Allegato 4 alla Disposizione n. 40 del 01 Ottobre 2018

"Indicazioni operative per redazione di linee guida per la valutazione di impatto del rischio (DPIA)

Versione del documento	1.0
Data emissione	01/10/2018
Stato del documento	Definitivo
Nome del file	*"Indicazioni operative per redazione di linee guida per la valutazione di impatto del rischio (DPIA).docx"*

Sommario

1 Contesto di riferimento....3
2 Premessa....5
2.1 Oggetto e obiettivo del documento....5
2.2 Ambito di applicazione del documento....5
2.3 Validità e Aggiornamento del documento....6
2.3.1 Soggetti Approvatori....6
2.3.2 Soggetto verificatore....7
2.3.3 Versione del documento....7
3 Quadro normativo....8
3.1 Definizioni normative di riferimento....8
3.2 Adempimenti prescritti dalla normativa....11
3.3 Soggetti attivi....16
3.3.1 Ruoli coinvolti....16
4 Standard utilizzabili....19
4.1 ISO/IEC 29134:2017....19
4.1.1 Obiettivo della ISO/IEC 29134....19
4.1.2 Sintesi dei Contenuti della ISO/IEC29134....19
4.1.3 Utilizzo della ISO/IEC 29134....20
5 Contenuti ed interazioni del processo DPIA....21
5.1 Che cosa è la DPIA e a che cosa serve....21
5.2 Quando si effettua la DPIA....21
5.3 Quando è obbligatorio effettuare un DPIA....23
5.4 Quando è possibile non effettuare un DPIA....25
5.5 I contenuti della DPIA....26
5.6 DPIA e Analisi dei rischi....27
5.6.1 Metodologia di analisi dei rischi nella DPIA....27
5.6.2 Strumenti a supporto di un processo DPIA....28
5.6.3 Integrazione dell'analisi dei rischi DPIA con l'analisi dei rischi del ISMS....29
5.7 DPIA e altri adempimenti/processi GDPR....30
5.7.1 Registro dei trattamenti....30
5.7.2 Data breach e incident management....30
6 Processo DPIA....32
6.1 Il processo DPIA....32
6.2 Valutazione preliminare....33
6.2.1 Raccolta delle informazioni per la valutazione preliminare....33
6.2.1 Valutazione della conformità....34
6.2.2 Valutazione dell'obbligo/esenzione DPIA....35
6.3 Esecuzione DPIA....36

6.3.1 Raccolta delle informazioni per l'analisi dei rischi....36
6.3.2 Valutazione dei rischi....37
6.3.3 Valorizzazione contromisure e rischio residuo....37
6.3.4 Valutazioni e Piano di trattamento dei rischi....38
6.4 Formalizzazione dei risultati....38
6.5 Consultazione preventiva....39
6.5.1 Quando è necessaria la consultazione preventiva....39
6.5.2 Contenuti della consultazione preventiva....40
6.5.3 Processo della consultazione preventiva....40
6.6 Revisione del processo DPIA....41
7 Aspetti sanzionatori....43
7.1 Violazioni....43
7.2 Sanzioni....43
8 Allegati....44

1 Contesto di riferimento

La presente introduzione è necessaria al fine di inquadrare sotto un profilo contestuale il Regolamento Europeo nr. 679/2016 (*General Data Protection Regulation* meglio noto come GDPR), entrato in vigore il 24 maggio 2016 ma pienamente applicabile a partire dal 25 maggio 2018, che andrà ad uniformare ed armonizzare le legislazioni dei Paesi Europei con riguardo alla materia di protezione dei dati personali.

L'esigenza di una rivisitazione della normativa in materia di protezione dei dati personali si apprezza in relazione al mutato contesto politico, economico e sociale di riferimento del tutto differente rispetto a quello degli anni 90, periodo nel quale l'impatto e la cultura del dato non era così centrale come invece è oggi; ciò è dato dallo sviluppo repentino delle moderne tecnologie (in primis mobile devices, smartphone, tablet, social network, ecc.; in seconda battuta strumenti IOT (Internet of things), sistemi di Data Analytics e Big Data, Business Intelligence, ecc.) nemmeno immaginabile negli anni che chiudevano il secolo scorso, grazie alle quali è pensabile e apprezzabile anche il valore economico del dato.

Accanto a questa constatazione di tipo "sociologica" va da sé che il programma di integrazione europeo che vede come base di partenza la creazione di un mercato unico europeo, da realizzarsi inizialmente attraverso la libera circolazione di persone, servizi e merci, non possa non tenere in considerazione anche della libera circolazione del "dato personale" così come puntualmente sottolineato dai "considerando" del Regolamento fino anche alla maggiore rilevanza di questa libertà rispetto alla tutela del dato in sé come diritto soggettivo (considerando nr. 4).

A seguito di questa breve introduzione storica/sociologica ed avviando la riflessione sul terreno giuridico, in prima battuta preme precisare che la scelta di tipologia di intervento del legislatore Europeo risulta alquanto significativa nella misura in cui, con la scelta di un Regolamento, non viene lasciata agli Stati membri alcuna possibilità di intervento (se non in termini di adozione di provvedimenti volti ad armonizzare la normativa nazionale) stante la piena applicabilità del Regolamento a dispetto della presenza, come successo invece in passato in materia di protezione di dati personali, di direttiva europea (95/46) che necessitava di un atto di recepimento (Dlgs. 196/2003, meglio noto come codice della privacy).

In riferimento invece ai contenuti della presente legge si sottolinea come l'approccio che propone il Regolamento sia del tutto differente rispetto a quello proposto dal codice privacy nazionale.

Principio fondamentale che impernia l'intera normativa è infatti quello di **accountability** (la capacità di rendere conto delle azioni) il quale illustra, di fatto, una responsabilizzazione dei soggetti coinvolti in materia di protezione di dati personali; questi infatti secondo il dettato normativo non dovranno più ragionare in termini di mero adempimento alla norma di riferimento, come invece accaduto fino ad oggi con riferimento ai dettami del codice della privacy.

In tal senso il principio di accountability deve essere letto sotto un duplice profilo: esso non solo è il principio che ispira l'adeguamento/l'adempimento degli enti alla normativa europea, ma è anche il punto di partenza per **dimostrare** la compliance (il rispetto, l'aderenza) dell'ente/organizzazione alla norma europea.

Ciò significa che un ente/organizzazione può disattendere una prescrizione del Regolamento, avendo tuttavia cura di indicare in apposito documento le ragioni in forza delle quali si ritiene di non dover seguire il dettato normativo.

Oltre quindi a lasciare uno spazio di intervento ai soggetti Titolari del trattamento in ordine alla scelta di adozione delle novità introdotte dal GDPR, obbligandoli comunque ad una seria riflessione in ordine alle politiche da adottare per essere conformi al Regolamento, si segnalano a titolo esemplificativo alcuni istituti del tutto lontani dalla logica "burocratica" del Codice Privacy.

Si richiama inevitabilmente quindi al processo di istituzione e conservazione del **registro di trattamenti** in capo ai titolari e responsabili del trattamento che consente quindi di avere una chiara panoramica dei trattamenti di dati personali che vengono effettuati all'interno dell'organizzazione che fa per l'appunto capo al titolare o al responsabile; a ciò si aggiunga l'organizzazione del processo che porta il titolare o responsabile del trattamento in contatto con l'autorità garante e con i soggetti interessati in caso di violazione di dati nota anche come ***Data Breach***, che come sarà meglio trattato nel proseguo dell'elaborato non si limita al solo furto di dati.

Ancora, la previsione di una conduzione di **Valutazione di impatto** per quei trattamenti che presentino un rischio elevato per i diritti e le libertà degli interessati.

Sotto il profilo dei soggetti attivi e protagonisti, in questo nuovo quadro, viene introdotta la figura del ***Data Protection Officer – DPO*** (obbligatorio per tutti gli enti pubblici) il quale si andrà a configurare da un lato come consulente per i Titolari e i Responsabili dei trattamenti, attraverso una continua verifica della *compliance* dell'organizzazione/ente rispetto ai dettami del GDPR, ma anche come punto di riferimento per i soggetti interessati rappresentando per questi ultimi il referente interno dell'organizzazione con il quale interfacciarsi in materia di protezione dei dati personali.

In conclusione, come già emerso dalla disamina condotta, a mutare è l'atteggiamento della normativa rispetto alla tematica della protezione dei dati personali, esso infatti impone una riflessione preventiva rispetto alla materia *de qua*, che porta quindi ad adattare la propria organizzazione in base alle opportunità che si intendono cogliere, lasciando non solo ampi spazi di autonomia ai soggetti Titolari/Responsabili ma anche abbandonando quell'approccio di mero adempimento richiesto dalla normativa. In sintesi, non è sufficiente avere "le carte a posto".

