VALUTAZIONE DI IMPATTO PRIVACY

ARTICOLO 35 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.

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) [*OBBLIGO LEGALE*] o e) [*COMPITO DI INTERESSE PUBBLICO*], 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.

(89) La direttiva 95/46/CE ha introdotto un obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali. Mentre tale obbligo comporta oneri amministrativi e finanziari, non ha sempre contribuito a migliorare la protezione dei dati personali. È pertanto opportuno abolire tali obblighi generali e indiscriminati di notifica e sostituirli con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali tipi di trattamenti includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali 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.

(95) Il responsabile del trattamento, se necessario e su richiesta, dovrebbe assistere il titolare del trattamento nel garantire il rispetto degli obblighi derivanti dallo svolgimento di una valutazione d'impatto sulla protezione dei dati e dalla previa consultazione dell'autorità di controllo.

Una DPIA consiste in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali4 (attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli)

la DPIA è una procedura che permette di realizzare e dimostrare la conformità con le norme

A. Qual è l'oggetto della DPIA? Un singolo trattamento ovvero un insieme di trattamenti simili

LA DEFINIZIONE DI UN PERIMETRO

POSSIBILI RIFERIMENTI:

LA FINALITÀ DEL TRATTAMENTO

LE CATEGORIE DI INTERESSATI

GLI STRUMENTI UTILIZZATI

LA STRUTTURA DI RIFERIMENTO

VALUTAZIONE PIA

Un titolare può ritenere, nella maggioranza dei casi, che quando un trattamento soddisfa **due dei criteri sotto indicati sia necessario condurre una DPIA**

Viceversa, può darsi il caso di un trattamento che riflette gli esempi indicati ma che, a giudizio del titolare, non "può presentare un rischio elevato". In casi del genere, il titolare dovrà motivare e documentare la scelta della mancata conduzione della DPIA, allegando o annotando l'opinione del responsabile della protezione dei dati.

Inoltre, il principio di responsabilizzazione prevede che ciascun titolare "*tiene un registro delle attività di trattamento svolte sotto la propria responsabilità*" comprendente, fra l'altro, le finalità del trattamento, una descrizione delle categorie di dati e i destinatari dei dati stessi, nonché "*ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1*" (art. 30, paragrafo 1) e deve valutare se vi sia la probabilità di un rischio elevato anche se potrà decidere, in ultima analisi, di non condurre una DPIA.

1. **TRATTAMENTI VALUTATIVI O DI SCORING, COMPRESA LA PROFILAZIONE E ATTIVITÀ PREDITTIVE**, in particolare a partire da
"*aspetti riguardanti il rendimento professionale,*
la situazione economica,
la salute,
le preferenze o gli interessi personali,
l'affidabilità o il comportamento,
l'ubicazione o gli spostamenti dell'interessato"

(considerando 71 e 91). A titolo esemplificativo si possono citare un

istituto finanziario che effettui lo screening dei propri clienti utilizzando un database di rischio creditizio ovvero un database per la lotta alle frodi o al riciclaggio e al finanziamento del terrorismo (AML/CTF);

una società operante nel settore delle biotecnologie che offra test genetici direttamente ai consumatori per finalità predittive del rischio di determinate patologie o in generale per lo stato di salute;

una società che crei profili comportamentali o di marketing a partire dalle operazioni o dalla navigazione compiute sul proprio sito web.

2. **DECISIONI <u>AUTOMATIZZATE</u> CHE PRODUCONO SIGNIFICATIVI effetti giuridici o di analoga natura**: trattamenti finalizzati ad assumere decisioni su interessati che producano "*effetti giuridici sulla persona fisica*" ovvero che "*incidono in modo analogo significativamente su dette persone fisiche*(art. 35, paragrafo 3, lettera a)).

Per esempio, il trattamento può comportare
l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione.
Il trattamento che produce effetti minimi o nulli su un interessato non soddisfa questo specifico criterio.
Per maggiori dettagli sui concetti in gioco si rimanda alle Linee-guida in materia di profilazione che il Gruppo di lavoro si appresta a pubblicare.

