridurre i rischi privacy per gli individui interessati coinvolti dal rilascio di un nuovo progetto, soluzione o regola

6.1 Valutazione preliminare

La fase 1 ha come obiettivo la specificazione delle peculiarità del progetto oggetto d'analisi e la valutazione della necessità di effettuare o meno una valutazione di impatto.

Tale valutazione dovrà essere condotta alla luce delle indicazioni metodologiche del GDPR e delle [Linee guida WP29], che saranno da integrare con gli eventuali spunti interpretativi che potranno essere emessi a livello locale sulla base delle indicazioni della [Legge Delega], dei Codici di Condotta emanati a livello locale, ecc.

A tale scopo, sarà opportuno prevedere una descrizione sistematica dei trattamenti previsti e dei relativi elementi di caratterizzazione in termini di natura, ambito e contesto del trattamento, con lo scopo di identificare e rendere espliciti: i tipi di dati oggetto del trattamento, i volumi dei dati trattati, i destinatari e i relativi criteri di accessibilità, le modalità e gli strumenti del trattamento, gli asset che sostengono il trattamento dei dati la durata del periodo di conservazione.

Allo stesso modo, concorrono alla valutazione anche l'analisi della necessità e della proporzionalità del trattamento rispetto alle finalità, con lo scopo 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.

In questa fase può esser fatto riferimento agli adempimenti già previsti nel contesto delle misure obbligatorie che consistono in misure comunque necessarie ma non sufficienti per i trattamenti esposti a rischio elevato. Tra queste va considerato:

- il riferimento alle clausole di legittimità del trattamento (GDPR, art. 6)
- l'uso dei dati limitati a quanto necessario per lo specifico trattamento (minimizzazione)
- la cancellazione al termine previsto per la conservazione
- le informazioni e notifiche rese agli interessati
- il rispetto dei diritti di accesso, rettifica, cancellazione, opposizione, limitazione e portabilità dei dati da parte degli interessati
- specifici obblighi incombenti da parte dei responsabili del trattamento e nel caso di contitolarità
- garanzie per i trasferimenti transnazionali di dati.

Per questi motivi, l'attività può essere suddivisa in due sotto-fasi: raccolta informazioni e esecuzione della valutazione.

6.1.1 Raccolta informazioni

Obiettivo della sotto-fase è raccogliere le informazioni necessarie per dettagliare:

- **su cosa verte il progetto o il nuovo trattamento**: occorre evidenziare le nuove funzionalità che verranno esposte, le interfacce che dovranno essere utilizzate, l'operatività offerta o attesa dall'utente

È bene ricordare che:

La DPIA è parte integrante dell'approccio Privacy by Design, anzi aiuta ad assicurare che i problemi potenziali siano identificati negli stadi iniziali del progetto, quando la possibilità di indirizzarli è spesso più efficace e meno costosa

- quali **misure dovranno essere garantite per impostazione predefinita**: in pratica le misure opportune per assicurare il rispetto dei principi generali del Regolamento
- **quali finalità si propone il trattamento:** quali siano i tipi di dati e i tipi di trattamento coinvolti, ad es. se si prevede di comporre una profilazione degli utenti, di usare dati biometrici, di includere nel trattamento dati di minori o di soggetti deboli, da chi si prevede debba essere usato il servizio e in quale ambito
- come si ritiene che potranno essere **ulteriormente trattati i dati,** dovendo sempre prevedere possibili usi al di fuori dei trattamenti specificati e prefigurare eventuali usi illeciti
- qual è il **legittimo interesse** del Titolare di trattare i dati

- quali sono **ulteriori necessità** per i responsabili del trattamento di accedere ai dati dei sistemi informatici **ai fini della sicurezza** per prevenire gli eventi imprevisti o per contrastare le frodi e gli illeciti.

Pertanto, i dati da raccogliere, articolabili anche a mezzo di check-list, sono i seguenti:

ID	Informazioni da raccogliere
1	Descrizione sintetica del progetto
2	Descrizione del perimetro geografico di intervento
3	Descrizione dei principali attori coinvolti nella gestione del progetto (service provider, outsourcer, ecc.) e localizzazione delle piattaforme tecnologiche utilizzata
4	Tipologia dei dati trattati
5	Base giuridica del trattamento
6	Modalità di raccolta dei dati e di trattamento
7	Finalità del trattamento
8	Periodo e logiche di conservazione dei dati
9	Analisi delle condizioni e delle tipologie di trattamenti che rendono obbligatoria o facoltativa l'esecuzione della DPIA sulla base delle indicazioni delle line guida WP, di altre indicazioni interpretative locali, di considerazioni proprie della Società, ecc.
10	Distribuzione delle responsabilità del trattamento (data controller / data processor) tra i vari soggetti coinvolti nel progetto
11	Modalità con cui si prevede che gli interessati potranno manifestare i propri diritti (canali di accesso, di richiesta, ecc.)
12	Eventuali trasferimenti di dati in Paesi extra UE e nazionalità degli Interessati coinvolti
13	Necessità di considerare specificità normative locali
14	Descrizione delle misure tecniche e organizzative previste per la sicurezza dei dati. Tali misure potranno essere integrate con ulteriori misure da definire in sede di DPIA
15	Quali possono essere gli ulteriori stakeholder, anche non appartenenti all'azienda (es: categorie di interessati), e quali possono essere i soggetti più adatti a rappresentarli, nell'ambito dell'eventuale proseguimento nell'esecuzione della DPIA.

Tabella 6: Elenco informazioni da raccogliere

Tenendo conto di eventuali altri trattamenti in essere, o nel caso specifico di applicazione della procedura a modifiche rilevanti a trattamenti esistenti, l'attività di raccolta informazioni deve quindi essere completata con le seguenti valutazioni:

ID	Valutazioni sul Trattamento
1	Il trattamento previsto comporta la raccolta di nuove informazioni sugli individui (rilevante in particolare in caso di modifiche su trattamenti esistenti)?
2	Il trattamento previsto richiede che gli individui forniscano informazioni sulle proprie inclinazioni?
3	Le informazioni sugli individui saranno divulgate a soggetti che in precedenza non hanno avuto accesso a tali informazioni?
4	Si prevede di utilizzare le informazioni sugli individui per uno scopo attualmente non previsto o secondo un trattamento non ancora utilizzato?
5	Il trattamento previsto prevede l'uso di nuove tecnologie che potrebbero essere percepite come intrusive dei sistemi di protezione dei dati personali? (ad es. biometria o riconoscimento facciale)
6	Le informazioni sugli individui sono di tali da sollevare verosimilmente aspettative di protezione specifiche dei dati personali (es. dati sanitari, casellario giudiziario o altre informazioni sensibili)?
7	Il trattamento previsto richiederà di contattare gli individui per ottenere uno specifico consenso in un modo che essi potranno trovare invadente?

Tabella 7: Valutazioni sul Trattamento

6.1.2 Esecuzione della Valutazione

La presente sotto-fase ha come obiettivo la focalizzazione d'analisi sugli elementi raccolti e la finalizzazione della decisione relativa alla necessità di effettuare o meno una valutazione di impatto.

A cosa serve la DPIA?

Come previsto dall'art. 35 del Regolamento per valutazione di impatto sulla protezione dei dati (o DPIA – data protection impact assessement) si intende il processo che deve essere attivato, prima di procedere al trattamento, al fine di valutare l'impatto sulla protezione dei dati personali di alcune tipologie di trattamento nei casi richiamati dal regolamento stesso e meglio specificati nelle [Linee guida WP29].

In tale fase un ruolo chiave è svolto dal DPO o dalle Funzioni incaricate di gestire la privacy-compliance (es. Privacy Compliance Officer), che dovranno esplicitare anche le motivazioni per cui si è arrivati a tale decisione.

Nel caso in cui si verificassero dei possibili conflitti decisionali, in particolare rispetto alla decisione di non procedere con la DPIA, dovranno essere specificate le responsabilità finali per la decisione e le possibili logiche di "escalation" gerarchica nel caso in cui il ruolo di DPO non sia stato istituito.

Come previsto da [Linee guida WP29], i trattamenti che presentano un elevato rischio intrinseco sono in linea generale quelli che soddisfano almeno due dei criteri definiti nella Metodologia (§9), Tabella 19.

Sebbene, come detto sopra, le [Linee guida WP29] indicano come linea di condotta nello stabilire la necessità di una DPIA la presenza di almeno due dei suddetti criteri, i soggetti che partecipano alla Valutazione Preliminare dovranno considerare, adottando un approccio conservativo, l'effettiva esigenza di procedere all'esecuzione della DPIA stessa anche in presenza di un solo fattore, in relazione alle caratteristiche del contesto ed ai dati raccolti nella sotto-fase precedente (§6.1.1).

6.2 Esecuzione DPIA

La struttura logica della fase deve prevedere:

- Analisi dei rischi
  - Analisi dei trattamenti
  - Identificazione delle diverse categorie di rischi cui i dati personali sono soggetti nell'ambito dei trattamenti previsti dal progetto;
  - Per ciascuna categoria, stima dei valori di probabilità e gravità/impatto e, conseguentemente, del rischio inerente;
- Identificazione delle misure e calcolo del rischio residuo

In particolare, i seguenti paragrafi descrivono il flusso della procedura di analisi e gestione dei rischi connessi al trattamento. Per gli aspetti relativi alla metodologia di valutazione, fare riferimento a §9.

6.2.1 Analisi dei Rischi

6.2.1.1 Analisi dei Trattamenti

Una valutazione approfondita dei rischi è possibile solo se si evidenziano gli elementi che caratterizzano il trattamento dei dati. Occorre descrivere:

- su quali processi aziendali si distribuiscono le componenti del trattamento previste
- quali informazioni sono utilizzate nelle singole fasi
- quali asset (es. hardware, software, reti, persone, canali di trasmissione, documenti cartacei) sostengono il trattamento nelle singole fasi
- a cosa servono i dati, ovvero per quale finalità
- da chi sono ottenute le informazioni, a chi sono comunicate
- chi ne deve avere accesso

Questa fase della procedura di DPIA può essere supportata da fonti informative già disponibili all'interno dell'organizzazione per descrivere come i dati saranno utilizzati (es. un diagramma che riporti i flussi informativi tra i vari soggetti o sistemi o processi, la sequenza prevista delle operazioni di gestione dei dati, rapporti sull'uso delle informazioni, mappe informative, registri di asset informativi), a partire da quanto già raccolto in fase di Valutazione Preliminare (§6.1.1).

6.2.1.2 Identificazione delle diverse categorie di rischi

In questa fase occorre valutare gli aspetti che espongono il trattamento in esame a rischi di protezione e a rischi di sicurezza (informatica o fisica) dei dati personali. Più correttamente, o quanto meno in relazione a definizioni e concetti derivanti da standard internazionali in materia di *Risk Management,* il Regolamento con il termine *Rischi* pare talvolta riferirsi alle c.d. *minacce*, ovvero le categorie di eventi che possono determinare un effetto negativo sull'Interessato (materiale o immateriale, vedere Considerando 83), ed in altri casi alle possibili *conseguenze* o *tipologie di violazioni* sui trattamenti.

Pertanto, l'organizzazione deve identificare tanto le violazioni che le modalità con cui nel perseguire lo specifico trattamento, potranno generarsi (in modo volontario o accidentale) tali violazioni alla protezione dei dati personali degli interessati. Ciò consiste nell'identificare e gestire in modo sistematico l'insieme delle *minacce* effettivamente applicabili ai dati personali trasmessi, conservati o comunque trattati, a partire dalla descrizione dei trattamenti (§6.2.1.1) precedentemente svolta. Per maggiori dettagli su come svolte tale attività si faccia riferimento ai criteri per la valutazione del rischio sui trattamenti descritti nella sezione relativa alla Metodologia (§9.2)

Può essere utile applicare a queste fasi un set di quesiti (a titolo di esempio §Tabella 8) che consenta di far emergere le vulnerabilità e le minacce e su queste determinare gli effetti ovvero gli impatti.