2 Premessa

2.1 Oggetto e obiettivo del documento

A partire dal 25 maggio 2018, tutti i Titolari del trattamento – pubblici e privati – dovranno applicare quanto previsto dall'articolo 35 e 36 del GDPR relativamente agli aspetti di valutazione d'impatto sulla protezione dei dati e consultazione preventiva, così come previsto anche dalla direttiva 2016/6803.

Una valutazione d'impatto sulla protezione dei dati è un processo volto a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, analizzando detti rischi e determinando le misure necessarie per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione, in quanto sostengono i titolari del trattamento non soltanto nel rispetto dei requisiti del regolamento generale sulla protezione dei dati, ma anche al fine di dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24). In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo volto a garantire e dimostrare la conformità ed in generale il principio di "**accountability**".

Inoltre, laddove una valutazione d'impatto sulla protezione dei dati riveli la presenza di rischi residui elevati, il titolare del trattamento sarà tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento (articolo 36, paragrafo 1).

Il presente documento di indirizzo tiene quindi conto di quanto previsto dalla normativa di riferimento citata ma resta comunque soggetta a possibili futuri aggiornamenti sulla base di eventuali interventi in materia da parte del Garante Privacy.

2.2. Ambito di applicazione del documento

Il presente documento di indirizzo ha lo scopo di fornire indicazioni utili in grado di coadiuvare Regione Toscana e gli Enti ad essa collegati, nella più veloce e completa definizione di un processo - e relative procedure - per la gestione di tutte le attività sottostanti gli aspetti di Data Protection Impact Assessment (d'ora in poi definito anche sinteticamente DPIA).

Ai sensi dell'art. 35 par. 1 si definisce che "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali*".

Quindi, l'applicazione di un processo DPIA diventa obbligatoria tutte le volte che ci troviamo in presenza di un trattamento che vuoi per via della tipologia di dati trattati, vuoi per le modalità di trattamento o per le finalità, comporta un rischio elevato per i diritti e le libertà delle persone fisiche.

Per poter inquadrare meglio l'obbligatorietà dell'applicazione di un processo DPIA si può fare riferimento a quanto espresso dalla linea guida WP248 17/IT (gruppo articolo 29) che riporta le principali casistiche di trattamenti che possono comportare un rischio elevato per i diritti e le libertà delle persone fisiche:

- Profilazione degli interessati
- Realizzazione di valutazioni automatiche con effetti legali o comunque significativi
- Monitoraggio sistematico degli interessati
- Trattamento dati sensibili
- Elaborazione di dati su larga scala utilizzando più fonti di dati di origine diversa
- Uso di nuove tecnologie o soluzioni organizzative
- Trasferimento dati oltre i confini UE
- Trattamenti che impediscono all'interessato di esercitare un proprio diritto o l'uso di un servizio o l'attivazione di un contratto.

Le presenti indicazioni si applicano quindi in tutti i casi in cui Regione Toscana e gli enti ad essa collegati si dovessero trovare a valutare trattamenti che in qualche maniera ricadono nell'ambito delle categorie sopra citate o che comunque in generale possono presentare, anche potenzialmente, rischi elevati. Ulteriori approfondimenti a riguardo della applicazione del processo di DPIA si possono trovare all'interno del par. 5.2

Il presente documento richiama e sottolinea inoltre le principali responsabilità da definirsi all'interno di apposite linee guida e/o procedure a cura di Regione Toscana e Enti ad essa collegati al fine di regolamentare i processi DPIA.

2.3. Validità e Aggiornamento del documento

2.3.1. Soggetti Approvatori

Approvatore	Referente e Ruolo	Data

2.3.2. Soggetto verificatore

Verificatore	Referente e Ruolo	Data

2.3.3.Versione del documento

Stato	Versione	Autore	Descrizione	Data

3. Quadro normativo

- REGOLAMENTO 2016/679/UE: Articoli 35 e 36
- Considerando C84, C89, C90, C91, C92, C93, C94, C95
- WP248 - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679

3.1. Definizioni normative di riferimento

Anonimizzazione: tecnica di trattamento dei dati personali tramite la quale i dati personali non possano più essere attribuiti a un interessato specifico, nemmeno attraverso l'utilizzo di informazioni aggiuntive.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Autorità di controllo: è l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Cifratura: tecnica di trattamento dei dati personali tramite la quale i dati personali vengono resi non intellegibili a soggetti non autorizzati ad accedervi.

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Contitolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altri determina le finalità e i mezzi di trattamento dei dati personali;

Data Breach: è un incidente di sicurezza in cui i dati personali vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato o persi accidentalmente.

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di

identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

DPIA: acronimo di Data Protection Impact Assessment (valutazione di impatto sulla protezione dei dati).

Interessato: persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

Misure di sicurezza: misure tecniche ed organizzative adeguate per garantire un livello di sicurezza dei dati trattati adeguato al rischio.

Nuovo trattamento: trattamento di dati personali che comporta l'utilizzo di nuove tecnologie o è di nuovo tipo e in relazione al quale il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.

Privacy by-design / by-default: l'incorporazione della privacy a partire dalla progettazione di un processo aziendale, con le relative applicazioni informatiche di supporto. La prima introduce la protezione dei dati fin dalla progettazione per caso specifico, la seconda per impostazione predefinita di una pluralità di casi tra loro omogenei.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del regolamento;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Responsabile della Conservazione documentale: si tratta della figura preposta alla gestione e supervisione del processo di conservazione dei documenti (digitali o cartacei).

Security Manager: è la figura preposta alla gestione e supervisione del processo di Security Incident Management.

Sub responsabile: persona fisica o giuridica designata dal responsabile del trattamento previa autorizzazione scritta del titolare del trattamento;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare o suo delegato del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Titolare del trattamento o suo delegato: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

3.2. Adempimenti prescritti dalla normativa

Ai sensi dell'art 35 del GDPR "Valutazione d'impatto sulla protezione dei dati":

1. *Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*

2. *Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.*
3. *La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:*
   a) *una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*
   b) *il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o*
   c) *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*
4. *L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.*
5. *L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.*
6. *Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione. 4.5.2016 L 119/53 Gazzetta ufficiale dell'Unione europea IT*
7. *La valutazione contiene almeno:*
   a) *una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;*
   b) *una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;*
   c) *una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e*
   d) *le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.*
8. *Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.*
9. *Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.*

10. *Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.*
11. *Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.*

Ai sensi dell'art 36 del GDPR "**Consultazione preventiva"**:

1. *Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora 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.*
2. *Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.*
3. *Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:*
   a) *ove applicabile, 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;*
   b) *le finalità e i mezzi del trattamento previsto;*
   c) *le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;*
   d) *ove applicabile, i dati di contatto del titolare della protezione dei dati; 4.5.2016 L 119/54 Gazzetta ufficiale dell'Unione europea IT*
   e) *la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;*

f) *ogni altra informazione richiesta dall'autorità di controllo.*

4. *Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.*
5. *Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.*

In capo alla Regione Toscana e agli enti collegati, in caso di nuovi trattamenti o durante la revisione dei trattamenti esistenti vige:

A) Obbligo di redigere una valutazione di impatto sulla protezione dei dati quando questi possono presentare un rischio elevato per i diritti e le libertà delle persone.

Si evidenzia quindi che la redazione di un DPIA è obbligatoria quando vi è :

- **un trattamento con un rischio probabile per i diritti e le libertà delle persone fisiche.**

Nello specifico:

l'ente deve valutare preventivamente la potenzialità del rischio del trattamento tenendo in considerazione alcune informazioni che gli devono consentire di decidere se procedere o meno alla realizzazione della DPIA, nello specifico occorre almeno valutare:

- gli strumenti tecnologici, in modo particolare quelli nuovi, utilizzati al fine del trattamento,
- la natura del trattamento
- I dati oggetto del trattamento
- Il contesto e le finalità del trattamento.

Occorre inoltre tenere presente che alcuni trattamenti sono esclusi dalla obbligatorietà della valutazione di impatto:

- trattamenti esenti secondo gli elenchi forniti dall'autorità di controllo (art. 35 par.5)
- Particolari trattamenti leciti fra cui
  - il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, par. 1, lett. c);
  - il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1, lett. e)

Ulteriori dettagli per la definizione dei trattamenti che richiedono la realizzazione di una DPIA sono trattati all'interno del paragrafo 5.2

B) Obbligo di consultare l'autorità di controllo (prima di procedere al trattamento) qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi la presenza di un rischio elevato nel trattamento in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

Nello specifico:

tale obbligo è previsto se si ritiene che il trattamento sottoposto a DPIA violi il regolamento GDPR, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio.