***3.* MONITORAGGIO SISTEMATICO: trattamenti utilizzati per osservare, monitorare o controllare gli interessati**, compresa la raccolta di dati attraverso reti o "*la sorveglianza sistematica di un'area accessibile al pubblico*" (art. 35, paragrafo 3, lettera c).14 Questa tipologia di monitoraggio costituisce un criterio, ai fini della DPIA, in quanto la raccolta di dati personali può avvenire in circostanze tali da non consentire agli interessati di comprendere chi vi stia procedendo e per quali finalità. Inoltre, è talora impossibile per gli interessati sottrarsi a questa tipologia di trattamenti in aree pubbliche (o pubblicamente accessibili). L'interpretazione del termine "sistematico" fornita dal WP29 (si vedano le "Linee-guida sul responsabile della protezione dei dati" (16/EN WP243)) è la seguente: - che avviene per sistema; - predeterminato, organizzato o metodico; - che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; - svolto nell'ambito di una strategia. Il WP29 interpreta l'espressione "area accessibile al pubblico" nel senso di un luogo aperto alla generalità delle persone, per esempio una piazza, un centro commerciale, una strada, una biblioteca pubblica.	

***4.* DATI SENSIBILI O DATI DI NATURA ESTREMAMENTE PERSONALE:** si tratta delle categorie particolari di dati personali di cui all'art. 9 (per esempio, informazioni sulle opinioni politiche di una persona fisica) oltre ai dati personali relativi a condanne penali o reati di cui all'art. 10. A titolo di esempio, si può citare un ospedale che conserva le cartelle cliniche dei pazienti, o un investigatore privato che conserva informazioni su soggetti responsabili di reati. Al di là di queste disposizioni del regolamento, vi sono talune categorie di dati che possono aumentare i rischi eventuali per i diritti e le libertà delle persone fisiche. Si tratta di dati personali considerati sensibili (nell'accezione comune del termine), in quanto connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza) ovvero in quanto incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) ovvero in quanto una loro violazione comporta evidentemente un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti). A tale proposito, può essere pertinente la circostanza per cui i dati siano già stati resi pubblici dall'interessato ovvero da terzi. Il fatto che un certo dato personale sia disponibile pubblicamente può essere un elemento da prendere in esame nel valutare l'aspettativa di un utilizzo ulteriore di tale dato per determinati scopi. Il criterio in oggetto può riferirsi anche a dati quali documenti personali, email, agende, appunti tratti da lettori elettronici dotati di dispositivi per la presa di appunti, e informazioni molto personali contenute in applicazioni che consentono di tenere traccia del proprio stile di vita.	

***5.* TRATTAMENTI DI DATI SU LARGA SCALA:** il regolamento non offre definizioni del concetto di "larga scala", anche se il considerando 91 fornisce indicazioni in merito. In ogni caso, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori seguenti al fine di stabilire se un trattamento sia svolto su larga scala: a. numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; b. volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; c. durata, o persistenza, dell'attività di trattamento; d. ambito geografico dell'attività di trattamento.	

***6.* COMBINAZIONE O RAFFRONTO DI INSIEMI DI DATI, per esempio derivanti da DUE O PIÙ TRATTAMENTI SVOLTI PER DIVERSE FINALITÀ e/o da TITOLARI DISTINTI**, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato	

***7.* DATI RELATIVI A INTERESSATI VULNERABILI** (ES. considerando 75): il	

trattamento di questa tipologia di informazioni rappresenta un criterio ai fini della DPIA in quanto è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento, nel senso che il singolo può non disporre del potere di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti. La categoria degli interessati vulnerabili comprende anche i
minori, che. si può ritenere non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali,
i **dipendenti**,
quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela
soggetti con patologie psichiatriche,
richiedenti asilo
anziani
pazienti) e
ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.