ID	Quesiti
1	Quanti dati personali potrebbero essere divulgati, modificati o resi indisponibili?
2	Chi sono gli individui i cui dati potrebbero essere divulgati. modificati o resi indisponibili? Staff (dipendenti, collaboratori), dati relativi a propri clienti o fornitori, o dati relativi ai clienti dei propri servizi?
3	Quanto sono sensibili i dati che potrebbero essere divulgati modificati o resi indisponibili? Sono incluse categorie speciali di dati, data finanziari, informazioni pubbliche,…?
4	Che cosa potrebbero rilevare di un individuo a una terza parte se i dati dello stesso fossero divulgati, manomessi o resi indisponibili?
5	Che conseguenze potrebbero avere questi individui? Ci potrebbero essere rischi alla salute o alla reputazione, perdite finanziarie o una combinazione di questi o ad altri aspetti della propria vita? la violazione potrebbero comportare un furto di identità o una frode, danni fisici, disturbi pscicologici, umiliazione o un danno reputazionale?
6	Ci potrebbero essere conseguenze più ampie quali un rischio alla salute pubblica, o la perdita di fiducia in un servizio offerto dall'organizzazione?

Tabella 8: Quesiti a supporto per l'identificazione delle categorie di rischio

6.2.1.3 Analisi del rischio per la protezione dei dati

Una DPIA, per stimare il rischio, mira a determinare in particolare le minacce e gli impatti sui diritti e le libertà degli interessati (GDPR art.35.7, Considerando 84, 90).

Occorre procedere, una volta identificare le fonti di rischio rilevanti nel contesto specifico in esame, tradurle in gradi di probabilità e in gradi di impatto.

6.2.1.3.1 Stima dell'impatto

Gli impatti si possono dividere in due categorie, a seconda che i danni causati all'Interessato siano:

a) materiali: in caso di violazione della sicurezza, come ad esempio la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso illegale ai dati con conseguenti perdite finanziarie o altri impatti economici,
b) immateriali: in caso di perdita della riservatezza o dell'autenticità dei dati con conseguente discriminazione, pregiudizio alla reputazione, limitazione dei diritti dell'Interessato, furto o usurpazione dell'identità.

Gli impatti nei confronti degli individui, come sottospecie dei "danni alla persona", possono essere categorizzati in vario modo; tuttavia è importante che siano considerati i danni:

- legati alla violazione della sicurezza fisica
- legati alla violazione dei dati di identificazione (logica, sui sistemi) o attinenti l'identità personale, comunque riferibili al principio della riservatezza
- materiali (es. perdite finanziarie o al patrimonio, perdite dovute a frodi)
- morali o biologici (es. turbamento per la diffusione di una notizia riservata, compromissione di uno stato di salute, evento lesivo dei diritti umani inviolabili o dell'integrità della persona)
- sociali (es. quando intervengono conseguenze di tipo discriminatorio, perdite di autonomia)

Va considerato anche che alcuni effetti potranno ripercuotersi sulla stessa organizzazione se non indirizzati correttamente. Ad esempio, un progetto che è esposto sul fronte del pubblico aumenta anche i rischi di multe, di danni reputazionali o di perdite di business se rilasciato con carenze o soluzioni inappropriate. Pertanto, è opportuno che queste analisi vengano inserite nei rischi di progetto più che nella DPIA.

Per maggiori informazioni sulla valutazione di impatto, si faccia riferimento agli aspetti metodologici descritti in §9.2.2.

6.2.1.3.2 Valutazione della probabilità

La valutazione della probabilità e svolta in relazione alle minacce ed alla loro capacità di determinare le categorie di conseguenze precedentemente determinate sul trattamento (§Tabella 20). Tale capacità è definita *vulnerabilità*, che misura in particolare in quale misura e per quali motivi il Trattamento è esposto ad una certa minaccia.

Per maggiori informazioni sulla valutazione della probabilità, si faccia riferimento agli aspetti metodologici descritti in §9.2.3.

6.2.1.3.3 Calcolo del rischio

Una volta determinati probabilità e impatti, per ogni categoria di violazione (anche in forma aggregata), sarà possibile determinare un valore di rischio complessivo, espresso secondo una scala. Fare riferimento al paragrafo §9.2.4 per un dettaglio sulle modalità di calcolo e sulle possibili scale di valutazione.

Al fine di documentare e gestire i risultati dell'analisi, l'organizzazione può dotarsi di una sorta di *Privacy Risk Register*[5] dove sono riportate le descrizioni delle valutazioni fatte, al fine di dettagliare la mappatura dei rischi. È presumibile che, in base al principio di proporzionalità, progetti di minore portata elaborino una mappatura del rischio meno dettagliata rispetto ad altri più complessi.

[5] Il termine è coniato all'interno del presente documento per facilitare la comprensione del testo, e non corrisponde ad un documento espressamente richiesto dal GDPR. Resta inteso che il Regolamento chiede al Titolare di essere *accountable*, ovvero di documentare ed essere in grado di dimostrare le motivazioni delle scelte adottate, quale che sia la modalità.

Segue un esempio di *Privacy Risk Register* che esamina possibili rischi **verso gli interessati**:

Vulnerabilità	Minaccia	Probab. [P1]	Effetto / Impatto	Gravità [G1]
Controlli inadeguati di blocco alla divulgazione dei dati di identità	Possono aumentare la probabilità di diffusione impropria delle informazioni	3	Rischio materiale di perdita dovuta alla sottrazione dell'identità	4
Il contesto in cui l'informazione viene usata o resa nota può cambiare nel tempo	Può portare ad un uso per scopi diversi da quelli intesi inizialmente senza che gli interessati lo sappiano	2	Rischio morale di tensione e di fastidio nel vedersi coinvolto in attività non di interesse o non volute	3
Nuovi metodi di sorveglianza	Possono comportare una intrusione ingiustificata	3	Rischio per la sicurezza fisica	4
Una raccolta massiccia di informazioni su individui	Può portare a prendere misure nei loro confronti	4	Rischio morale di subire attività intrusive e di subire ingerenze inattese	4

Tabella 9: Esempio di documentazione del rischio calcolato sul trattamento

6.2.2 Identificazione delle misure e calcolo del rischio residuo

Obiettivo della fase è identificare le misure necessarie a garantire un'adeguata mitigazione di probabilità e impatti relativi alle minacce precedentemente identificate.

Se la DPIA è svolta per valutare nuovi trattamenti o nuove soluzioni tecnologiche a supporto di un trattamento esistente, in questa fase possono essere eseguite anche verifiche tecniche e controlli specifici al fine di verificare il reale livello di protezione realizzato dalle misure in essere (a titolo esemplificativo e non esaustivo penetration test, vulnerability assessment, audit su terze parti, ecc.).

L'analisi deve offrire una serie di possibili opzioni per indirizzare ciascun rischio, Considerando che lo scopo non è quello di eliminarlo completamente, quanto piuttosto **ridurre il rischio in termini di probabilità di accadimento e/o di gravità dell'impatto ad un livello accettabile**. Dunque, mentre si decide sulle possibili soluzioni, è sempre utile soppesare se gli scopi e i risultati di un'azione siano proporzionati alla riduzione dell'impatto previsto. A supporto dell'individuazione delle possibili misure di mitigazione dei rischi, fare riferimento agli aspetti metodologici definiti in §9.4.

6.2.2.1 Calcolo del rischio residuo

A valle dell'individuazione delle misure, il rischio dovrebbe essere ricalcolato in modo che sia evidente il valore effettivo (o residuo) rispetto a quello potenziale (o inerente) calcolato all'inizio, in assenza delle misure di mitigazione, così da poter pesare l'efficacia della misura introdotta.

Fare riferimento alla descrizione della metodologia (§9.2.4) per i dettagli sulle modalità di calcolo.

Sulla base degli interventi eseguiti il *Privacy Risk Register* deve essere aggiornato per riflettere come le misure introdotte abbiano mitigato il livello di rischio. Questi elementi di registrazione rispondono alla necessità di documentare il processo di analisi seguito per costituire la base di evidenza che assicura la conformità richiesta dal Regolamento.

6.3 Finalizzazione e decisione finale

6.3.1 Convalida dei risultati

I principali risultati che la DPIA dovrebbe aver consentito a questo punto sono:

- identificazione dei dati da proteggere (oggetto) e classificazione dei trattamenti (natura)
- identificazione delle vulnerabilità, delle minacce e delle relative probabilità
- identificazione degli impatti
- identificazione delle misure opportune e dell'efficacia attesa
- valutazione delle risorse disponibili, di quelle approvvigionabili e dei costi
- stima dei rischi residui a cui è esposto il trattamento
- valutazione degli interventi prioritari (in particolare in caso di modifiche rilevanti a trattamenti o tecnologie in essere)
- necessità di misure di ulteriore mitigazione da pianificare (in particolare in caso di modifiche rilevanti a trattamenti o tecnologie in essere).

L'organizzazione deve considerare quindi la **fattibilità** delle misure ipotizzate, in termini di tecnologie disponibili e **costi** di attuazione (Considerando 94).

È bene ricordare che:

Se gli esiti della valutazione dimostrano che il rischio residuo è elevato e non mitigabile rispetto alla tecnologia disponibile / costi ragionevoli di attuazione, occorre consultare l'Autorità di Controllo fornendo le evidenze dell'analisi

Alcuni costi sono di natura prettamente finanziaria, ad esempio quando deve essere acquistato un nuovo software per garantire un maggiore controllo sull'accesso e sulla conservazione. In ogni caso i maggiori costi devono essere bilanciati rispetto ai benefici attesi, Considerando, da un lato, le maggiori garanzie che interventi più consistenti possono comportare alla protezione dei dati e dall'altro minori rischi di sanzioni, rivalse, ricorsi o abusi oltre ai conseguenti effetti reputazionali.

Negli stadi finali occorre riesaminare i passaggi precedenti e decidere di convalidare la DPIA ed il rischio residuo. Questo per sostenere un processo di miglioramento continuo mediante la revisione e il monitoraggio dei cambiamenti seguiti nel tempo.

Per le soluzioni che si è deciso di realizzare è opportuno tener traccia dei passi seguiti nel processo decisionale, compreso chi li abbia approvati. Parimenti, se si fosse deciso di accettare un rischio, dovrebbe essere esplicita l'argomentazione sostenuta e l'assunzione di responsabilità.

Rif. Rischio	Soluzione decisa	Requisito derogato	Approvato da

Tabella 10: Esempio di documentazione delle decisioni adottate

6.3.2 Report della DPIA

Si ritiene utile giungere alla conclusione delle attività producendo un **report finale,** da allegare alla documentazione di progetto, per riassumere la procedura e i passi compiuti per mitigare i rischi e per consentire di ricostruire a posteriori i motivi delle scelte fatte sulla base dei rischi individuati. La pubblicazione di tale report non è un requisito legale del GDPR, pertanto la decisione è rimessa al Titolare. Si consideri che la pubblicazione della procedura DPIA può anche costituire una forma di trasparenza verso gli interessati che ne richiedano la consultazione e diventare così una strategia di comunicazione.

È bene ricordare che:

La DPIA deve dimostrare la conformità al Regolamento del trattamento e delle tecnologie coinvolte. In tal senso, è un modo efficace per rispondere agli obblighi normativi in senso più esteso

Il report deve inoltre esplicitare la frequenza di aggiornamento del DPIA (vedere §8), tanto maggiore quanto più si utilizzino tecnologie in evoluzione o potenziali variazioni nei processi di trattamento).

L'analisi conclusiva dovrà infine evidenziare se i livelli di rischio residuo sono adeguati, in particolare dovrà essere verificato l'allineamento alla propensione al rischio privacy richiesto dal Titolare. Se gli esiti della valutazione DPIA rivelano che il rischio residuo è elevato e non mitigabile rispetto alla tecnologia disponibile o a costi ragionevoli di attuazione, occorre **consultare l'Autorità di Controllo** per chiedere un parere fornendo le evidenze dell'analisi compiuta. A tale scopo, è opportuno che il Titolare (o il suo delegato, ad esempio il Privacy Compliance Officer) consulti il DPO, qualora sia stato designato in merito alla verifica della correttezza e della conformità della DPIA al GDPR.

6.3.2.1 Integrazione dei risultati della DPIA nel piano di progetto

I rilievi DPIA e le azioni dovrebbero esser integrati con il piano di progetto complessivo man mano che evolve. Anche se la maggior parte dell'impegno per la DPIA risiede nelle fasi iniziali del progetto, potrebbe essere necessario riesaminare le assunzioni preliminari negli stadi successivi dello sviluppo del progetto per avere conferma che le soluzioni siano state correttamente realizzate e abbiano ottenuto l'effetto atteso.