C) Obbligo di consultare l'autorità di controllo (prima di procedere al trattamento) in relazione al trattamento per l'esecuzione di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

Il titolare del trattamento, o il suo delegato, dovrà quindi sempre consultare l'autorità di vigilanza qualora il diritto dello Stato membro in questione prescriva che i titolari del trattamento consultino l'autorità di controllo e/o ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica (articolo 36, paragrafo 5).

1.1 Soggetti attivi

I soggetti attivi sono tutti coloro che si occupano sin dalla fase di raccolta delle informazioni, dei trattamenti del processo e della procedura di DPIA.

1.1.1 Ruoli coinvolti

Ruolo aziendale	Responsabilità principali nel processo di DPIA
Titolari del trattamento	• Delega la responsabilità sul processo di DPIA al Process Owner e l'eventuale consultazione preventiva quando necessaria • Fornisce le risorse organizzative e finanziarie affinché sia possibile la realizzazione del processo di DPIA ed i conseguenti adeguamenti normativi e di sicurezza.
Process Owner (responsabile del processo a cui afferisce il trattamento)	• Coordina le attività necessarie alla DPIA per i nuovi trattamenti ed è responsabile della verifica della implementazione delle misure di sicurezza necessarie. • E' responsabile della raccolta delle informazioni sul trattamento per le verifiche preventive • E' responsabile delle verifiche preventive di conformità del trattamento • Coadiuva il DPO nelle verifiche preventive sull'obbligatorietà della esecuzione di una DPIA • In caso di un trattamento esistente che presenta un cambiamento del profilo di rischio coordina le attività per l'aggiornamento della DPIA • Implementa la strategia nella gestione del trattamento • Segnala al Titolare e al DPO il nuovo trattamento e/o la modifica di un servizio esistente nel caso di modifica del profilo di rischio • Partecipa alla valorizzazione degli impatti e probabilità per le minacce individuate • Assiste il DPO nella richiesta di Consultazione Preventiva

Ruolo aziendale	Responsabilità principali nel processo di DPIA
Referente interno	• Descrive e documenta il trattamento in tutte le sue caratteristiche • Collabora con Process Owner, il CISO e/o il Security Manager nella valutazione dell'impatto privacy • Assiste il Process Owner e il DPO nelle verifiche preventive (conformità e necessità DPIA) • Assiste il Process Owner nel garantire il rispetto degli obblighi di DPIA, tenendo conto della natura del trattamento e delle informazioni a loro disposizione. • Nel caso in cui il trattamento preveda l'impiego di Sistemi Informatici esterni, si confronta con i Responsabili Esterni che forniscono il servizio. • Supervisiona l'implementazione delle misure di sicurezza necessarie. • Partecipa alla valorizzazione degli impatti e probabilità per le minacce individuate • Collabora con il Process Owner, il CISO e/o il Security Manager nel processo di Consultazione Preventiva.
DPO	• Assiste il Process Owner nella definizione della Strategia e nello svolgimento della DPIA, monitora lo svolgimento, verifica 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. • È Responsabile della verifica preventiva di obbligatorietà della DPIA • Coadiuva il Process Owner nella verifica preventiva di conformità del trattamento • È responsabile del processo di consultazione preventiva e fungere da interfaccia per l'Autorità di Controllo.
CISO o Security Manager (in alternativa al CISO)	• Supporta il processo di DPIA con riguardo alle esigenze di sicurezza o operative. • Fornisce le informazioni di analisi dei rischi generali del ISMS • Coordina metodi e standard dell'analisi dei rischi dell'ISMS con l'analisi dei rischi DPIA • Partecipa alla valorizzazione degli impatti e probabilità per le minacce ICT individuate • Coordina l'implementazione delle misure di sicurezza necessarie emerse da DPIA in carico agli ICT Security Specialist. • Collabora con il Process Owner nel processo di Consultazione Preventiva.
ICT Security Specialist	• Supporta il processo di DPIA fornendo competenze ed informazioni relativamente agli aspetti tecnici di loro competenza • Partecipa alla valorizzazione degli impatti e probabilità per le minacce ICT individuate • Implementa le modifiche richieste in termini di soluzioni di sicurezza

4. Standard utilizzabili

4.1. ISO/IEC 29134:2017

4.1.1. Obiettivo della ISO/IEC 29134

Lo standard ISO/IEC 29134: 2017 "Information technology — Security techniques — Guidelines for privacy impact assessment" ha come obiettivo quello di fornire utili linee guida per lo svolgimento della valutazione di impatto sulla protezione dei dati, linee guida allineate alle indicazioni fornite dal Gruppo di Lavoro ex art. 29 in tema di Data Protection Impact Assessment (DPIA) all'interno del documento WP248 17/IT.

In particolare, lo standard ISO 29134 considera la DPIA come un processo che deve iniziare prima dell'effettuazione del trattamento dei dati personali, quando vi è ancora la possibilità di indirizzare il trattamento stesso (in un'ottica di "privacy by design").

4.1.2. Sintesi dei Contenuti della ISO/IEC29134

Entrando nel merito dello standard ISO 29134, questi al capitolo 5 ("5 Preparing the grounds for DPIA"), oltre a evidenziare i benefici della DPIA, fornisce le linee guida per definire gli obiettivi di comunicazione del DPIA Report e per definire le responsabilità nello svolgimento della DPIA.

Il capitolo 6 ("6 Guidance on the process for conducting a DPIA") fornisce le linee guida applicabili al processo di valutazione di impatto, con riferimento a considerazioni di carattere generale ("6.1 General"), alla individuazione dei casi in cui la DPIA è necessaria per quello specifico trattamento di dati ("6.2 Determine whether a DPIA is necessary (threshold analysis)"), alla preparazione dello svolgimento della DPIA ("6.3 Preparation of the PIA"), allo svolgimento della PIA ("6.4 Perform the DPIA") ed alle azioni a seguire ("6.5 Follow up the DPIA").

Il capitolo 7 ("7 DPIA report") fornisce infine le linee guida per predisporre il Report di Valutazione di Impatto con riferimento ad aspetti generali ("7.1 General"), alla struttura del report ("7.2 Report structure"), allo scopo ("7.3 Scope of DPIA"), ai requisiti ("7.4 Privacy requirements"), alla valutazione ("7.5 Risk assessment) ed al trattamento ("7.6 Risk treatment plan") dei rischi, alle decisioni conseguenti ("7.7 Conclusion and decisions") ed alla sintesi del report ("7.8 PIA public summary").

Sono inoltre presenti 4 allegati

- Allegato A: criteri per la definizione delle scale degli impatti e delle probabilità
- Allegato B: esempi di minacce generiche
- Allegato C: guida alla comprensione dei termini utilizzati
- Allegato D: Esempi illustrati a supporto del processo PIA

4.1.3. Utilizzo della ISO/IEC 29134

La ISO/IEC 29134: 2017 è una norma facoltativa che può essere utilizzata, associata alle linee guida WP248 art.29, per strutturare al meglio un processo DPIA e le relative responsabilità all'interno dell'organizzazione. La norma fornisce inoltre spunti interessanti per la strutturazione dei report finali. All'interno dell'allegato B troviamo anche alcuni esempi di minacce che possono essere prese in considerazione durante il processo di valutazione degli impatti e dei rischi.

Si tenga presente nel contempo che la norma è molto orientata ai rischi tecnici e/o comunque legati a minacce e vulnerabilità intrinseche nelle modalità di trattamento delle informazioni senza prendere in considerazione, al contempo, i rischi derivanti da trattamenti che, in quanto tali (per i loro contenuti e finalità) possono presentare dei rischi a prescindere dalle possibili vulnerabilità tecniche.

2 Contenuti ed interazioni del processo DPIA

2.1 Che cosa è la DPIA e a che cosa serve

Il Data Protection Impact Assessment (DPIA) è un processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo. Il DPIA va inquadrato come uno strumento essenziale e fondamentale per tutti i titolari e responsabili del trattamento al fine di dar corso al nuovo approccio alla protezione dei dati personali richiamato dal regolamento europeo e fortemente basato sul principio della accountability.

Un processo di DPIA può riguardare una singola operazione di trattamento dei dati. Tuttavia, si potrebbe ricorrere a un singolo DPIA anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Ciò potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Oppure, un singolo DPIA potrebbe essere applicabile anche a trattamenti simili attuati da diversi titolari del trattamento dei dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile un DPIA di riferimento, attuare le misure descritte nello stesso, e fornire una giustificazione per la realizzazione di un unico DPIA.

2.2 Quando si effettua la DPIA

L'art. 35 del GDPR stabilisce che è necessario effettuare una DPIA in tutti i casi in cui le operazioni di trattamento presentano rischi elevati per i diritti e le libertà delle persone fisiche in virtù della loro natura, portata o finalità o quando possono procurare un danno economico o sociale importante.