8. **UTILIZZI INNOVATIVI O APPLICAZIONE DI NUOVE SOLUZIONI TECNOLOGICHE O ORGANIZZATIVE**, come
l'associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici
, e così via. Il regolamento chiarisce (art. 35, paragrafo 1, e considerando 89 e 91) che l'utilizzo di una nuova tecnologia, definito "*in conformità con il grado di conoscenze tecnologiche raggiunto*" (considerando 91), può comportare l'obbligo di condurre una DPIA, in quanto il ricorso a una nuova tecnologia può generare forme innovative di raccolta e utilizzo dei dati cui può associarsi un rischio elevato per i diritti e le libertà delle persone. Nei fatti, le conseguenze sul piano individuale e sociale del ricorso a una nuova tecnologia sono talora ignote. La DPIA aiuterà il titolare a comprendere e gestire tali rischi. Per esempio, alcune applicazioni legate all' "Internet delle cose" potrebbero avere impatti significativi sulla vita privata e le abitudini delle persone, e, quindi, necessitano di una DPIA.

9. **TUTTI QUEI TRATTAMENTI CHE, DI PER SÉ, "*IMPEDISCONO [AGLI INTERESSATI] DI ESERCITARE UN DIRITTO O DI AVVALERSI DI UN SERVIZIO O DI UN CONTRATTO*"** allo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento.

"LARGA SCALA" i "considerando"

(90) In tali casi, è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento.

(91) Ciò dovrebbe applicarsi in particolare ai trattamenti su **larga scala**, che mirano al trattamento **di** una **notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati** e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti. È opportuno altresì effettuare una valutazione d'impatto sulla protezione dei dati nei casi in cui i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza. Una valutazione d'impatto sulla protezione dei dati è altresì richiesta per la sorveglianza di zone accessibili al pubblico su larga scala, in particolare se effettuata mediante dispositivi optoelettronici, o per altri trattamenti che l'autorità di controllo competente ritiene possano presentare un rischio elevato per i diritti e le libertà degli interessati, specialmente perché impediscono a questi ultimi di esercitare un diritto o di avvalersi di un servizio o di un contratto, oppure perché sono effettuati sistematicamente su larga scala.

Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati.

LARGA SCALA (LINEE GUIDA DPO - DICEMBRE 2016)

2.1.3. "Larga scala"

In base all'articolo 37, paragrafo 1, lettere b) e c) del RGPD, occorre che il trattamento di dati personali avvenga su larga scala per far scattare l'obbligo di nomina di un RPD. Nel regolamento non si dà alcuna definizione di trattamento su larga scala, anche se il considerando 91 fornisce indicazioni in proposito.

In realtà è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; d'altra parte, ciò non significa che sia impossibile, col tempo, individuare alcuni standard utili a specificare in termini oggettivi e quantitativi cosa debba intendersi per "larga scala" con riguardo ad alcune tipologie di trattamento maggiormente comuni.

Anche il WP29 intende contribuire alla definizione di questi standard pubblicando e mettendo a fattor comune esempi delle soglie applicabili per la nomina di un RPD.

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.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;

- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);

- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di *fast food*;

- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;

- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;

- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;

- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

LARGA SCALA (LINEE GUIDA PIA - OTTOBRE 2017)

5. Trattamenti di dati su larga scala: il regolamento non offre definizioni del concetto di "larga scala", anche se il considerando 91 fornisce indicazioni in merito. In ogni caso, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori seguenti al fine di stabilire se un trattamento sia svolto su larga scala:

a. numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;

b. volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento;

c. durata, o persistenza, dell'attività di trattamento;

2.1.4. "Monitoraggio regolare e sistematico" (LINEE GUIDA DPO - DICEMBRE 2016)

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, il considerando 24 menziona il "*monitoraggio del comportamento di detti interessati*"[15] ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di **pubblicità comportamentale**.

Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati.