È probabile che i progetti di grande estensione ottengano benefici da un processo di revisione più formale. Una DPIA potrebbe generare azioni che restano attive dopo che la valutazione è finita per cui è necessario che su tali azioni continui il monitoraggio.

In questa fase occorre mettere in luce ciò che si è appreso nel corso del progetto, soprattutto gli errori compiuti e le considerazioni che si vorrebbe evitare nei progetti futuri.

6.4 Consultazione Preventiva

È difficile individuare un criterio certo che indichi in modo puntuale quando il rischio residuo sia elevato e, di conseguenza, sorga l'obbligo della Consultazione.

Il rischio elevato va infatti valutato caso per caso, ed anche per questo ambito vale il principio dell'accountability. Nel **report finale** (§6.3.2) il Titolare del trattamento ha indicato le misure previste per affrontare i rischi; la norma precisa che nell'individuare tali misure il Titolare deve dimostrarne "la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione" (GDPR, art. 35, par. 7, lett. d).

È questa quindi la chiave che consente di capire se il rischio residuo è elevato e, di conseguenza, se deve essere consultata l'autorità: la DPIA deve dimostrare che le misure siano adeguate, e tale valutazione compete al Titolare che deve non solo argomentare il motivo per cui le ha ritenuto adeguate ma deve anche essere in grado di dimostrarlo (assumendosi la responsabilità qualora in una successiva verifica tale dimostrazione dovesse risultare non sufficiente). A tale scopo, è opportuno che la scelta sia basata su criteri oggettivi definiti coerentemente con l'approccio metodologico di valutazione del rischio, come descritto in §9.3.

In queste valutazioni un ruolo chiave è svolto dal DPO o dalle Funzioni incaricate di gestire la compliance (es. Privacy Compliance Officer), che dovranno esplicitare le decisioni risultanti dall'effettuazione della DPIA nonché le relative motivazioni (per maggiori dettagli, fare riferimento a §7).

6.5 Ruoli e Responsabilità

La attività previste nell'ambito della procedura di DPIA, e successivamente al completamento del progetto, sono di seguito rimappate sulle fasi per la successiva definizione puntuale dei ruoli e delle responsabilità:

Attività	Paragrafi di riferimento
Segnalazione nuovo trattamento	6.1 Valutazione preliminare
Valutazione preliminare	6.1 Valutazione preliminare
Esecuzione DPIA	6.2 Esecuzione DPIA
Implementazione delle misure sicurezza	6.3 Finalizzazione e decisione finale
Monitoraggio DPIA	6.3 Finalizzazione e decisione finale e Capitolo 0
Verifica di Conformità della DPIA	6.3 Finalizzazione e decisione finale
Approvazione	6.3 Finalizzazione e decisione finale
Consultazione preventiva all'Autorità di Controllo	6.3 Finalizzazione e decisione finale e Capitolo 0
Pubblicazione	6.3 Finalizzazione e decisione finale

Tabella 11: Macro-Attività – Esecuzione DPIA

Si riporta di seguito a titolo di esempio una possibile attribuzione di responsabilità all'interno del contesto aziendale di riferimento (§4):

	R01 PCO	R02 PM	R03 StOld	R04 Specialista	R06 Legal/CM	R07 DPO	R08 RTD	R09 CISO
Segnalazione nuovo trattamento	I	A/R		I		C	I	I
Valutazione preliminare	A	R		C		R	R	R
Esecuzione DPIA	A	R	C	C		C	R	C
Implementazione misure sicurezza	A	R		C		C	R	R
Monitoraggio DPIA	A	R		C		R	R	C
Verifica Conformità DPIA	A	C			C	R	C	C
Approvazione	A/R	I				I	I	I
Consultazione preventiva (cap. 0)	A/R	I				C	I	I
Pubblicazione	A/R	I	I	I	I	I	I	I

Tabella 12: Esecuzione DPIA – Esempio di matrice RACI

Legenda:

- **Responsible (R)**: esegue e/o assegna l'attività;
- **Accountable (A)**: ha la responsabilità sul risultato dell'attività (univocamente assegnato);
- **Consulted (C)** collabora nell'esecuzione dell'attività;
- **Informed (I)**: è informato dell'esecuzione dell'attività

7 Consultazione Preventiva

Qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio, il Titolare del trattamento, prima di procedere al trattamento, consulta l'Autorità di Controllo.

L'art. 36 del GDPR prevede quindi questo ulteriore adempimento, che non è una vera e propria procedura autonoma rispetto a quella prevista per la redazione della DPIA, quanto una sua possibile conclusione.

7.1 Il contenuto della Consultazione Preventiva

Nel momento in cui il Titolare del trattamento attiva una Consultazione Preventiva deve allegare una relazione per la quale non è richiesto che sia utilizzato uno standard specifico (alla data di emissione della presente linea guida – ndr), ma che deve avere il contenuto minimo indicato nell'art. 36, par. 3 del GDPR.

In particolare il Titolare del trattamento dovrà indicare:

- se ne ricorrono le condizioni, le rispettive responsabilità del Titolare del trattamento, dei Contitolari del trattamento e dei Responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
- 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.

Nella richiesta di Consultazione Preventiva devono inoltre essere indicati i dati di contatto del DPO.

Infine, dovrà essere allegata la valutazione d'impatto effettuata.

L'Autorità di Controllo potrebbe comunque non ritenere sufficiente la documentazione presentata e in tal senso avrà in ogni caso facoltà di richiedere ulteriori informazioni (GDPR, art. 36, par. 3, lett. f) senza particolari limiti.

7.2 Procedimento della consultazione presso l'Autorità di Controllo

Il Titolare del trattamento, quando la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio, deve consultare l'Autorità di Controllo "prima di procedere al trattamento". Anche se l'art. 36 non lo specifica, deve inoltre ritenersi che non basta avere richiesto la Consultazione preventivamente, ma debba altresì continuare ad astenersi dall'iniziare il trattamento fino a che non si sia concluso il procedimento di consultazione.

Il fatto che, nelle more del procedimento di consultazione il Titolare debba comunque astenersi dall'iniziare il trattamento è peraltro confermato dai termini molto rigorosi che la norma ha ritenuto di imporre (otto settimane prorogabili una sola volta di altre sei) entro cui l'Autorità di Controllo deve comunque concludere

la Consultazione. Termini rigorosi che si spiegano con il fatto che nel frattempo il Titolare vede fortemente limitata la propria attività, non potendo iniziare il trattamento (si pensi al caso in cui il trattamento abbia un ruolo centrale nell'esercizio dell'attività di impresa).

Il fatto che la mancata Consultazione Preventiva, ove sia necessario farla, sia soggetta a sanzione, lascia ipotizzare che, a scanso di possibili responsabilità, essa venga attivata dai Titolari del trattamento non solo nei casi in cui ci sia un acclarato rischio residuo elevato, ma anche nei casi in cui il rischio sia semplicemente dubbio.

Nel caso in cui non dovesse pervenire alcuna risposta entro il termine di otto settimane, il silenzio dell'Autorità potrà quindi essere interpretato come una implicita conferma che non sono stati ravvisati motivi di contrasto tra il trattamento che si intende iniziare ed il regolamento. Poiché le otto settimane decorrono dal ricevimento della richiesta di Consultazione (GDPR, art. 36 par. 2), è raccomandabile per i Titolari del trattamento di utilizzare modalità di invio della richiesta in grado di attestare in modo certo la data del ricevimento, salvo il caso in cui l'Autorità nazionale abbia fissato delle regole per l'invio di tali comunicazioni, regole alle quali si renderà comunque necessario attenersi.

Se invece l'Autorità ha ravvisato una possibile violazione del regolamento in quanto per il trattamento in questione il Titolare non abbia identificato o mitigato sufficientemente il rischio, la medesima potrà:

- fornire un parere scritto al Titolare del trattamento e al Responsabile del trattamento, qualora quest'ultimo abbia assistito il Titolare nella valutazione di impatto e nella richiesta di Consultazione Preventiva; oppure
- segnalare, entro un mese dl ricevimento della richiesta di Consultazione, la proroga di ulteriori sei settimane. Anche la segnalazione della proroga è comunicata al Titolare ed al Responsabile (se del caso) del trattamento.

La proroga è prevista nei casi di "complessità del trattamento previsto". Si ritiene pertanto che nel rendere il parere l'autorità specifichi i motivi per cui ha ritenuto di avvalersi di tale proroga.

7.3 Poteri dell'Autorità di Controllo

A conclusione del procedimento, l'Autorità di Controllo emette un "parere".

Sul contenuto di tale parere è opportuno soffermarsi in quanto la denominazione utilizzata, "Consultazione" preventiva, non appare perfettamente idonea a descrivere tutti i poteri effettivamente esercitati dall'Autorità di Controllo in questa occasione.

L'Autorità di Controllo può infatti limitarsi a fornire un parere, fornendo ad esempio suggerimenti sulla modalità migliore per attuare il trattamento, ma può anche, se del caso, avvalersi dei poteri di cui all'art. 58 (come indicato nel GDPR, art. 36 par. 2).

Nel momento in cui esercita i poteri di cui all'art. 58 il parere cambia completamente aspetto ed assume le caratteristiche che lo avvicinano molto ad un vero e proprio provvedimento di autorizzazione preventiva.

7.4 Integrazioni da parte di discipline nazionali

Il regolamento ammette la possibilità che la disciplina della Consultazione Preventiva possa essere integrata dalle normative nazionali.

Queste ultime potranno prevedere casistiche particolari in cui è obbligatorio che i titolari del trattamento consultino l'Autorità di Controllo e ne ottengano l'autorizzazione preliminare, qualora l'esecuzione del trattamento sia necessario ai fini della esecuzione di un compito di interesse pubblico o sia inerente alla protezione sociale e alla sanità pubblica.

La libertà di normazione nazionale appare quindi particolarmente limitata sia nella finalità (può solo rendere specificamente obbligatoria la Consultazione, ma non può fare il contrario, vale a dire esonerare dall'obbligo generale della Consultazione Preventiva) sia nell'ambito di applicazione (esecuzione di un compito di interesse pubblico o inerente alla protezione sociale e alla sanità pubblica).

7.5 Ruoli e Responsabilità

Ai fini dell'attivazione della richiesta di Consultazione Preventiva, il ruolo fondamentale è rivestito dal Titolare del trattamento.

È il Titolare del trattamento che, effettuando la DPIA, ha la responsabilità di rilevare l'adeguatezza delle misure rispetto al rischio. Di conseguenza, è sempre il Titolare che, preso atto del fatto che i rischi non possano essere gestiti in misura efficace, attiva la procedura di richiesta di Consultazione.

Un ruolo importante è inoltre assicurato dal DPO, il quale partecipa alla procedura di valutazione di impatto fornendo un parere al Titolare (il quale è tenuto a consultarsi con lui, come indicato dal GDPR, art. 35 par. 2). Nel fornire tale parere, il DPO potrà eventualmente segnalare che dalla valutazione è emerso un rischio residuo elevato, tale da rendere necessario attivare la Consultazione Preventiva dell'Autorità di Controllo.

Tale parere non è vincolante per il Titolare del trattamento il quale, sotto la propria responsabilità e secondo il principio dell'accountability, potrà discostarsene non consultando l'Autorità, nonostante il DPO lo abbia consigliato, o viceversa.

Naturalmente, l'Autorità di Controllo può però valutare sfavorevolmente la condotta del Titolare del trattamento, qualora quest'ultimo non abbia attivato la Consultazione Preventiva, contro il parere del DPO, anche ai fini dell'applicazione delle sanzioni.

La necessità di rendere reperibile il DPO, indicando i suoi dati di contatto nella richiesta, chiarisce che anche nella procedura di Consultazione Preventiva l'interlocutore privilegiato dell'Autorità di Controllo è costituito per l'appunto dal DPO (GDPR, art. 39, par. 1, lett. e). Presumibilmente è a lui dunque che l'Autorità si rivolgerà chiedendogli cosa avesse consigliato al Titolare del trattamento nel parere espresso ai sensi dell'art. 35 par. 2.