La DPIA deve essere effettuata prima di procedere al trattamento, già dalla fase di progettazione del trattamento stesso anche se alcune delle operazioni di trattamento non sono ancora note, in coerenza con i principi di privacy by design e by default per determinare se il trattamento deve prevedere misure opportune in grado di mitigare i rischi.

L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità

La valutazione DPIA concorre quindi, insieme ad eventuali altri processi di valutazione e gestione del rischio (es. Gestione del rischio in ambito ISMS) alla "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" come previsto dall'art. 25.

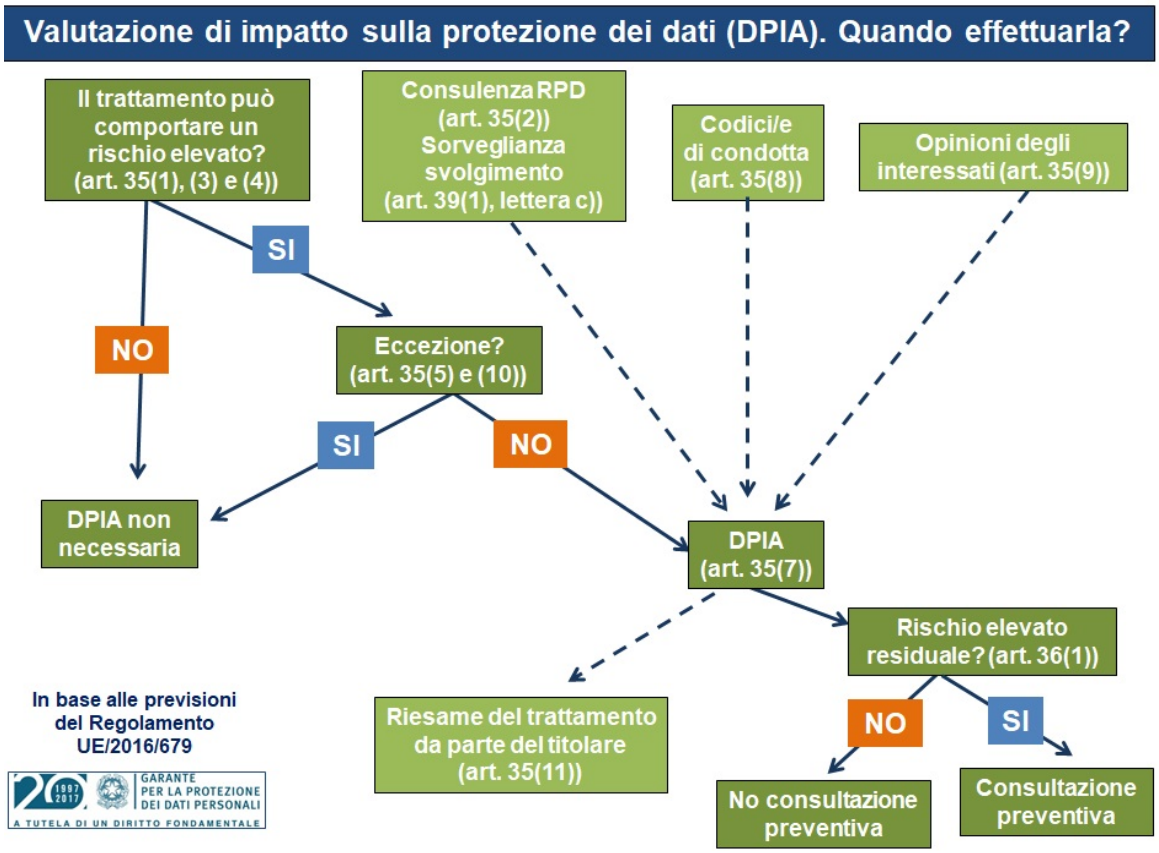
Ciò consente di acquisire le necessarie conoscenze sulle misure, garanzie e meccanismi da prevedere per mitigare il rischio e assicurare la conformità del trattamento al GDPR, prima che possano essere arrecati danni ai diritti ed alle libertà delle persone fisiche.

Al fine di garantire la corretta attivazione di un processo di DPIA è bene definire alcuni punti di attenzione in cui valutare appunto la necessità di realizzare o meno un Privacy Impact Assessment:

- Introduzione di nuovi trattamenti nell'ambito di nuovi processi e/o nuove attività aziendali;
- Importanti revisioni del modello organizzativo, con effetti su processi e relativi trattamenti;
- Nuovi servizi informativi e/o modifica dei servizi informatici in essere a supporto di trattamenti esistenti;
- Variazioni significative a Trattamenti in essere.

Anche se il regolamento evidenzia l'applicazione della valutazione di Impatto per i nuovi trattamenti, è comunque consigliabile (suggerito anche dalla linea guida WP248) valutare anche i trattamenti in corso prima del 25 maggio 2018 arrivando comunque a determinare la loro conformità al GDPR e la necessità o meno di effettuare una DPIA.

A seguire uno schema interessate (fonte Garante Privacy Italiano) che chiarisce il processo di valutazione della obbligatorietà di un processo DPIA (di seguito descritto nel paragrafo 5.3) e tutti gli elementi che ne concorrono.



2.3 Quando è obbligatorio effettuare un DPIA

La realizzazione di una valutazione d'impatto sulla protezione dei dati è **obbligatoria** soltanto qualora il trattamento "**possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche**" (articolo 35, paragrafo 1, 3 e 4).

Sebbene una valutazione d'impatto sulla protezione dei dati possa essere richiesta anche in altre circostanze, l'articolo 35, paragrafo 3, fornisce alcuni esempi, non esaustivi, di casi nei quali un trattamento "possa presentare rischi elevati":

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche12;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".

Vi possono essere trattamenti a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati e sui quali è necessario effettuare una DPIA.

La linea guida WP248 offre alcuni spunti e criteri di valutazione da tenere in considerazione al fine di valutare la necessità o meno di effettuare una DPIA di un trattamento. Le indicazioni prevedono che nel caso in cui un trattamento ricada in almeno due delle seguenti categorie si renda necessario lo sviluppo di un processo di valutazione di impatto:

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"
2. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche";
3. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico";
4. dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10.
5. trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:
    - il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
    - il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
    - la durata, ovvero la persistenza, dell'attività di trattamento;

- la portata geografica dell'attività di trattamento;

6. creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;
7. dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a causa dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti.
8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc.;
9. quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto.

In alcuni casi, un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno di questi criteri richieda una valutazione d'impatto sulla protezione dei dati.

Nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, si raccomanda di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati.

L'Autorità di controllo può redigere inoltre 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.

5.4 Quando è possibile non effettuare un DPIA

Una valutazione d'impatto sulla protezione dei dati non è richiesta nei seguenti casi:

- quando il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1);
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35, paragrafo 11);
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto

dell'adozione di tale base giuridica (articolo 35, paragrafo 10), a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;

- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5).

5.5 I contenuti della DPIA

L'art. 35 al paragrafo 7 definisce il contenuto minimo che deve comunque essere assicurato per la redazione di un DPIA:

- "una descrizione dei trattamenti previsti e delle finalità del trattamento";
- "una valutazione della necessità e proporzionalità dei trattamenti";
- "una valutazione dei rischi per i diritti e le libertà degli interessati";
- "le misure previste per:
  - "affrontare i rischi";
  - "dimostrare la conformità al presente regolamento".

Partendo dai punti offerti dal paragrafo 7 ed integrandoli con i suggerimenti offerti dalle line guida WP248 si propone uno schema di massima per la realizzazione di una DPIA conforme alle prescrizioni del GDPR:

1. la descrizione sistematica del trattamento e delle finalità;
2. la descrizione della natura, dell'ambito, del contesto e degli scopi del trattamento;
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 dell'asset model su cui si basano i dati personali (es. Siti, hardware, software, reti, organizzazione, ecc.);
6. la valutazione della necessità e la proporzionalità del trattamento;
7. la descrizione delle misure previste per conformarsi al regolamento;
8. la descrizione del modo in cui sono gestiti i rischi per i diritti e le libertà degli interessati;
9. la descrizione dell'origine, della natura, della particolarità e della gravità dei rischi;
10. la determinazione delle misure previste per il trattamento di tali rischi;
11. la descrizione del modo in cui sono coinvolte le parti interessate;
12. il parere del DPO;
13. le opinioni eventualmente raccolte dagli interessati o dei loro rappresentanti.

5.6. DPIA e Analisi dei rischi

5.6.1. Metodologia di analisi dei rischi nella DPIA

Uno degli aspetti più rilevanti nella realizzazione di un'analisi dei rischi è fissare fin da subito una metodologia definita, condivisa e ripetibile in grado di accompagnare l'azienda in un processo ricorsivo da

ripetersi con cadenza puntuale o al cambiare del contesto di riferimento. Spesso l'elemento più rilevante di un'analisi dei rischi non è tanto il valore assoluto dei suoi risultati, in termini spesso "qualitativi", ma è il confronto dei risultati rispetto alla precedente "elaborazione" che deve far comprendere all'azienda il trend di miglioramento in corso.