L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del WP29:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;

- ricorrente o ripetuto a intervalli costanti;

- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del WP29:

- che avviene per sistema;

- predeterminato, organizzato o metodico;

- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;

- svolto nell'ambito di una strategia.

Alcune esemplificazioni:

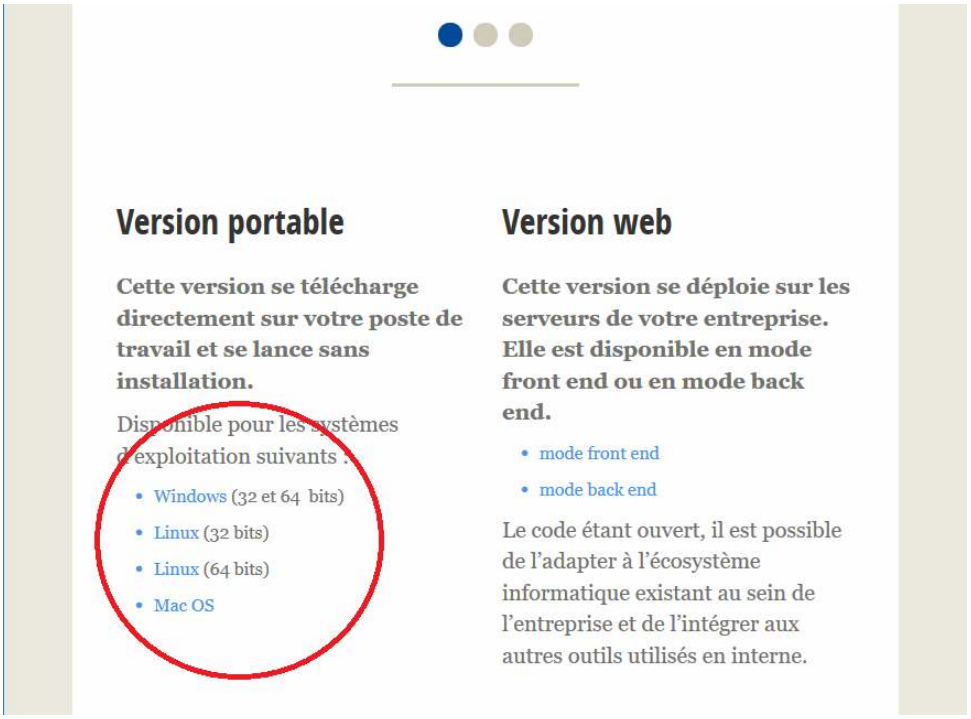
- curare il funzionamento di una rete di telecomunicazioni;
- la prestazione di servizi di telecomunicazioni;
- il reindirizzamento di messaggi di posta elettronica;
- profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio);
- tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili;
- programmi di fidelizzazione;
- pubblicità comportamentale;
- monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili;
- utilizzo di telecamere a circuito chiuso;
- dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

http://www.garanteprivacy.it/regolamentoue

Disponibile un software - gratuito e liberamente scaricabile dal sito www.cnil.fr - che offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal WP29 nelle Linee-guida sulla DPIA

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

V V V V V V V V V V V V V V V V V V



DI SEGUITO I QUESITI PROPOSTI DALLA PROCEDURA

CONTESTO

Questa sezione offre una visuale chiara del trattamento di dati personali in questione.

PANORAMICA

Questa parte permette di identificare e presentare l'oggetto dello studio.

- ⇨ Quale è il trattamento in considerazione?
  Presenta un breve sunto del trattmento: nome, scopo, finalità, contesto di uso, etc.
- ⇨ Quali sono le responsabilità legate al trattamento?
  Descrivi le responsabilità degli stakeholder: il titolare del trattamento, gli eventuali responsabili interni e co-incaricati.
- ⇨ Ci sono standard applicabili al trattamento?
  Elenca gli standard rilevanti applicabili al trattamento, specialmente i codici di condotta e le certificazioni di protezione dati.