Chi è il "Titolare della Protezione dei Dati"?

Questa figura insolita e inattesa è indicata nell'art. 36, par. 3, lett. d.

Non abbiate paura, non serve definire un nuovo ruolo: la versione inglese del GDPR chiarisce infatti che si tratta del "solito" Data Protection Officer!

Verificare se la condotta del Titolare sia stata coerente con tale parere potrebbe influenzare il successivo approfondimento da parte dell'Autorità.

La norma in esame non individua invece un ruolo specifico per il Responsabile del Trattamento. Tuttavia, il Considerando 95 del GDPR precisa che il Responsabile del trattamento, se necessario e su richiesta, dovrebbe assistere il Titolare del trattamento sia per la valutazione d'impatto che per la Consultazione Preventiva.

Il Responsabile del trattamento interviene pertanto se è richiesto dal Titolare. Interviene inoltre a prescindere da una richiesta del Titolare quando "necessario". Si può ritenere che la necessità derivi dalle specifiche peculiarità del trattamento, le quali potranno rendere necessario l'intervento del Responsabile in quanto maggiormente competente ed informato sulle sue caratteristiche specifiche.

A completamento di quanto descritto sopra, si riporta a titolo di esempio una possibile strutturazione delle attività, per identificare successivamente gli attori che possono essere coinvolti nell'ambito del contesto aziendale di riferimento (§4):

Attività	Paragrafi di riferimento
Decidere la Consultazione Preventiva	7.1 Il contenuto della consultazione preventiva
Attivare il processo di Consultazione Preventiva	7.2 Procedimento della consultazione presso l'Autorità di Controllo
Gestire la comunicazione con l'Autorità di Controllo	7.2 Procedimento della consultazione presso l'Autorità di Controllo
Decidere le azioni da fare in caso di esito negativo o di richiesta di modifiche	7.3 Poteri dell'Autorità di Controllo
Implementare le azioni	7.3 Poteri dell'Autorità di Controllo

Tabella 13: Macro-Attività – Consultazione Preventiva

Nel seguito sono identificati i ruoli e le responsabilità nell'ipotesi che il Titolare abbia attivato il DPO:

	R01 PCO	R02 PM	R07 DPO	R08 RTD	R09 CISO	R10 OT
Decidere la Consultazione Preventiva	A/R		C			
Attivare processo di Consultazione	A	I	R	R	I	I
Comunicazione con l'Autorità di Controllo	R		A/R			
Decidere le azioni da fare	A/R	C	C	C	C	C
Implementare le azioni	I	R	C	R	C	R

Tabella 14: Consultazione Preventiva – Esempio di matrice RACI

8 Revisione DPIA

8.1 Quando ripetere una DPIA

Poiché le operazioni di trattamento sono dinamiche e soggette a continui cambiamenti, la DPIA è una **procedura periodica** e non efficace se svolta una volta soltanto. Non solo: è opportuno effettuare un riesame della DPIA ad intervalli regolari almeno per verificare che non siano intervenute variazioni di rilievo.

Se un **trattamento esistente** deve essere modificato, occorre che sia riesaminato prima di modificarlo per assicurare che sia fatto evolvere in modo conforme.

Per i trattamenti in essere al momento dell'entrata in vigore del Regolamento occorre eseguire una valutazione preliminare di esposizione a rischi maggiori come da criteri riportati nelle [Linee Guida WP29] e, sulla base di questa, individuare se le misure in essere consentono soluzioni adeguate o se devono essere previste misure addizionali. Nel caso di esposizioni a un rischio residuo, si ritiene opportuno, ma non obbligatorio, che venga eseguita una DPIA anche per i trattamenti in essere. Infatti, è previsto che non sia necessaria una DPIA per i trattamenti già verificati e autorizzati da un'Autorità di Controllo prima del maggio 2018 ed eseguiti senza che siano intervenute variazioni rispetto alla verifica precedente. Quando siano mutati invece l'ambito di applicazione, le finalità, i dati personali raccolti, l'identità del Titolare del trattamento o dei destinatari, il periodo di conservazione dei dati o le misure tecniche e organizzative rispetto alla prima verifica effettuata dall'Autorità di Controllo, questo comporterà l'obbligo di una nuova DPIA.

8.2 Necessità di revisione della DPIA

Di regola, una DPIA dovrebbe essere rivista e rivalutata periodicamente: le [Linee Guida WP29] indicano che tale revisione debba essere svolta *almeno* ogni tre anni. Risulta tuttavia necessario procedere ad una revisione della DPIA nei seguenti casi:

- Cambiamento sulle attività di trattamento, in termini di:
  - Contesto (variazione della locazione fisica o di elementi ambientali dell'azienda, nuovi vincoli, funzioni e struttura organizzativa, innesto di politiche e processi aziendali, leggi, norme e contratti)
  - Modalità di raccolta dei dati personali (mediante modulo cartaceo o form elettronico, direttamente dall'Interessato o indirettamente da terzi)
  - Finalità del trattamento
  - Tipologia di dati personali trattati (personali comuni, sensibili e/o particolari, relativi a condanne penali e reati)
  - Destinatari (personale interno all'organizzazione o verso terzi)
  - Combinazioni di dati (integrazione con dati provenienti da altre sorgenti, correlazione di informazioni censite su diverse basi dati)

  - Trasferimento di dati all'estero (all'interno della UE o verso paesi od organizzazioni internazionali al di fuori della UE)

-

- Modifica ai rischi relativi alla Data Protection con impatti sui diritti e le libertà delle persone fisiche, derivanti da:
  - Sistemi informativi a supporto (subentro di un nuovo Service Provider, migrazione di servizi in Cloud, ecc.)
  - Nuovi scenari di rischio (furti di identità e frodi informatiche, introduzioni di attacchi avanzati e azioni non autorizzate)
  - Insorgenza di potenziali impatti sulle qualità di riservatezza, integrità e disponibilità dei dati personali
  - Nuove minacce (naturali, ambientali, tecniche, di terrorismo o sabotaggio, provenienti da comportamenti volontari o accidentali)
  - Attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali
  - Dismissione di elementi di presidio esistenti

-

- Mutamenti nel contesto organizzativo o sociale per l'attività di trattamento, ad esempio perché gli effetti di determinate decisioni automatizzate sono diventati più significativi oppure perché nuove categorie di interessati sono diventati vulnerabili alla discriminazione.

8.3 Linee guida sulle modalità operative della revisione della DPIA

In termini generali, la prima volta che viene eseguita una DPIA, sarà necessario individuare e censire in modo puntuale gli elementi di contesto sui cui svolgere l'analisi.

Nello svolgimento di una revisione della DPIA, molte informazioni sono già state raccolte e disponibili per una successiva analisi; in linea principio sarà pertanto necessario recepire solamente le variazioni rispetto al contesto di riferimento iniziale. A titolo di esempio, riportiamo di seguito due tabelle, utili al censimento delle informazioni per determinare il contesto e rilevare eventuali cambiamenti (fonte [CNIL]):

Tipologia di dati personali	Categoria di Interessati	Destinatari (e giustificazioni)	Utenti autorizzati all'accesso (e giustificazione)	Periodo di conservazione (e giustificazione)

Tabella 15: Censimento dei dati personali

Processo generico	Descrizione dettagliata del processo	Sistema informatico su cui risiede il dato personale	Altre risorse a supporto
Collezione			
Conservazione			
Uso			
Trasferimento			
Cancellazione			

Tabella 16: Censimento delle risorse a supporto

Per una rivalutazione del contesto, è quindi opportuno ripetere le valutazioni poste nella fase di valutazione preliminare della procedura di DPIA (rif.§6.1) in §Tabella 7.

8.4 Ruoli e responsabilità

Gli attori coinvolti nella revisione della DPIA saranno gli stessi della sua prima esecuzione, pertanto si potrà utilizzare la stessa matrice RACI riportata nel paragrafo 7.4. Potrebbe essere necessario coinvolgere ulteriori attori in relazione ai cambiamenti di contesto che hanno portato ad una esigenza di revisione DPIA (vedere §8.1).

La revisione della DPIA ha come input principale il risultato della precedente DPIA, quindi in termini di rivalutazione della stessa, si consiglia di procedere seguendo i seguenti passi:

1. Attivare la revisione, sulla base dei cambiamenti rispetto al contesto iniziale
2. Raccogliere le informazioni e/o effettuare una verifica delle informazioni censite, al fine di assicurarsi che non vi sia la necessità di ulteriori integrazioni
3. Attivare la procedura di modifica della DPIA, per rivalutare i rischi sulla base delle variazioni apportate, utilizzando la stessa procedura, la metodologia, gli algoritmi e gli strumenti di supporto previsti per la prima esecuzione.

Attività	Paragrafi di riferimento
Attivazione della procedura di revisione	8.2 Necessità di revisione della DPIA
Raccolta delle informazioni	8.3 Linee guida sulle modalità operative della revisione della DPIA
Attivazione del processo di modifica del DPIA	8.3 Linee guida sulle modalità operative della revisione della DPIA

Tabella 17: Macro-Attività – Revisione DPIA

Si riporta di seguito a titolo di esempio una possibile attribuzione di responsabilità all'interno di un'azienda, nell'ipotesi che il Titolare abbia attivato il DPO.

	R01 PCO	R07 DPO	R08 RTD	R09 CISO	R10 OT
Attivazione della procedura	A/R	C	I	I	I
Raccolta delle informazioni	I	C	R	C	R
Attivazione della procedura di modifica della DPIA	A	C	I	I	R

Tabella 18: Revisione DPIA – Esempio di matrice RACI

Legenda:

- **Responsible (R)**: esegue e/o assegna l'attività;
- **Accountable (A)**: ha la responsabilità sul risultato dell'attività (univocamente assegnato);
- **Consulted (C)** collabora nell'esecuzione dell'attività;
- **Informed (I)**: è informato dell'esecuzione dell'attività

9 Metodologia di valutazione di impatti e rischi

Il presente capitolo descrive:

1. le modalità di valutazione di un nuovo trattamento in relazione alle possibili conseguenze sui diritti e sulle libertà dell'Interessato
2. i criteri necessari per stimare un trattamento "ad alto rischio"
3. i criteri per la valutazione del rischio sul trattamento
4. le modalità di valutazione dei casi in cui il rischio residuo è da ritenere ancora elevato, tanto da rendere necessaria la comunicazione all'Autorità
5. le misure per la protezione dei trattamenti che il Titolare può selezionare per la mitigazione dei rischi individuati

relativamente agli aspetti metodologici che il Titolare deve definire antecedentemente all'esecuzione della DPIA.

Per garantire una piena responsabilità (accountability) delle scelte adottate, è opportuno che la metodologia prevista, sulla base della quale si fondano le scelte successivamente poste in essere, sia anch'essa opportunamente documentata e resa disponibile in caso di richieste da parte dell'Autorità di Controllo.

9.1 Criteri per stimare un trattamento "ad alto rischio"

Come più volte ricordato nel presente documento, il Regolamento impone ai Titolari di mettere in atto misure idonee a garantire ed essere in grado di dimostrare l'osservanza dello stesso, tenendo conto, fra gli altri, dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (GDPR, art. 24, paragrafo 1).

Il riferimento ai diritti e alle libertà degli interessati va inteso in primo luogo come relativo al diritto alla privacy, ma può riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

Per tale ragione appare opportuno riprendere quanto riportato nelle [Linee Guida WP29], per definire i criteri per determinare se un trattamento possa essere considerato "ad alto rischio" e quindi soggetto a DPIA.