Lo scopo è sempre quello di ridurre al minimo, per quanto possibile, i rischi con una corretta valutazione e successiva gestione.

L'analisi del rischio è quindi un processo per identificare e valutare il danno causabile da minacce e vulnerabilità in combinazione su uno o più Asset aziendali ben precisi. Serve inoltre a giustificare le contromisure, a valutare che siano efficaci, di costo ragionevole, effettivamente applicabili al contesto e in grado di rispondere in tempo alle minacce.

Permette anche di assegnare una priorità di trattamento dei rischi e consentire di determinare l'investimento necessario all'azienda per proteggersi da essi.

Gli obiettivi principali dell'analisi del rischio sono:

- Identificarlo
- Quantificare l'impatto
- Permettere di individuare il bilanciamento ottimale tra l'impatto e il costo delle misure di sicurezza necessarie a ridurlo

È quindi una funzione che vede la possibilità di subire perdite al seguito del verificarsi di un evento dannoso rappresentabile con la seguente funzione: **R = f (I, P, V)**

Dove R (il rischio) è funzione delle vulnerabilità e degli Impatti (I) e Probabilità (P) delle possibili Minacce che possono insistere sulle vulnerabilità.

L'analisi dei rischi, in estrema sintesi, si sostanzia nelle risposte alle seguenti domande:

- Quali sono i miei asset da proteggere e qual' è il loro valore? (i dati e i trattamenti)
- Cosa potrebbe accadere? (qual è la minaccia e su quale vulnerabilità può insistere?)
- Quale danno potrebbe causare (qual è l'impatto sui diritti dell'interessato?)
- Quanto spesso può accadere? (qual è la frequenza di accadimento?)

Risulta quindi chiaro che uno dei primi elementi da identificare in una analisi dei rischi è il dominio degli asset su cui intervenire e il loro valore. Solo una corretta valorizzazione ci consente di sviluppare una corretta analisi dei rischi arrivando a contromisure che siano in linea ed adeguate al valore dell'asset da proteggere.

Applicando quanto espresso sopra al contesto di un'analisi dei rischi in ambito DPIA è evidente che tale analisi ha come obiettivo minimizzare la probabilità e impatti che possibili violazioni dei dati personali potrebbe comportare agli individui (distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato ai dati personali - art. 32 GDPR).

Per ciò che riguarda invece il valore alla base delle analisi dei rischi in ambito GDPR deve essere chiaro che non si tratta del valore che l'informazione ha per l'azienda (che comunque può essere tenuto in

considerazione per la valutazione di ulteriori soluzioni di sicurezza per la protezione del valore legato alla proprietà intellettuale dell'informazione) ma bensì al valore che il trattamento, e le relative informazioni in esso contenute, hanno per l'interessato.

Il regolamento generale sulla protezione dei dati offre ai titolari del trattamento la flessibilità di stabilire la struttura e la forma precise della valutazione d'impatto sulla protezione dei dati in maniera da consentire che la stessa si adatti alle pratiche di lavoro esistenti.

La linea guida WP248 offre alcuni esempi di metodologie differenti riportati all'interno dell'allegato 1 (Esempi di quadri UE esistenti di valutazione d'impatto sulla protezione dei dati) per contribuire all'attuazione dei requisiti essenziali stabiliti nel regolamento generale sulla protezione dei dati.

Sono inoltre definiti all'interno dell'allegato 2 (WP248 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile) dei criteri comuni che oltre che a chiarire i requisiti essenziali del regolamento, possono essere utilizzati anche per dimostrare che una particolare metodologia di valutazione d'impatto sulla protezione dei dati soddisfa i parametri imposti dal regolamento generale sulla protezione dei dati.

Ulteriori spunti per una corretta definizione di un processo ed una metodologia di analisi dei rischi possono essere ricavati dalla **ISO/UNI 31000:2010** che è una norma internazionale che fornisce principi e linee guida generali sulla gestione del rischio e dal "**Handbook on Security of Personal Data Processing**" pubblicato da ENISA (agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione - centro di competenze in materia di sicurezza informatica in Europa) che fornisce spunti interessanti per la definizione degli elementi atti a quantificare i rischi in relazione alle conseguenze per l'interessato.

5.6.2. Strumenti a supporto di un processo DPIA

Si evidenzia inoltre che per via della complessità di un processo DPIA e relativa fase di analisi dei rischi sarebbe bene, quando possibile, affidarsi a strumenti applicativi specializzati in grado di gestire tutte le fasi del processo e in grado di riproporre la sua applicabilità nel tempo.

Infatti, le variabili in gioco in un processo di analisi dei rischi sono molteplici (dimensioni di analisi, trattamenti, vulnerabilità, minacce, ecc.) e spesso può non risultare semplice mapparli e calcolarne il rischio con strumenti non strutturati quali possono essere, ad esempio, dei fogli di calcolo elettronici (spesso usati nei processi più semplici di analisi dei rischi)

Un esempio di un software applicativo per la gestione di un processo DPIA è "PIA", scaricabile gratuitamente dal sito di CNIL (Autorità francese per la protezione dei dati).

Il software, al quale ha aderito anche il garante Italiano, non costituisce un modello al quale fare sempre riferimento (si ricorda che è stato concepito soprattutto per le PMI), ma può offrire un focus sugli elementi principali di cui si compone la procedura di DPIA. Può quindi costituire un utile supporto metodologico e di orientamento allo svolgimento di una DPIA, ma non va inteso come schema predefinito per ogni valutazione d'impatto che va integrata in ragione delle tipologie di trattamento esaminate.

Può servire inoltre per comprendere meglio quali possono essere i requisiti di base di un applicativo DPIA adeguato alla propria realtà aziendale procedendo quindi ad una software selection più mirata e consapevole.

5.6.3. Integrazione dell'analisi dei rischi DPIA con l'analisi dei rischi del ISMS

Il GDPR fa riferimento all'obbligo del titolare (ed eventualmente del responsabile) di tenere conto dei rischi che i trattamenti possono comportare per i diritti e le libertà delle persone fisiche in due norme diverse:

- l'art.24 e 25, collocano l'analisi dei rischi fra le caratteristiche dei trattamenti di cui occorre tener conto per mettere in atto tutte le misure tecniche e organizzative adeguate
- l'art. 35, che prevede invece una specifica valutazione di impatto quando i trattamenti, considerate le circostanze indicate nella norma, possono presentare rischi elevati per gli interessati.

Anche dalla lettura della WP248 emerge che, in base all'art. 24, ogni trattamento deve essere analizzato dal titolare anche al fine di verificare se i rischi che ne derivano siano o no elevati. Ne consegue che anche l'analisi implicitamente prevista dall'art.24 è finalizzata all'accertamento del livello di rischio perché solo a valle di questa il titolare può decidere se il rischio per i cittadini sia elevato o meno.

In questo senso, come sottolinea il WP248, prima di porre in essere un qualunque trattamento, è sempre necessaria l'analisi dei rischi che possono derivarne.

La differenza tra le misure di sicurezza da adottare per via di quanto previsto dagli art. 24 e 25 e quelle che devono essere adottate per via di quanto previsto dall' art. 35 emerge solo a valle della analisi preventiva dei trattamenti, ed è sulla base di questa che il titolare dovrà decidere in concreto quali misure adottare.

Quanto espresso quindi dagli art.24 e 25 può essere riconducibile al concetto di Privacy by default, applicabile quindi a tutti i trattamenti a prescindere dalla loro potenziale criticità derivante dal trattamento di informazioni che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Ne deriva che è sempre necessaria un'analisi dei rischi di "base" in grado di garantire una sicurezza minima e una conformità sulle modalità di trattamento su tutti i trattamenti in essere.

A tal fine quindi, qualora l'azienda sia dotata di un ISMS e abbia effettuato un'analisi dei rischi (es. per la ISO27001) tale analisi può essere utilizzata come base per valutare la conformità requisiti espressi dagli art. 24 e 25 ed integrata con eventuali ulteriori criteri se necessario (estensione degli asset nel dominio dell'analisi dei rischi, ulteriori dimensioni di analisi per la Data Protection, estensione delle minacce e vulnerabilità, ecc.)

5.7. DPIA e altri adempimenti/processi GDPR

5.7.1. Registro dei trattamenti

Anche se la tenuta del Registro del Trattamento in alcuni casi non è ritenuta obbligatoria è comunque uno strumento da valutarsi, a prescindere dalla sua obbligatorietà, per tenere controllati gli Asset primari della nostra analisi dei rischi (appunto i trattamenti).

Infatti, tutte le volte che siamo in presenza di un rischio diventa quasi automatico procedere alla tenuta del registro dei trattamenti almeno come supporto per tutto il processo di analisi dei rischi.

Ne consegue che tutte le volte che si ritiene di dover procedere ad effettuare una DPIA è necessario procedere immediatamente alla tenuta del registro dei trattamenti.

Il registro dei trattamenti dovrà poi riportare una sintesi delle contromisure di sicurezza (sia tecnologiche che organizzative) emerse sia da un'analisi dei rischi di carattere più generale (art. 24 e 25) ma soprattutto dalle misure rese necessaria dalla applicazione della DPIA.

5.7.2. Data breach e incident management

Un processo di Data Breach va equiparato ad un processo più ampio di incident management dove non solo è necessario gestire l'immediatezza degli incidenti e tenerne traccia ma è fondamentale effettuare un'analisi a posteriori per apportare le adeguate azioni correttive e di miglioramento sul proprio sistema di gestione delle informazioni.

Solitamente quindi i dati raccolti dal processo di Incident management sono uno degli input fondamentali del processo di Analisi dei rischi: rappresentano infatti una delle fonti di minacce e vulnerabilità estremamente preziose proprio perché accadute nell'ambito della propria organizzazione (e quindi contestualizzate).

Alla stessa stregua quindi anche le informazioni raccolte dal processo di Data Breach (equiparabili al concetto di Incident Management) sono da riportarsi sia al processo più esteso di valutazione dei rischi secondo quanto previsto dall'art. 24 e 25 del GDPR ma contestualmente anche come input per il processo DPIA che va visto come una ulteriore verticalizzazione del processo di analisi dei rischi applicato su trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche.

Dall'altra parte le informazioni processate e documentate all'interno di una DPIA possono essere fondamentali nel processo di comunicazione dell'incidente (al Garante e/o agli interessati) al fine di dimostrare al meglio, per quanto possibile, che erano stati valutati correttamente tutti gli aspetti di rischio applicando, conseguentemente, adeguate contromisure.

6. Processo DPIA

6.1. Il processo DPIA

Un processo DPIA normalmente si compone di 5 fasi principali:

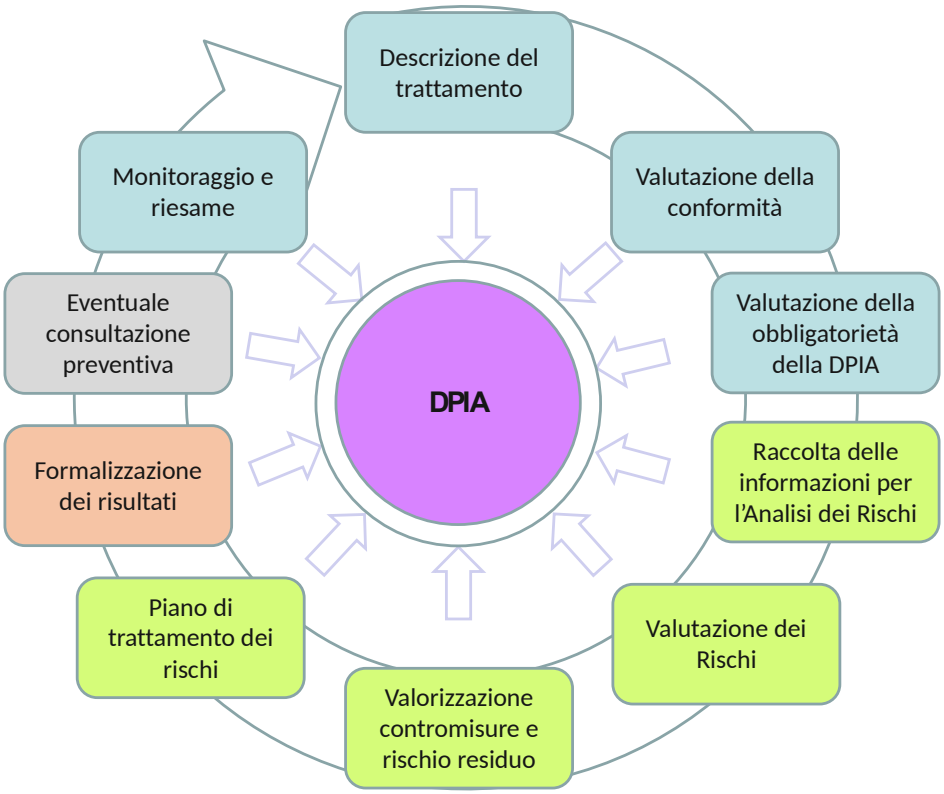
1. **Valutazione preliminare**: scopo dell'attività è quella di raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento è conforme al regolamento GDPR e in

seconda battura comprendere se quel trattamento deve essere sottoposto ad una valutazione DPIA. L'attività quindi si scompone di 3 sotto fasi:

   a. Descrizione del trattamento
   b. Valutazione della conformità
   c. Valutazione della obbligatorietà di condurre una DPIA

2. **Esecuzione DPIA**: una volta determinata la necessità di procedere ad una attività di DPIA si rende necessario procedere alla raccolta delle informazioni necessarie allo sviluppo successivo delle attività di analisi dei rischi e produzione del piano dei trattamenti. L'attività si scompone in ulteriori 4 sotto fasi:
   a. Raccolta delle informazioni per l'analisi dei rischi
   b. Valutazione dei rischi
   c. Valorizzazione contromisure e rischio residuo
   d. Piano di trattamento dei rischi
3. **Formalizzazione dei risultati**: 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. Eventuale **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.
5. **Monitoraggio e Riesame**: il processo DPIA è riconducibile al ciclo di Denim, dove le attività una volta terminate devono prevedere un monitoraggio dei risultati raggiunti e un conseguente riesame costante al fine di garantire nel tempo la mitigazione dei rischi e la conformità al Regolamento Europeo anche a fronte di fisiologici cambiamenti a cui sono soggetti tutti i trattamenti (contesto interno e esterno, finalità del trattamento, strumenti utilizzati, organizzazione aziendale, ecc.)

A seguire uno schema riassuntivo dei principali passaggi previsti da un processo DPIA



6.2. Valutazione preliminare

6.2.1. Raccolta delle informazioni per la valutazione preliminare

In questa fase devono essere fornite le informazioni rilevanti ai fini del censimento del trattamento stesso e per la valutazione dei rischi, tra cui sinteticamente:

- le categorie di soggetti interessati dal trattamento;
- le finalità del trattamento;
- le categorie di dati oggetto del trattamento;
- le modalità di trattamento;
- il luogo / i luoghi di conservazione dei dati trattati;
- i processi aziendali che saranno coinvolti nell'attuazione del trattamento

La responsabilità per il censimento e la raccolta delle informazioni relative al trattamento è in capo al Process Owner responsabile del processo a cui afferisce il potenziale trattamento, coadiuvato dal Referente interno.

Si tenga presente inoltre che solitamente le attività di valutazione preliminare, nel caso della presenza di un processo per la tenuta del Registro dei trattamenti, sono tipicamente inserite all'interno di tale processo come attività propedeutiche al censimento del trattamento e suo inserimento all'interno del Registro del trattamento stesso. Ulteriori approfondimenti sul processo di tenuta del registro dei trattamenti sono contenuti all'interno del documento "**Indicazioni operative per il Registro delle attività di trattamento**"

Un ulteriore dettaglio dei dati da raccogliere è possibile trovarlo sia negli attributi del Registro dei trattamenti sia all'interno dell'allegato nr. 2 al presente documento. Si consiglia inoltre di utilizzare anche i contenuti presenti all'interno dell'allegato 1 "*WP248 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile*" quale strumento di ulteriore verifica della completezza delle informazioni raccolte.

6.2.2. Valutazione della conformità

Una volta raccolte tutte le informazioni utili a identificare e censire il trattamento, si rende necessaria, come prima attività, 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.

Il Referente interno dei dati personali dell'unità organizzativa di appartenenza del Process Owner, avvalendosi se necessario del supporto del DPO, verifica che vi siano tutti i presupposti per effettuare un trattamento conforme ai requisiti GDPR. La responsabilità per la corretta esecuzione delle verifiche preventive rimane comunque in carico al Process Owner.

Si dovranno verificare almeno i seguenti aspetti:

- il trattamento rispetta i princìpi applicabili al trattamento dei dati personali (CAPO II del GDPR):
    - principio di liceità, correttezza e trasparenza;
    - principio di limitazione della finalità;
    - principio di minimizzazione dei dati;
    - principio di esattezza dei dati;
    - principio di limitazione della conservazione dei dati;
    - principio di integrità e riservatezza.
- il trattamento rispetta i diritti degli interessati (CAPO III del Regolamento):
    - diritto di informazione;
    - diritto di accesso ai dati;
    - diritto di portabilità dei dati;
    - diritto di rettifica dei dati;
    - diritto di cancellazione dei dati ("diritto all'oblio");
    - diritto di limitazione del trattamento;
    - diritto di opposizione al trattamento.