Le Linee Guida elencano infatti nove criteri, di seguito presentati. Nel caso in cui un trattamento soddisfi almeno due di tale criteri, lo stesso deve essere considerato "ad alto rischio" e quindi rendere necessario condurre una DPIA. I criteri sono i seguenti[6]:

ID	Titolo	Descrizione Criterio	Ulteriori riferimenti normativi
1	**Valutazioni o assegnazione di punteggi**	Includono la profilazione e la previsione, in particolare su "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"	Considerando 71 e 91
2	**Decisioni automatizzate con significativi effetti giuridici**	Trattamenti che mirano a prendere decisioni sui soggetti interessati che producono "effetti giuridici sulla persona fisica" o che "incidono significativamente in modo analogo su dette persone fisiche"	GDPR articolo 35.3
3	**Monitoraggio sistematico**	Trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o per "la sorveglianza sistematica di un'area accessibile al pubblico" (art. 35.3). Questa tipologia di monitoraggio costituisce un criterio, ai fini della DPIA, in quanto la raccolta di dati personali può avvenire in circostanze tali da non consentire agli interessati di comprendere chi la stia applicando e per quali finalità oppure è impossibile per gli interessati sottrarsi a questa tipologia di trattamenti nelle aree ad accesso pubblico. Il concetto di sistematico va valutato secondo uno o più dei seguenti criteri: effettuato secondo un sistema; pre-organizzato, organizzato o metodico; effettuato nell'ambito di un piano generale per la raccolta dei dati; svolto come parte di una strategia.	[Linee Guida DPO] GDPR articolo 35.3
4	**Dati sensibili o di natura strettamente personale**	Si tratta delle categorie particolari di dati personali di cui all'art. 9 (per esempio, informazioni sulle opinioni politiche di una persona fisica) oltre ai dati personali relativi a condanne penali o reati di cui all'art. 10. Questo criterio include anche: a) dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), ovvero i dati sull'ubicazione (la cui raccolta mette in gioco la libertà di circolazione), i dati finanziari (che potrebbero essere utilizzati per frodi); b) documenti personali, email, agende, appunti tratti da lettori elettronici dotati di dispositivi per la presa di appunti, e informazioni molto personali contenute in applicazioni che consentono di tenere traccia del proprio stile di vita.	GDPR artt. 9 e 10
5	**Trattamenti di dati su larga scala**	Il GDPR non definisce ciò che costituisce una vasta scala, anche se il Considerando 91 fornisce alcune indicazioni. In ogni caso, il WP29 raccomanda di considerare in particolare i seguenti fattori per determinare se l'elaborazione viene eseguita su larga scala: a) numero di soggetti interessati, sia come numero specifico o come percentuale della popolazione di riferimento; b) volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; c) durata o persistenza dell'attività di trattamento; d) estensione geografica del trattamento.	Considerando 91
6	**Combinazione o raffronto di insiemi di dati**	Ad esempio originati da due o più trattamenti svolti per finalità diverse o da Titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative del soggetto Interessato.	[Opinion WP 203], p.24
7	**Dati relativi a soggetti vulnerabili**	Il trattamento di questa tipologia di informazioni rappresenta un criterio ai fini della DPIA in quanto è marcato lo squilibrio di poteri fra l'Interessato e il Titolare del trattamento, nel senso che il singolo può non disporre del potere di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti (es. minori, dipendenti, soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti).	Considerando 75
8	**Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative**	Ad esempio, combinare l'uso del fingerprint e del riconoscimento facciale per un miglior controllo fisico degli accessi, ecc. Il GDPR chiarisce che l'uso di una nuova tecnologia, "in conformità con il grado di conoscenze tecnologiche raggiunto", può richiedere una DPIA.	GDPR art.35.1 Considerando 89, 91
9	**Trattamenti che impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto**	Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto. Si pensi, a titolo di esempio, allo screening dei clienti di una banca attraverso i dati registrati nella Centrale Rischi al fine di stabilire se ammetterli o meno a un finanziamento.	GDPR art.22 Considerando 91

Tabella 19: Criteri di alto impatto per la DPIA

[6] Il lettore consideri questi criteri alla data di emissione del documento, tenendo conto di possibili aggiornamenti normativi successivi delle diverse linee guida emesse dal WP29 e di indicazioni o Provvedimenti dell'Autorità di Controllo del paese ove opera il Titolare

Naturalmente un trattamento assume un rischio sempre più alto quanto più sono i criteri che vengono soddisfatti dal trattamento stesso nella tabella precedente.

Si noti tuttavia che, nella stessa definizione delle [Linee guida WP29], le Autorità di Controllo europee hanno modificato i suddetti criteri per renderli più genericamente applicabili: da tali variazioni (ad esempio, prima della revisione di Ottobre 2017 era indicato anche il criterio relativo all'esportazione dei dati in paesi extra-UE) è evidente la necessità di aggiungere ai suddetti criteri delle riflessioni di volta in volta diverse, legate alle caratteristiche del nuovo trattamento e del contesto del Titolare, ivi compresa la possibilità di considerare "ad alto rischio" un Trattamento che soddisfi soltanto uno dei suddetti criteri. A tale scopo, per guidare le ulteriori valutazioni in relazione ai possibili danni cagionati all'Interessato per effetto del trattamento, si considerino le seguenti tipologie:

a) danni immateriali: perdita del controllo sui dati personali; discriminazione, pregiudizio alla reputazione; limitazione diritti Interessato; perdita riservatezza dati; furto/usurpazione identità;

b) danni materiali: violazione misure sicurezza – come la distruzione, perdita, modifica, divulgazione non autorizzata, l'accesso illegale ai dati personali trasmessi/conservati/trattati – ma anche perdite finanziarie o altri rischi economici.

È bene ricordare che:

Tutti i trattamenti di dati presentano una percentuale di rischio materiale/immateriale ma solo alcuni presentano rischi ELEVATI che richiedono la DPIA (cfr. Considerando 76). La DPIA va effettuata per tutti quei trattamenti in cui i rischi indicati al Considerando 75, idonei a soddisfare il requisito di gravità, risultino anche essere probabili a seguito della valutazione oggettiva di cui al Considerando 76.

9.2 Criteri per la valutazione del rischio sui trattamenti

Di per sé i criteri sopra elencati, o meglio il fatto che un trattamento soddisfi o meno due o più dei criteri sopra elencati, determina se un trattamento deve essere considerato ad alto rischio o meno. D'altro canto, da soli tali criteri non possono esprimere una valutazione del rischio potenziale del trattamento estesa ad una scala in grado di determinare l'effettiva natura e dimensione delle possibili conseguenze.

È bene ricordare che:

Le organizzazioni potrebbero decidere di usare standard di settore o proprie metodologie di Risk Management per aiutarsi a categorizzare, identificare e misurare i rischi

Per poter esprimere tale valutazione si rende pertanto necessario introdurre una serie di elementi atti a quantificare i rischi in relazione alle conseguenze per l'interessato. **A tal proposito, oltre a quanto di seguito proposto, il lettore può fare riferimento alle metodologie descritte in [Enisa Handbook] e [CNIL]**.

9.2.1 Violazioni, minacce e scenari di rischio

In primo luogo, si consideri che l'intera attività di DPIA, così come tutte le attività volte a proteggere i trattamenti, hanno come obiettivo minimizzare la probabilità e gli impatti che possibili violazioni dei dati personali (i.e. data breach) potrebbero comportare agli individui. Per violazione dei dati personali si intende una violazione quale la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso non

autorizzato ai dati personali (art. 32 GDPR). A titolo esemplificativo, nella tabella seguente sono riportate le possibili tipologie di violazioni sui trattamenti dei dati personali e le relative cause (i.e. *minacce*). Esse sono state tratte dal GDPR, art. 32.2, e dalle [Linee Guida Data Breach]:

ID	Tipologia di violazione	Descrizione (minacce)
1	**Distruzione**	Indisponibilità irreversibile o di lunga durata di dati personali trattati dal Titolare. La violazione può essere relativa a: • eliminazione logica non autorizzata (es. cancellazione dei dati) • eliminazione fisica (es. danneggiamento o distruzione dei supporti di memorizzazione o dei documenti cartacei) • eliminazione logica o fisica dei dati in formato elettronico, il cui ripristino da documenti cartacei è possibile ma con un impiego di tempo elevato, tale da poter generare effetti sull'Interessato. In questo scenario, i dati personali possono essere *recuperati* solo: - direttamente dall'Interessato - da fonti esterne quali fonti pubbliche e/o di terze parti (es: Pubbliche Amministrazioni); - da archivi cartacei (in caso di distruzione, il recupero da tali archivi si suppone estremamente complesso, di lunga durata e con il rischio di ottenere dati non aggiornati)
2	**Indisponibilità**	Indisponibilità, irreversibile o temporanea, dei mezzi e degli strumenti necessari per effettuare il trattamento dei dati da parte degli interessati o del Titolare per l'erogazione di servizi richiesti o per conto dell'Interessato. L'Indisponibilità non implica la Distruzione dei dati personali. L'Indisponibilità irreversibile di un mezzo o strumento richiede l'adozione di nuovi mezzi o strumenti per accedere ai dati. Tale violazione può essere relativa a: • indisponibilità dei sistemi e dei servizi informatici mediante i quali le informazioni sono accessibili (es: in caso di attacco informatico) • indisponibilità di mezzi e strumenti necessari per l'accesso alle informazioni (es: perdita di una chiave di decifratura o di un token hardware di accesso con la possibilità di accedere ai dati in backup o altri archivi) • indisponibilità degli strumenti atti a identificare l'informazione all'interno di grandi archivi cartacei o elettronici • degrado prestazionale dei servizi informatici, che determina l'impossibilità di perfezionare operazioni di trattamento • modifiche tecnologiche che rendono impossibile la decodifica di dati rappresentati secondo particolari formati di memorizzazione.
3	**Perdita**	Perdita del supporto fisico di memorizzazione dei dati (es. privazione, sottrazione, smarrimento dei dispositivi contenti i dati oppure dei documenti cartacei). La Perdita di un supporto fisico di memorizzazione dei dati non implica che si sia verificata anche un'altra violazione quale Distruzione, Indisponibilità, Accesso o Divulgazione: ad esempio, un disco DVD perso può contenere una copia cifrata[7] di dati.
4	**Alterazione**	Alterazione non autorizzata dei dati, che può determinare: • la comunicazione di informazioni erronee a enti esterni all'azienda (es. istituzioni, società, persone, ecc..) o al pubblico (Internet); • errori nel trattamento o trattamento non conforme • decisioni errate con effetti sull'Interessato. In alcuni casi l'Alterazione può seguire un Accesso ai dati da parte di soggetti non aventi diritto. In altri casi può essere dovuta ad errori nel trattamento.
5	**Divulgazione**	Comunicazione o diffusione non autorizzate od improprie dei dati personali, non corrispondenti a informazioni di pubblico dominio, verso terze parti, anche se non note o identificabili. In alcuni casi la Divulgazione può seguire un Accesso ai dati da parte di soggetti non aventi diritto. In altri casi può essere dovuta a trattamenti non conformi di dati riservati.
6	**Accesso**	Effettivo accesso (anche in sola visualizzazione) ai dati trattati dall'azienda da parte di soggetti non aventi diritto al momento della violazione. L'Accesso ai dati non implica che si sia verificata anche un'altra violazione quale Distruzione, Alterazione o Divulgazione: il soggetto non avente diritto potrebbe utilizzare a proprio favore le informazioni ricavabili dai dati senza distruggerli, alterarli o divulgarli.

Tabella 20: Tipologie di violazioni e minacce applicabili ai Trattamenti

[7] La cifratura dei dati, per essere efficace, richiede che le chiavi di cifratura siano integre, non violate e non divulgate.

In termini di impatto, come detto sopra ogni violazione può causare conseguenze di varia tipologia. In riferimento a quanto previsto dagli artt.32, 33 e 35, e relativi Considerando, le conseguenze sul trattamento possono essere ricondotte a tre principali categorie o "*scenari di rischio*", in funzione delle proprietà di sicurezza che la violazione può compromettere:

R – perdita di Riservatezza: I dati personali sono divulgati a individui, organizzazioni, enti non autorizzati;

I – violazione dell'Integrità: I dati personali sono incompleti o non corretti o modificati senza le opportune autorizzazioni

D – perdita di Disponibilità: I dati personali non sono accessibili o utilizzabili quando necessario

Ogni violazione può determinare uno o più scenari, sebbene sia possibile identificarne uno prevalente, come nell'esempio:

ID	Tipologia di violazione	Proprietà compromessa (scenario)
1	**Distruzione**	Disponibilità (D)
2	**Indisponibilità**	Disponibilità (D)
3	**Perdita**	Disponibilità (D)
4	**Alterazione**	Integrità (I)
5	**Divulgazione**	Riservatezza (R)
6	**Accesso**	Riservatezza (R)

Tabella 21: Associazione tra tipologie di violazioni e scenari

Connesse con le tipologie di violazione, le *minacce* identificate precedentemente (§Tabella 20) costituiscono pertanto la causa della compromissione delle proprietà di Riservatezza, Integrità e Disponibilità dei dati del Trattamento, sia accidentale sia illecita, causando un danno (fisico, materiale, morale) agli interessati. Ne consegue che valutare il rischio sul trattamento significa, dal punto di vista metodologico, determinare e consolidare i valori di impatto e probabilità sui tre scenari "RID".