Anche nel caso della Valutazione della conformità, se esiste un processo per la tenuta del Registro dei trattamenti, è tipicamente inserita all'interno di tale processo come attività propedeutiche al censimento del trattamento e suo inserimento all'interno del Registro del trattamento stesso (si faccia sempre riferimento al documento *"Indicazioni operative per il Registro delle attività di trattamento*")

Qualora tutte le verifiche portino ad un esisto **positivo** il trattamento è conforme e si può procedere ad effettuare la valutazione successiva (Valutazione dell'obbligo/esenzione DPIA)

Qualora invece le verifiche portino ad un esito **negativo** il trattamento non può essere effettuato, almeno con le finalità, modalità e mezzi previsti all'interno dell'analisi appena effettuata.

6.2.2. Valutazione dell'obbligo/esenzione DPIA

Il DPO, con l'ausilio operativo del Process Owner e del Referente interno ha successivamente l'onere di verificare se il trattamento ricade nella casistica di quelli che necessitano obbligatoriamente di una valutazione di impatto privacy (DPIA)

Il DPO insieme al Referente interno e Process Owner verificheranno principalmente che:

- il trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (Art.35, par. 1);
- il trattamento ricade in una delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati (Art.35, par. 5);
- il trattamento risulta già normato di diritto (Art.35, par. 10).

A tal riguardo per valutare gli elementi di dettaglio che possono portare ad una valutazione della obbligatorietà o meno della realizzazione di un processo DPIA si faccia riferimento ai paragrafi 5.3 "Quando è obbligatorio effettuare un DPIA" e 5.4 "Quando è possibile non effettuare un DPIA" del presente documento.

Si suggerisce la produzione di checklist di dettaglio, prendendo spunto dai contenuti del presente documento di indirizzo e dalle linee guida WP248, per facilitare la raccolta e l'analisi delle informazioni che determinano o meno l'obbligatorietà di effettuare una DPIA su un trattamento.

Qualora la verifica porti ad un esito positivo, ovvero alla consapevolezza che si rende necessario procedere alla realizzazione del DPIA, allora si potrà procedere allo sviluppo del punto 6.3.

Nel caso invece in cui tale obbligatorietà non esista si passa comunque a formalizzare tale informazione all'interno del par. 6.4 Formalizzazione dei Risultati. È bene comunque che anche un esito negativo (DPIA non necessaria) sia ben documentato in tutte le sua parti in modo da dimostrare, anche all'esterno, di aver proceduto alla realizzazione di una valutazione preventiva completa e conforme al Regolamento Europeo.

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.

6.3. Esecuzione DPIA

6.3.1. Raccolta delle informazioni per l'analisi dei rischi

Una buona analisi dei rischi DPIA si basa sempre su una corretta e completa raccolta di informazioni preliminari in grado di caratterizzare il trattamento e le sue peculiarità.

E' quindi importante raccogliere alcune informazioni fra cui:

- Informazioni presenti all'interno dei trattamenti

- Processi aziendali su cui insistono i trattamenti
- Finalità dei dati raccolti
- Flussi informativi
- Autorizzati all'accesso alle informazioni
- Asset model a sostegno dei trattamenti (applicativi, hardware, reti, ecc.)

Tali informazioni si possono raccogliere o all'interno dell'organizzazione o da documentazione esistente e/o interviste oppure ricavandole da quanto raccolto durante la fase di verifiche preliminari.

Le valutazioni che dovranno essere fatte durante la fase di analisi dei rischi devono tenere in considerazione due aspetti fondamentali: sia i rischi derivanti dai contenuti intrinseci del trattamento stesso comprendenti soprattutto modalità e finalità sia i rischi derivanti da possibili violazioni di sicurezza della protezione del dato.

In entrambi i casi è importante identificare le minacce che insistono sui trattamenti (volontarie e/o accidentali) sempre nell'ottica della tutela dei diritti dell'interessato.

6.3.2. Valutazione dei rischi

La valutazione dei rischi all'interno di una DPIA è di norma sviluppata nel classico concetto di valutazione degli impatti e probabilità afferenti ad una serie di minacce in grado di compromette un asset (informativo)

Aldilà quindi della necessità di identificare il set di minacce (volontarie e/o accidentali) che insistono sul trattamento è utile, nella fase preliminare, identificare anche i possibili impatti e le relative scale di riferimento comprendenti anche le scale di probabilità di accadimento.

A seguire un esempio di impatti incentrati su un concetto di danno alla persona:

- Impatti derivanti da una violazione della sicurezza fisica;
- Impatti derivanti da una violazione dei dati di identificazione o attinenti l'identità personale;
- Impatti materiali (es. perdite finanziarie o al patrimonio, perdite dovute a frodi);
- Impatti 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);
- Impatti sociali (es. quando intervengono conseguenze di tipo discriminatorio, perdite di autonomia);

L'ente potrà, nell'ambito della definizione degli aspetti metodologici e strumentali da utilizzarsi per il calcolo dell'analisi dei rischi, definire le opportune scale di impatti e probabilità da utilizzarsi per tutte le valutazioni DPIA che dovranno essere sviluppate.

Completata la fase preliminare di prima configurazione dell'analisi dei rischi si provvederà a compilare, per ogni minaccia individuata, gli impatti e le relative probabilità di accadimento. L'onere della compilazione di tali informazioni è del Process Owner coadiuvato per gli aspetti tecnici dal CISO quando presente e/o dal Security Manager.

6.3.4.Valorizzazione contromisure e rischio residuo

Successivamente si procede di norma alla valorizzazione delle contromisure esistenti il cui onere è in capo al CISO e/o al Security Manager quando questo non è presente.

L'associazione di minacce e contromisure esistenti consente a questo punto di determinare il rischio effettivo che sarà confrontato con un valore di rischio accettabile precedentemente definito in associazione fra il Process Owner e il DPO.

Qualora il valore di rischio sia entro la soglia di accettabilità il trattamento potrà essere definito sufficientemente sicuro e si potrà procedere alla formalizzazione dei risultati all'interno del par. 6.4

Nel caso in cui invece il valore di rischio residuo risulti sopra la soglia di accettabilità si dovrà procedere a rivedere le contromisure applicate alzando il livello di implementazione delle contromisure esistenti oppure introducendo nuove contromisure più efficaci a protezione del trattamento analizzato.

In tal caso il valore di rischio sarà ricalcolato ottenendo quindi un nuovo valore di rischio residuo a seguito della applicazione delle nuove contromisure che a questo punto concorreranno alla preparazione del piano di trattamento dei rischi di cui al punto 6.3.2.

6.3.5. Valutazioni e Piano di trattamento dei rischi

Tutte le informazioni raccolte ed elaborate durante il processo di analisi dei rischi devono essere formalizzate a supporto della realizzazione del piano di trattamento. Tipicamente all'interno di un processo di analisi dei rischi occorre almeno tracciare:

- Dati e trattamenti da proteggere (asset primari)
- Valorizzazione delle vulnerabilità e minacce (Impatti e probabilità)
- Contromisure di mitigazione del rischio
- Valore del rischio residuo

Tutte queste informazioni concorrono a realizzare un piano di trattamento del rischio che deve essere supportato dalle relative risorse (economiche, organizzative e tecniche) affinché il piano sia effettivamente realizzabile.

La realizzazione del piano è di responsabilità del CISO (o Security Manager) con il supporto del Process Owner e del Referente interno.

La responsabilità di rendere il piano approvato ed operativo (risorse disponibili per la sua realizzazione) è in capo al Process Owner.

Il piano di trattamento dei rischi concorre, insieme a tutte le altre informazioni legate alle valutazioni preliminari, alla formalizzazione dei risultati della DPIA come descritto all'interno del paragrafo 6.4

6.4. Formalizzazione dei risultati

Tutta la documentazione prodotta all'interno del processo di DPIA, partendo dal censimento e descrizione del trattamento, passando dalle valutazioni preliminari per arrivare, quando necessario, al calcolo di analisi dei rischi e relativo piano di trattamento, devono concorrere alla realizzazione di un Report finale in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dal GDPR.

La valutazione complessiva di impatto, o una sua sintesi, può essere resa pubblica da parte del titolare in un'ottica di trasparenza nei confronti degli interessati.

Contenuti e modalità dell'eventuale pubblicazione può essere concordata con il DPO.

Il report deve inoltre esplicitare la frequenza di aggiornamento del DPIA, tanto maggiore quanto più si utilizzino tecnologie in evoluzione o si prevedono 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 Process Owner. Se gli esiti della valutazione DPIA rivelano che il rischio residuo è elevato e non mitigabile (tecnologie e/o costi inapplicabili) occorre consultare l'Autorità di controllo per chiedere un parere fornendo le evidenze dell'analisi compiuta (rif. par. 6.5 – consultazione preventiva).

A tale scopo, è opportuno che il Process Owner consulti il DPO in merito alla verifica della correttezza e della conformità della DPIA al GDPR e alla relativa necessità di consultazione preventiva.

6.5. Consultazione preventiva

Qualora la valutazione d'impatto sulla protezione dei dati a cui si è giunti al termine del processo DPIA e riportato all'interno del Report conclusivo, indichi che il trattamento possa presentare un rischio elevato in assenza di misure adottabili dal Titolare del trattamento in grado di attenuare il rischio, il Titolare del trattamento (o suo delegato), prima di procedere al trattamento, deve consultare l'Autorità di Controllo. Tale adempimento deve essere considerato parte integrante del processo di DPIA.

6.5.1. Quando è necessaria la consultazione preventiva

La consultazione preventiva all'autorità garante è quindi sostanzialmente obbligatoria in due casi:

- Ogni qualvolta il titolare del trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati)
- Qualora il diritto dello Stato membro in questione prescriva che i titolari del trattamento consultino l'autorità di controllo e/o ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica (articolo 36, par. 5).

5.5.2. Contenuti della consultazione preventiva

La responsabilità dell'attivazione della Consultazione preventiva è responsabilità del DPO, su delega del Titolare, in accordo con il Process Owner (o referente interno) a cui fa riferimento il trattamento oggetto della DPIA.

La consultazione preventiva, come indicato all'interno dell'art. 36 par. 3 deve contenere alcune informazioni fondamentali fra cui:

a) ove applicabile, 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;
b) le finalità e i mezzi del trattamento previsto;
c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;
d) ove applicabile, i dati di contatto del titolare della protezione dei dati;
e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;
f) ogni altra informazione richiesta dall'autorità di controllo.

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

Salvo diversa disposizione dell'Autorità garante è bene che la comunicazione di Richiesta di Consultazione avvenga con modalità che consentano di dimostrare la data certa della stessa comunicazione (es. PEC, Raccomandata, ecc.) visto che i tempi stabiliti per lo sviluppo del processo di consultazione preventiva decorreranno da tal data.

6.5.3. Processo della consultazione preventiva

Quando è stata richiesta una valutazione preventiva all'Autorità di Controllo, secondo quanto indicato all'interno del par. 6.5.1, il trattamento non può essere iniziato almeno fino a che in procedimento di consultazione preventiva si è concluso con successo.

L'autorità a questo punto ha 8 settimane, prorogabili una sola volta di altre 6 settimane, per concludere la consultazione.

Nel caso in cui non dovesse pervenire alcuna risposta entro il termine di otto settimane, il silenzio assenso 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 GDPR.

Se invece l'Autorità ha ravvisato una possibile violazione del regolamento in quanto per il trattamento in questione il Titolare non abbia identificato o attenuato sufficientemente il rischio, la medesima potrà fornire un parere scritto al Titolare del trattamento in tal senso.

Nel caso in cui invece il trattamento venga ritenuto particolarmente complesso da esaminare e richieda più tempo l'Autorità Garante potrà richiedere, entro un mese dal ricevimento della richiesta di Consultazione, una proroga di ulteriori sei settimane (solo per una volta).

6.6. Revisione del processo DPIA

La DPIA non è da intendersi come un'attività puntuale da effettuarsi una tantum ma è un processo, un processo che deve essere ciclicamente attuato e revisionato tutte le volte che si rende necessario in base ai cambiamenti interni o esterni che si dovessero presentare al trattamento.

Anche la linea guida WP248 sottolinea la necessità di effettuare la DPIA ad intervalli periodici, con una frequenza almeno triennale, anche se non dovessero sopraggiungere cambiamenti apparenti al trattamento.

Nel caso di modifiche a trattamenti esistenti si deve prevedere sempre una revisione della DPIA.

A seguire alcuni esempi di modifiche alle attività di trattamento, rischi connessi e cambiamenti nel contesto organizzativo o sociale che debbono indurre ad una revisione della DPIA:

- Cambiamento sulle attività di trattamento, in termini di:
    - Contesto
    - Finalità del trattamento,
    - Tipologia di dati personali trattati
    - Destinatari
    - Modalità di raccolta dei dati personali
    - Combinazioni di dati provenienti da fonti differenti
    - Trasferimento di dati all'estero
- Modifica ai rischi con impatto sui diritti degli interessati derivati da:
    - Presenza di nuove minacce
    - Modifica ai sistemi informativi a supporto del trattamento
    - Soppressione di contromisure esistenti
    - Nuovi scenari di rischio
    - Nuovi potenziali impatti sulle dimensioni di analisi (Riservatezza, Integrità, Disponibilità)
    - Attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali.

Inoltre, si rende comunque necessaria una revisione della DPIA tutte le volte che si è in presenza di mutamenti nel contesto organizzativo o sociale per il trattamento in essere.

7. Aspetti sanzionatori

7.1. Violazioni

Le linee guida che il Titolare dovrà predisporre per le proprie verifiche periodiche dovrà prevedere quanto meno l'individuazione della casistica delle possibili violazioni con riguardo ai diversi trattamenti e con riferimento agli obblighi giuridici del Titolare del trattamento così come delineati dalla normativa in materia di protezione dei dati personali.

Questo anche al fine di agevolare il controllo della compliance e l'adozione delle misure di contenimento del relativo rischio.

Con il termine violazioni si fa riferimento a quelle irregolarità nella gestione del processo di DPIA che possono essere oggetto di sanzione a seguito di controllo delle autorità di controllo individuate.

A titolo esemplificativo si può fare riferimento alla mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa, l'esecuzione in maniera errata di detta valutazione oppure la mancata consultazione dell'autorità di controllo laddove richiesto.

7.2. Sanzioni

La mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa (articolo 35, paragrafi 1, 3 e 4), l'esecuzione in maniera errata di detta valutazione (articolo 35, paragrafi 2 e da 7 a 9) oppure la mancata consultazione dell'autorità di controllo laddove richiesto (articolo 36, paragrafo 3, lettera e)), possono comportare una sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di EUR oppure, nel caso di un'impresa, pari a fino al 2% del fatturato annuo globale dell'anno precedente, a seconda di quale dei due importi sia quello superiore.

8. Allegati

Allegato 1 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile

Allegato 2 - Esempio di informazioni da raccogliere durante la fase di descrizione del trattamento

Allegato 1 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile

Il WP248 propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

- una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):
  - la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);
  - vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
  - viene fornita una descrizione funzionale del trattamento;
  - sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);
  - si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);
- la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):
  - sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):
    - misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
      - finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));
      - liceità del trattamento (articolo 6);
      - dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));
      - limitazione della conservazione (articolo 5, paragrafo 1, lettera e));
    - misure che contribuiscono ai diritti degli interessati:
      - informazioni fornite all'interessato (articoli 12, 13 e 14);
      - diritto di accesso e portabilità dei dati (articoli 15 e 20);
      - diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
      - diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
      - rapporti con i responsabili del trattamento (articolo 28);
      - garanzie riguardanti trattamenti internazionali (capo V);
      - consultazione preventiva (articolo 36).
- i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)):
  - l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:
    - si considerano le fonti di rischio (considerando 90);
    - sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
    - sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
    - sono stimate la probabilità e la gravità (considerando 90);
  - sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);
- le parti interessate sono coinvolte:
  - si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);
  - si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo)

Allegato 2 - Esempio di informazioni da raccogliere durante la fase di descrizione del trattamento

- **Denominazione del trattamento**
- **Finalità del Trattamento**
- **Titolare del Trattamento**
- **Responsabili del Trattamento:**
- **Data inizio**
- **Data fine** (quando nota)
- **Durata della conservazione dei dati**
- **Categorie di Soggetti interessate (una o più):**
  - Dipendenti / Collaboratori
  - Clienti
  - Potenziali Clienti
  - Fornitori / Consulenti
  - "Altri soggetti
- **Categorie di Dati da trattare:**
  - Dati Personali
  - Dati relativi alla salute
  - Dati biometrici
  - Dati genetici
  - Categorie particolari di Dati
  - Dati relativi a condanne penali e reati
- **Modalità di trattamento:**
  - In forma Elettronica
  - In forma Cartacea
- **Luogo/i di conservazione dei Dati:**
  - In forma Elettronica
  - In forma Cartacea
- **Processi Aziendali coinvolti nel Trattamento:**
  - Tipologia
  - Macro Processo/i
  - Processi di Dettaglio