9.2.2 Valutazione di impatto

Per ogni trattamento la valutazione di impatto di accadimento degli scenari potrebbe essere eseguita su una scala a più livelli di severità, come nell'esempio:

- ALTO impatto
- MEDIO impatto
- BASSO impatto

In termini generali, per valutare l'impatto sui parametri RID sarebbe necessario considerare se un eventuale data breach potrebbe comportare un danno fisico, materiale o immateriale agli individui che hanno subito la violazione dei propri dati; a titolo di esempio, se la violazione potrebbe portare a casi di discriminazione, perdita di identità o frode, perdita finanziaria o danno alla propria reputazione.

Entrando più nel concreto, per l'attività di valutazione dell'impatto RID di ogni specifico trattamento sono di seguito presentate alcune linee guida:

Scenario	Linee guida
(perdita di) Riservatezza	Per ogni trattamento l'assegnazione di un livello di severità al parametro Riservatezza dovrebbe essere basata sulle seguenti considerazioni: 1) Quanti dati personali potrebbero essere divulgati? 2) Chi sono gli individui i cui dati potrebbero essere divulgati? Staff (dipendenti, collaboratori), dati relativi a propri clienti o fornitori, o dati relativi ai clienti dei propri servizi? 3) Quanto sono sensibili i dati che potrebbero essere divulgati? Sono incluse categorie speciali di dati, data finanziari, informazioni pubbliche…? 4) Che cosa potrebbero rilevare di un individuo a una terza parte se i dati di un individuo fossero divulgati? 5) Che conseguenze potrebbero avere questi individui? Ci potrebbero essere rischi alla salute o alla reputazione, perdite finanziarie o una combinazione di questi o ad altri aspetti della propria vita? La violazione potrebbe comportare un furto di identità o una frode, danni fisici, disturbi psicologici, umiliazione o un danno reputazionale? 6) Ci potrebbero essere conseguenze più ampie quali un rischio alla salute pubblica, o la perdita di fiducia in un servizio che fornite?
(violazione della) Integrità	Per ogni trattamento l'assegnazione di un livello di severità al parametro Integrità dovrebbe essere basata sulle seguenti considerazioni: 1) Quanti dati personali potrebbero essere modificati? 2) Chi sono gli individui i cui dati potrebbero essere modificati? Staff (dipendenti, collaboratori), dati relativi a propri clienti o fornitori, o dati relativi ai clienti dei propri servizi? 3) Che conseguenze potrebbero avere questi individui? Ci potrebbero essere rischi alla salute o alla reputazione, perdite finanziarie o una combinazione di questi o ad altri aspetti della propria vita? La violazione potrebbe comportare un furto di identità o una frode, danni fisici, disturbi psicologici, umiliazione o un danno reputazionale? 4) Ci potrebbero essere conseguenze più ampie quali un rischio alla salute pubblica, o la perdita di fiducia in un servizio che fornite?
(perdita di) Disponibilità	Per ogni trattamento l'assegnazione di un livello di severità al parametro Disponibilità dovrebbe essere basata sulle seguenti considerazioni: 1) Quanti dati personali potrebbero essere indisponibili? 2) Chi sono gli individui i cui dati potrebbero essere indisponibili? Staff (dipendenti, collaboratori), dati relativi a propri clienti o fornitori, o dati relativi ai clienti dei propri servizi? 3) Che conseguenze potrebbero avere questi individui? Ci potrebbero essere rischi alla salute o alla reputazione, perdite finanziarie o una combinazione di questi o ad altri aspetti della propria vita? La violazione potrebbe comportare un furto di identità o una frode, danni fisici, disturbi psicologici, umiliazione o un danno reputazionale? 4) Ci potrebbero essere conseguenze più ampie quali un rischio alla salute pubblica, o la perdita di fiducia in un servizio che fornite?

Tabella 22: Linee guida per la valutazione dell'impatto

9.2.3 Stima della probabilità

Ciascuna violazione, come è possibile vedere in Tabella 20, può essere determinata dall'accadimento di una o più *minacce*; quanto sia possibile che tali minacce possano causare, nel contesto in esame, una violazione è la misura di *probabilità* che deve essere quantificata nel valutare il rischio sul trattamento.

La stima della probabilità deve essere svolta tenendo in particolare considerazione la tipologia di impatti che sono stati valutati: sarà infatti interesse dell'organizzazione prendere in considerazione le conseguenze più significative per l'Interessato, tralasciando la valutazione di rischi a impatto trascurabile. Anche la probabilità deve seguire quindi tale approccio: ad esempio, analizzando la tipologia di evento "malware", tipicamente ad elevata probabilità di accadimento, la probabilità stimata dovrà riferirsi ai casi in cui un'infezione possa effettivamente determinare le conseguenze più significative cui la valutazione di impatto ha fatto riferimento, tralasciando tutti i casi in cui la diffusione del malware possa causare disagi e problemi non rilevanti per l'Interessato.

La probabilità dovrà essere valutata in termini *potenziali,* ovvero senza considerare l'attuazione di specifiche misure di protezione, se la DPIA è svolta per valutare nuovi trattamenti o nuove soluzioni tecnologiche a supporto di un trattamento esistente.

Al contrario, in caso di modifiche rilevanti ad un trattamento in essere, o di cambiamenti significativi ad una soluzione tecnologica esistente, la stima di probabilità potrà tenere conto delle misure di protezione in essere, con lo scopo di verificare che il livello di protezione non sia variato significativamente.

I valori di probabilità determinati su ogni minaccia devono poi essere ricondotti a tre scenari di rischio: l'organizzazione può scegliere diversi criteri di aggregazione, in relazione al fatto che la stima della probabilità sia svolta secondo criteri qualitativi o quantitativi.

9.2.4 Calcolo del Rischio

Nella stima di un rischio solitamente si considerano i seguenti fattori:

- la causa (minaccia) e la relativa probabilità
- la natura dell'effetto (impatto) e la relativa gravità.

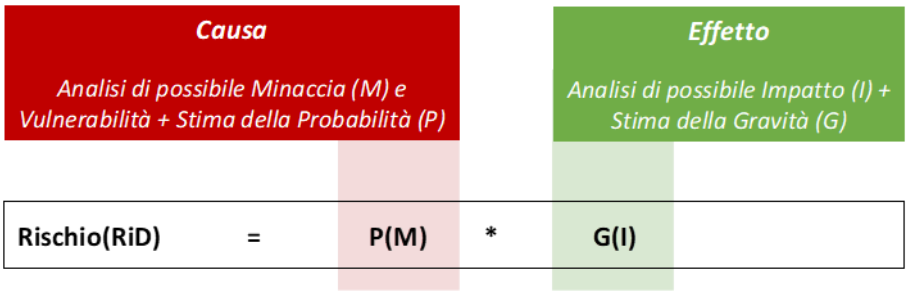

Figura 2: Formula del calcolo del rischio

Solitamente si considera che una minaccia aggredisca un sistema sfruttando una vulnerabilità o comunque una debolezza del sistema informativo: dunque una vulnerabilità può essere vista come una con-causa legata alla mancata risposta adeguata del sistema e nell'analisi viene spesso riportata, per brevità, come elemento descrittivo della minaccia.

Si noti come il risultato di rischio corrisponda ad una terna di valori, in relazione ai tre scenari: si potrà avere ad esempio un esito come il seguente:

Rischio(RID) = (Medio, Alto, Molto Alto)

Se ritenuto opportuno per finalità di reporting, tale risultato può essere aggregato in un unico valore: a tal fine è opportuno evitare criteri complessi che possano portare ad una sotto-valutazione dei rischi più elevati (es: eseguire una media dei risultati). In genere, si suggerisce di utilizzare il valore massimo di rischio tra quelli definiti per i tre scenari. A partire dal precedente esempio:

Rischio(RID) = (Medio, Alto, Molto Alto) ➔ **Rischio = Molto Alto**

Il Rischio è mitigato dai controlli (C) e dalle misure esistenti o previste di default. Di questi occorre stimare l'efficacia (E). Per questo si è soliti considerare il **Rischio inerente (o potenziale)** se calcolato al netto delle misure di mitigazione e il **Rischio residuo (o effettivo)** se a valle di tali misure.

La prima tipologia è quella di solito considerata per la DPIA di nuovi trattamenti e/o nuove tecnologie introdotte su un trattamento in essere e segue la formula descritta in Figura 2.

La valutazione di rischio effettivo viene svolta, al contrario, quando l'analisi è relativa ad una modifica rilevante di un trattamento o di una tecnologia esistente, su cui agiscono delle misure già implementate dall'organizzazione.

Il rischio residuo, infine, è calcolato secondo le medesime modalità del rischio effettivo, di seguito illustrate, da cui differisce solo in quanto, nella procedura di DPIA, ci si riferisce a questa tipologia di rischio a seguito della definizione di ulteriori misure di protezione, laddove necessarie.

In definitiva il Rischio effettivo sarà:

R eff(RID) = P(M) * G (I) / E (C)

Questa trattazione non si estende a considerare i possibili metodi di analisi qualitativi/quantitativi dei singoli parametri ma si limita a identificare in modo sintetico i fattori che devono rientrare nella valutazione.

Si suggerisce, in ogni caso, di valutare il rischio in termini di **coefficienti di probabilità e di gravità** secondo scale numeriche associate a classi di valori e di far corrispondere livelli omogenei del risultato del prodotto di questi fattori a corrispondenti gradi di rischio.

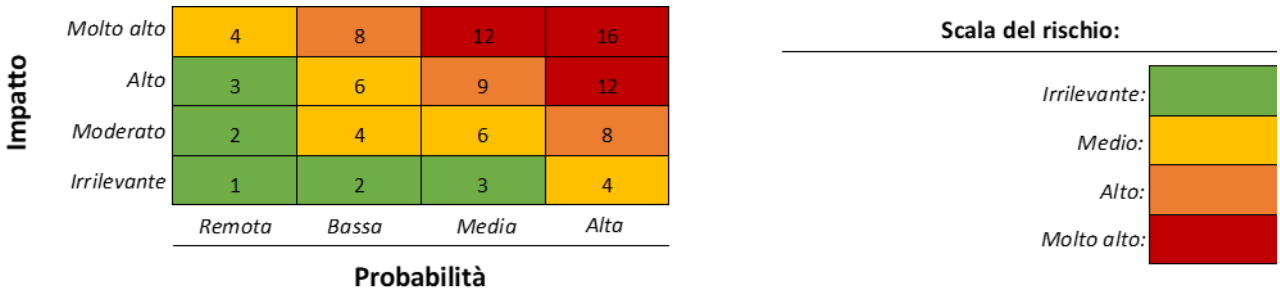

Figura 3: Esempio – Heatmap del calcolo del rischio

Laddove tale approccio sia ritenuto troppo complesso, la *heatmap* in Figura 3 può essere utilizzata per determinare il prodotto dei risultati di probabilità e impatto semplicemente selezionando la casella risultante all'incrocio delle due dimensioni (es: la riga corrispondente alla probabilità "2" e la colonna relativa all'impatto "2" indicano un livello di rischio "giallo", corrispondente a "medio")

9.3 Casi in cui è necessaria la Consultazione Preventiva

Definire un criterio metodologico per determinare il caso in cui sia necessario ricorrere alla Consultazione Preventiva può essere complesso.

Il Considerando 94 del GDPR indica come circostanze che possano costituire indizio per l'obbligatorietà della Consultazione Preventiva l'estensione e la frequenza del trattamento, da cui potrebbe derivare un danno o un'interferenza con i diritti e le libertà della persona fisica.

Nelle [Linee guida WP29] sono citati degli esempi molto utili per la definizione dei criteri utilizzabili per la valutazione del rischio residuo elevato. Dal loro esame si evince infatti che i criteri di valutazione considerati nelle Linee Guida sono sostanzialmente due:

- **l'aspettativa di un danno potenziale elevato**. Si ha quando all'accadere dell'evento che le misure adottate non sono riuscite ad evitare il danno prodotto comporta delle "conseguenze significative, o addirittura irreversibili, e non eliminabili (per esempio, in caso di accesso illecito ai dati che comporti una minaccia per la vita degli interessati, la perdita o sospensione del rapporto lavorativo, un danno finanziario)";
- **l'elevata probabilità che l'evento dannoso possa accadere.** Nell'esempio delle [Linee guida WP29] tale caso di determina quando appare evidente che il rischio paventato si manifesterà, per esempio, a causa dell'impossibilità di ridurre il numero di soggetti in grado di accedere ai dati in ragione delle modalità di condivisione, utilizzo o distribuzione di tali dati, ovvero per l'assenza di salvaguardie contro una vulnerabilità ampiamente nota.

È utile in ogni caso soffermarsi su quest'ultimo esempio desunto dalle [Linee guida WP29], in quanto si rileva come non venga richiesto di effettuare una particolare analisi per il calcolo delle probabilità. Non occorrono pertanto particolari calcoli matematici, se appaia evidente che il rischio possa verificarsi, a causa della constatazione delle circostanze attuali o della considerazione dei precedenti già accaduti. Basta pertanto una valutazione basata sul buon senso e su ciò che risulta evidente già a prima vista.

Ovviamente i due criteri (danno potenziale ed elevata probabilità) devono entrambi essere presenti. Non potrà pertanto essere valutata come situazione di rischio elevato quella in cui il danno ipotetico sia molto grave ma con una probabilità estremamente scarsa che possa verificarsi. Così come non si avrà rischio elevato in presenza di un danno molto probabile ma dalle conseguenze stimabili molto lievi.

Più complesso è determinare la necessità quando almeno una delle due dimensioni del rischio (probabilità o impatto) non risulti al massimo valore possibile. In questo caso, l'obbligatorietà dell'accountability impone l'adozione di un approccio analitico basato su un criterio predeterminato e che consenta la ripetibilità della valutazione.

In relazione alle modalità di calcolo del rischio precedentemente definite (§9.2.4), l'organizzazione può stabilire, sulla heatmap di calcolo del rischio e/o sulla scala dei valori di rischio, un limite di adeguatezza (o limite di rischio, o propensione al rischio) che sia rispondente a quanto richiesto dal Regolamento.

La definizione di questo valore può essere basata sulla valutazione di rischio condotta periodicamente per rispondere ai requisiti dell'art.32 del GDPR, che potrà costituire un benchmark di riferimento rispetto ai rischi correntemente gestiti dall'organizzazione. Così, ad esempio, se l'analisi del rischio condotta ai fini

dell'art.32 non individua in nessun caso un rischio superiore ad un valore "medio", la soglia di adeguatezza potrà essere posizionata corrispondentemente anche per i nuovi trattamenti oggetto di DPIA.

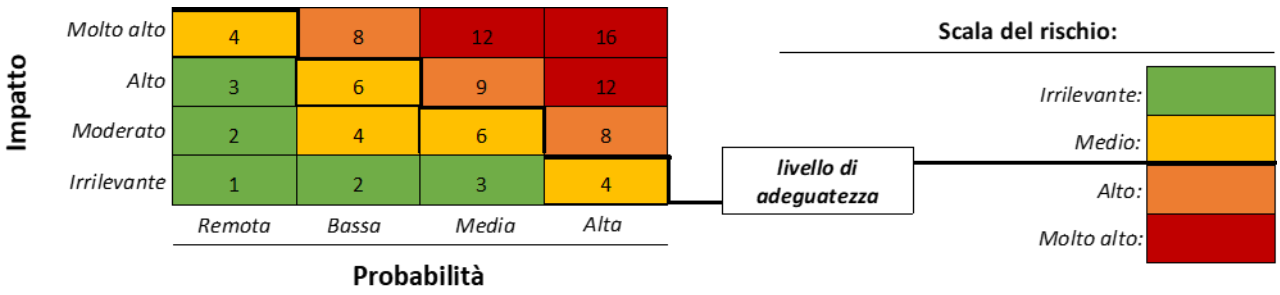

Figura 4: Esempio – Adeguatezza del rischio

È evidente quindi che ogni valutazione che individui un livello di rischio superiore al limite di adeguatezza definito renderà necessario il ricorso alla Consultazione Preventiva. Ulteriori soglie (a livelli di rischio inferiori) possono essere definite in modo cautelativo, per esempio per identificare i casi in cui, prima di stabilire se non sia necessaria la Consultazione Preventiva, sia opportuno o meno condividere la valutazione con ulteriori stakeholder e/o specialisti.

9.4 Misure per la protezione dei trattamenti

Il Titolare che, a seguito della valutazione di rischio potenziale, debba identificare le misure idonee per ridurre probabilità e impatti, deve innanzitutto considerare che l'ambito di scelta non debba essere ridotto alle sole soluzioni tecnologiche per la sicurezza ICT.

È infatti opportuno distinguere le attività e le soluzioni per la sicurezza dei dati (riferite ad un ambito di gestione informatica dei dati in genere) e le attività e le soluzioni per la protezione dei dati (riferite ad un ambito più esteso relativo ai dati personali)

Nell'attuale Codice sulla Protezione dei Dati Personali si parla di misure minime (di sicurezza) e di misure idonee dove il riferimento è quasi esclusivamente fatto alla sicurezza dei dati e dei sistemi informativi o tecnologici in genere, intesi come strumenti prevalenti del trattamento (benché nella definizione corrente siano citati anche i trattamenti privi dell'ausilio degli strumenti informatici). Già nell'attuale ordinamento è tuttavia presente il concetto fondamentale di misure di sicurezza adeguate, sottintendendo al fatto che la misura deve essere proporzionata al rischio.

Nel testo del GDPR gli aspetti di sicurezza dei dati (art. 32) e gli aspetti di protezione dei dati (art. 35) vengono trattati in due sezioni diverse anche se in entrambi i casi viene riferita la necessità di eseguire

valutazioni di rischio. La novità è che questa separazione permette di mettere meglio in evidenza le nuove misure suggerite dal GDPR che superano il concetto quasi riduttivo di misure di sicurezza per diventare più appropriate misure di protezione.

È bene ricordare che:

La DPIA deve contenere la caratterizzazione di tutte le operazioni di trattamento previste, una valutazione del rischio, le misure di sicurezza, le garanzie, i controlli e le soluzioni necessari alla protezione e alla sicurezza dei dati personali

Tutto ciò considerato, e tenuto anche conto delle misure suggerite in [Enisa Handbook], i controlli che il Titolare deve valutare per mitigare i rischi sul trattamento, devono comprendere:

1. Misure e controlli di tipo organizzativo, a loro volta raggruppabili in:
   a. **Organizzazione e governance:** specifici ruoli e responsabilità all'interno dell'organizzazione, controlli interni di supervisione, governance dei progetti, regole di interazione e le rispettive responsabilità in caso di contitolarità di un trattamento
   b. **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
   c. **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.

Con riferimento al **controllo periodico, al monitoraggio e alla correlazione o alle aggregazioni statistiche:** nel testo non è molto evidente e si incontrano solo riferimenti al controllo da parte dell'Interessato, al monitoraggio da parte delle Autorità di Controllo e alle aggregazioni statistiche (al Considerando 13, 24, 71, 75, 162 e all'art. 39, si parla del controllo "interno", cioè a livello aziendale, del rispetto del Regolamento in citazioni piuttosto sintetiche); pur tuttavia si considera essenziale considerare questi interventi tra le misure organizzative.

2. Misure e controlli di tipo tecnologico, come, ad esempio:
   a. tenere aggiornato il software, la configurazione delle reti e dei sistemi informatici,
   b. assicurare l'efficienza degli impianti e dei dispositivi
   c. disattivare i servizi di sistema non necessari
   d. dismettere i servizi o il software non usati o comunque obsoleti
   e. memorizzare le password in registri di sistema protetti e non accessibili dagli utenti
   f. prevedere meccanismi di autenticazione robusta
   g. accertare l'appropriatezza dei siti in base al trattamento previsto dei dati
   h. modificare i settaggi e le credenziali di default
   i. eseguire test di vulnerabilità o di stress dei sistemi

j. neutralizzare vulnerabilità note (es. SQL injection)
k. configurare servizi di trasmissione o di comunicazione protetti (es. SSL, TLS, SFTP)

3. Misure e controlli sui dati e sugli archivi, come, ad esempio:
   a. decidere di non raccogliere o memorizzare specifici tipi di informazioni se non necessarie
   b. definire periodi di conservazione mirati allo stretto tempo necessario per poi prevedere la distruzione
   c. dare garanzia della qualità dei dati
   d. eseguire i backup, partizionare gli archivi dei dati
   e. controllare gli accessi logici
   f. assicurare la possibilità di de-indicizzazione dei dati quando richiesto
4. **Anonimizzazione:** rimozione o mascheratura delle informazioni personali quando non necessarie (ad esempio la mascheratura dell'indirizzo IP nasconde localizzazione geografica di un utente)
5. **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)
6. **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.
7. **Misure e controlli di sicurezza fisica**, come, ad esempio sui supporti cartacei, sugli accessi fisici, sulla sicurezza degli impianti, dell'hardware e dei macchinari, protezione da fonti di rischio non umane etc.

Quale cifratura per il GDPR?

Si noterà che il documento non include la cifratura tra i controlli sui dati e sugli archivi, né sui controlli di tipo tecnologico. Ai fini del GDPR non è infatti sufficiente un qualunque tipo di cifratura, ma tale misura va valutata in relazione alle minacce che intende contrastare. Ad esempio, la cifratura del file system e, più in generale, ogni soluzione c.d. di "cifratura trasparente" è adeguata a mitigare il furto (fisico) di supporti di memorizzazione, ma non la maggior parte degli attacchi logici (se si viola un account legittimo di un sistema, si avrà accesso al file system "in chiaro").

A livello di applicazione, per proteggere i dati da attacchi logici, la cifratura dovrebbe essere una funzionalità dell'applicazione stessa, in grado di consentire l'accesso al dato in chiaro solo a specifici utenti. Per quanto quindi più efficace, anche in tal caso un amministratore infedele potrebbe avere accesso alle chiavi di decifratura contenute in file di configurazione e quindi potenzialmente a tutti i dati personali.

9.4.1 Misure di protezione "by default"

Il GDPR fa evolvere il concetto di misura minima.

Occorre far riferimento all'Art. 5 dove viene arricchito l'insieme dei princìpi generali che devono esser soddisfatti per qualunque tipo di dato, per qualunque tipo di trattamento e per qualunque finalità: questi aspetti ci portano al concetto di privacy by default, che non possono essere esclusi nel perimetro di valutazione della DPIA, anche in relazione al calcolo del rischio residuo. In termini sommari, è possibile assumere che come l'attuale Codice di protezione dei dati personali richiede che le misure minime di sicurezza (di cui agli art.33, 34, 35, 36 e al Disciplinare Tecnico – Allegato B della legge 196/2003) devono arricchirsi, quando necessario, di ulteriori misure idonee, così i principi generali riportati all'Art. 5 e al Considerando 78 e 108 del GDPR (dunque riferibili alla privacy by default o per "impostazione predefinita" richiamata dall'art.25 e dal Considerando 78) devono integrarsi con le misure identificate a seguito della procedura di DPIA.

Possiamo sintetizzare queste misure nel rispetto dei principi di: **minimizzazione, liceità e trasparenza, compatibilità** (dei trattamenti alle finalità), **sicurezza e contrasto all'uso illecito, accuratezza e aggiornamento, periodo di conservazione, prevalenza dell'interesse pubblico**. Ne consegue che il soddisfacimento dei seguenti principi, applicabili *by default* nel trattamento dei dati personali, può essere considerato una misura necessaria ma non sufficiente:

1) I dati personali devono essere trattati in modo lecito e legittimo. Questo comporta che:

- siano definite le finalità di ciascun trattamento
- sia data trasparenza agli interessati circa i trattamenti applicati ai loro dati
- siano definite le condizioni per gli specifici trattamenti
- siano gestiti i consensi individuali al trattamento
- siano considerati prevalenti gli interessi sociali

2) I dati personali devono essere ottenuti solo per i trattamenti specificati e non devono essere trattati in modo diverso o incompatibile con lo scopo dichiarato. Questo comporta che debba essere verificato se lo scopo di una nuova iniziativa è coperto dai trattamenti già dichiarati e se eventuali nuovi scopi potenziali sono stati identificati

3) I dati personali devono essere adeguati, pertinenti e non eccessivi rispetto allo scopo per cui sono trattati (minimizzazione dei dati soggetti a trattamento). Questo comporta che:

- l'informazione che si sta usando sia di qualità adeguata allo scopo per cui è usata
- siano definiti quali dati non servono senza compromettere lo specifico trattamento

4) I dati personali devono essere accurati e, quando necessario, tenuti aggiornati. Questo comporta che:

- debba esser definito un modo per controllare la correttezza dei dati quando ottenuti dagli interessati o da altre fonti
- se si sta ottenendo nuovo software sia possibile correggere i dati se necessario

5) I dati personali trattati per qualunque scopo non devono essere conservati per un periodo maggiore di quanto sia necessario rispetto agli scopi intesi. Questo comporta che:

- siano definiti i periodi di conservazione in modo compatibile con le esigenze del trattamento
- siano definiti i meccanismi, prevalentemente automatici, per cancellare le informazioni in conformità ai periodi di conservazione previsti

6) I dati personali devono essere trattati in conformità ai diritti degli interessati. Questo comporta che:

- i sistemi consentano di rispondere alle richieste di accesso da parte degli interessati, di limitare o di opporsi al trattamento, di rettificare i propri dati, di richiederne la cancellazione (diritto all'oblio), di esercitarne il diritto di portabilità ad altro operatore
- se un progetto include una finalità di marketing, deve esistere una procedura che consenta agli interessati di escludere che i propri dati siano usati per quello specifico scopo
- se un Interessato ne chiede la rimozione (oblio) questa deve essere garantita

7) Devono essere adottate adeguate misure tecniche e organizzative per contrastare l'uso o l'accesso non autorizzato o illecito dei dati personali e per prevenire la perdita o la distruzione o il danneggiamento degli archivi anche accidentale. Questo comporta che:

- vengano applicate tecniche di pseudonimizzazione fin dalle prime fasi di trattamento
- i sistemi siano provvisti di sistemi di protezione per prevenire i rischi di sicurezza (accessi, alterazioni, perdite non volute)
- siano date istruzioni ed effettuato addestramento per assicurare che lo staff tecnico conosca come operare con i sistemi esistenti e quelli nuovi in modo sicuro
- sia consentito al responsabile del trattamento di applicare e migliorare le caratteristiche di sicurezza

8) I dati personali non devono essere trasferiti in un paese al di fuori della UE a meno che quel territorio assicuri un adeguato livello di protezione per i diritti e le libertà degli interessati in relazione ai trattamenti previsti. Questo comporta che:

- sia valutata l'esigenza eventuale di trasferire i dati della UE
- nel caso, sia definita la modalità con cui viene assicurata la protezione dei dati

10 Strumenti a supporto

Uno strumento progettato per supportare le organizzazioni nella DPIA dovrebbe avere come obiettivo la **governance della procedura di DPIA rendendola trasparente, comprovabile e documentata**.

Lo strumento individuato deve essere un valido supporto alle attività previste dalla procedura, in particolare in merito:

- alla raccolta e all'organizzazione di informazioni in modo efficace, nonché alla classificazione dei dati personali, coerentemente con il Registro dei Trattamenti
- alla descrizione sistematica delle operazioni previste e delle finalità del trattamento
- alla valutazione della necessità, proporzionalità e non eccedenza dei trattamenti
- alla valutazione dei rischi per i diritti e le libertà degli interessati
- alla determinazione dei requisiti utili per la definizione delle misure tecniche, organizzative e di processo necessarie per gestire i rischi associati al perimetro logico e fisico in cui sono operati i trattamenti.

10.1 Caratteristiche dello strumento

Le caratteristiche principali che uno strumento a supporto della procedura di DPIA dovrebbe avere sono:

- essere pienamente integrato con il sistema a supporto della Governance GDPR, in particolare:
  - con i principi e processi di **Privacy by Design** e **Privacy by Default** sviluppati dal contesto organizzativo;
  - con l'esistente Registro dei Trattamenti;
  - con il registro dei **Data Breach** in quanto una perdita di dati accertata potrebbe innescare la necessità di un riesame a fini precauzionali;
  - con **l'analisi periodica del rischio ex art.32**, in quanto una rilevazione a posteriori di nuove tipologie di dati trattati potrebbe comportare la necessità di una nuova DPIA
- essere eventualmente integrabile con i sistemi pre-esistenti di IT Service Management:
  - Asset Management e CMDB
  - tool a supporto dei processi di Business Continuity
  - Service Desk
- mantenere la correlazione tra la DPIA ed il trattamento oggetto della stessa, con storicizzazione di tutte le analisi effettuate, ovvero:
  - permettere la consultazione di tutte le procedure DPIA effettuate nel tempo
  - tenera traccia di quanto analizzato, delle considerazioni e verifiche effettuate comprese eventuali iterazioni con l'Autorità di Controllo
  - consentire la Firma Digitale (con apposizione di Marca Temporale) degli esiti registrati ai fini della dimostrabilità delle considerazioni effettuate
- essere costantemente allineato con il modello dell'organizzazione aziendale in modo da individuare correttamente i ruoli da coinvolgere tramite interscambi automatizzati con il sistema informativo aziendale, rendendo così possibile l'invio di messaggi di controllo e notifica

- gestire e documentare le attività svolte nell'ambito della procedura di DPIA con particolare focus verso:
    - i dati raccolti e le finalità della raccolta
    - i ruoli coinvolti e le relative responsabilità
    - le metodologie
    - le tempistiche
    - il work-flow della procedura
- supportare la procedura per casistiche distinte:
    - DPIA per nuovi trattamenti
    - DPIA dei trattamenti in essere (utile per recuperare il pregresso nella fase iniziale)
    - DPIA per modifiche sostanziali di elementi fondamentali dei trattamenti in essere (adozione nuove tecnologie, aggiunte nuove tipologie di dato e finalità, modifica volumi dei dati trattati)
    - eventi significativi con impatto sui trattamenti oggetto di precedenti DPIA (es. data Breach)
- comprendere una funzionalità che permetta di realizzare l'analisi necessaria a determinare e formalizzare l'effettiva necessità di operare la valutazione di impatto
- prevedere l'utilizzo di questionari di valutazione personalizzabili per guidare la raccolta dati e storicizzare le risposte ottenute. Tali questionari dovrebbero prevedere interfacce/accessi diversi in funzione dei ruoli degli intervistati per facilitare l'imputazione dei diversi dati, peculiari per ogni ruolo, che concorrono all'elaborazione della DPIA
- prevedere la possibilità di importare nello strumento lavori pregressi dell'azienda realizzati mediante strumenti di Office Automation (excel, word, ecc.)
- prevedere una metodologia utile a determinare uno "scoring" relativo alla rischiosità intrinseca del trattamento
- permettere la definizione delle esigenze in termini di misure di sicurezza in modalità utilizzabili dalle funzioni che realizzeranno le soluzioni a supporto del trattamento:
    - produzione di Requisiti – Demand
    - produzione di supporti utilizzabili anche come requisito al fornitore per eventuali trattamenti in outsourcing
    - produzione di Dashboard e Report diversi, in relazioni alle diverse funzioni aziendali
- permettere la memorizzazione di ogni comunicazione intercorsa con l'Autorità di Controllo ai fini delle eventuali verifiche di liceità del trattamento
- avere una funzionalità che permette di produrre la richiesta di Consultazione Preventiva, in conformità con quanto richiesto dal Regolamento.

10.2 Utilizzo di un prodotto DPIA fin dal primo periodo di adeguamento

Essendo quella di DPIA una procedura basata sul miglioramento continuo, l'utilizzo di uno strumento viene ritenuto sicuramente opportuno sin dalla fase iniziale, cioè sin dal primo censimento delle informazioni e dei dati trattati dall'azienda in modo da poter pianificare e gestire un piano di analisi. A tal fine è fondamentale l'integrazione con il Registro dei Trattamenti, che consente di individuare i trattamenti che possono determinare rischi elevati per i diritti e le libertà degli interessati. Inoltre, l'utilizzo di uno strumento per condurre una DPIA permetterebbe anche l'esecuzione di eventuali operazioni periodiche o schedulate, per evitare dimenticanze o errori.

Infine, in tale scenario il DPO avrebbe a disposizione uno strumento di overview e monitoraggio dei Processi DPIA in corso, con possibilità di intervento nei casi di mancata tempestività nella gestione degli stessi, in modo da giungere ad una situazione di conformità verificabile nel più breve tempo possibile.

Autori e Contributori

In rigoroso ordine alfabetico, si riportano di seguito e si ringraziano Coordinatori, Editor, Autori e Contributori.

Coordinatori e Editor

Andrea Antonielli, Ricercatore Osservatorio Information Security & Privacy, Politecnico di Milano
Luca Bechelli, Collaboratore Osservatorio Information Security & Privacy Politecnico di Milano, Direttivo e Comitato Tecnico-Scientifico Clusit
Giorgia Dragoni, Ricercatrice Osservatorio Information Security & Privacy, Politecnico di Milano
Gabriele Faggioli, Responsabile Scientifico Osservatorio Information Security & Privacy Politecnico di Milano, Presidente Clusit
Vinicio Mazzei, IT Risk, Security and Compliance Manager, Saipem
Alessandro Piva, Direttore Osservatorio Information Security & Privacy, Politecnico di Milano
Antonio Ricotta, Data Manager, Automobile Club d'Italia
Enrico Luigi Toso, IT regulatory risk and control specialist, DB CONSORZIO S.C.a R.L. (gruppo DEUTSCHE BANK S.p.A.)

Autori e Contributori

Andrea Abate, Sr. Advisor, SINERGY S.p.A. – Lutech Group
Sergio Brizio, Account & Project Manager, TESISQUARE
Marco Ceccon, Sr. Advisor, SINERGY S.p.A. – Lutech Group
Elena Colazzo, Security Consulting Consultant, Accenture
Germana Di Salvo, Security and Privacy Consultant, Spike Reply
Mariangela Fierro, Security Senior Manager, Application Security Lead in ICEG (Italy, Central Europe, and Greece), Accenture
Vincenzo Galante, Security and Privacy Consultant, Spike Reply
Elisa Garavaglia, Chief Information Security Officer, Axa Global Direct
Gianluca Giaccardi, Chief Product Officer, TESISQUARE
Alessandro Gioso, Senior Principal System Engineer, Symantec Italia S.r.l.
Ivan M. Greggio, Compliance Manager, NEST2 S.p.A.
Giovanni Gugliotta, ICT Architecture & Security Manager, Ermenegildo Zegna
Fulvio Maffiodo, Security and Privacy Consultant, Spike Reply
Andrea Mercurio, Responsabile Security Operations and Products, AlmavivA
Stefano Minini, Partner / Advisory Risk & Compliance, BDO Italia S.p.A.
Giuseppe Morimondi, Head of IT Infrastructure & Information Security Officer, Bayer S.p.A.
Cosimo Orecchia, Manager / Advisory Risk & Compliance, BDO Italia S.p.A.
Alessandro Maria Ricci, Security Consultant, Horizon Security
Riccardo Roncon, Responsabile Sicurezza IT, ITAS Mutua – Gruppo ITAS Assicurazioni
Corrado Salvemini, Responsabile Sicurezza delle Informazioni, Carrefour Italia
Manuela Santini, Collaboratore Osservatorio Information Security & Privacy
Renato Sesana, Partner BRS, Grant Thornton Financial Advisory Services
Alessandra Toma, Avvocato, Poste Italiane S.p.A. (Sicurezza Informatica)
Gabriele Tori, Collaboratore Osservatorio Information Security & Privacy
Marco Vivian, Financial Lines Underwriter, Global Corporate & Commercial Italy - Generali Italia S.p.A.