NORMA

Descrizione dei trattamenti

Presentare una breve descrizione del trattamento in esame, la sua natura, lo scopo, il contesto, i propositi e i vincoli. Identificare il titolare dei dati e tutti gli incaricati. Elencare i riferimenti e le norme standard applicabili al trattamento, che sono necessari o devono essere rispettati, non ultimi i codici di condotta approvati (vedi Art. 40 del [GDPR]) e le certificazioni inerenti la protezione dei dati (vedi Art. 42 of the [GDPR])

DATI, PROCESSI E RISORSE DI SUPPORTO

Questa parte permette di definire e descrivere lo scopo del trattamento nel dettaglio.

- ⇨ Quali sono i dati trattati?
  elenca i dati raccolti e trattati definisci per ognuno la durata dell'archiviazione i destinatari e le persone con accesso
- ⇨ Com'è il ciclo di vita del trattamento dei dati?
  descrivi come funzione il processo (dalla raccolta alla distruzione) usando per esempio un diagramma di flusso dei dati ed una dettagliata descrizione dei processi effettuati
- ⇨ Quali sono le risorse di supporto ai dati?
  Elenca le risorse che ospitano i dati (sistemi operativi, applicazioni aziendali, database management systems, pacchetti office, protocolli, configurazioni etc.)

Dati e processo

Definire e descrivere l'ambito in dettaglio:
- i dati personali in questione, i loro destinatari e le durate di conservazione
- descrizione dei processi e delle risorse dedicate alla gestione dei dati personali per l'intero ciclo di vita dei dati stessi (dalla raccolta alla cancellazione)

Asset di supporto

Asset su cui si basano i trattamenti dei dati personali. Nota: questo può essere hardware, software, reti, persone, canali di trasmissione cartacei o documentazione

Principi Fondamentali

Questa sezione permette di generare lo schema di adeguamento secondo i principi considerati.

PROPORZIONALITÀ, NECESSITÀ

Questa sezione permette di dimostrare l'Implementazione dei mezzi necessari per abilitare le persone interessate ad esercitare i loro diritti.

- ⇨ Gli scopi del trattamento sono specifici, espliciti e legittimi?
  Spiegare perché le finalità del trattamento sono specifiche, esplicite e legittime.
- ⇨ Quali sono le basi legali che rendono il trattamento legittimo?
  Presentare le basi del trattamento (ad esempio consenso, esecuzione di un contratto, obbligo legale, interessi vitali etc.)
- ⇨ I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono stati trattati (minimizzazione dei dati)?
  spiegare perchè ogni dato raccolto è necessario per le finalità del trattamento
- ⇨ I dati sono accurati e mantenuti aggiornati?
  descrivere procedure per garantire aggiornamento
- ⇨ Quale è la durata della conservazione dei dati?
  spiegare perchè la durata risulta giustificata in base a requisiti legali o necessità

CONTROLLI PER PROTEGGERE I DIRITTI PERSONALI DEI SOGGETTI INTERESSATI

Questa sezione permette di dimostrare lemplementazione dei mezzi necessari per abilitare le persone interessate ad esercitare i loro diritti.

- ⇨ I soggetti interessati come sono informati del trattamento?
- ⇨ Come si ottiene il consenso dei soggetti interessati?
- ⇨ I soggetti interessati come esercitano i loro diritti di acceso alla portabilità dei dati?
- ⇨ Come i soggetti interessati esercitano i loro diritti alla rettifica e alla cancellazione?
- ⇨ i soggetti interessati come esercitano il loro diritto di restrizione e obiezione?
  descrivere i controlli attuati
- ⇨ Gli obblighi dei responsabili del trattamento sono chiaramente identificati e governati da un contratto?
  Per ogni responsabile del trattamento, descrivere le sue responsabilità, durata, finalità, scopo, istruzioni documentate, previa autorizzazione) e fornire i contratti, codici di condotta e certificazioni determinanti le missioni e gli obblighi
- ⇨ Nel caso di trasferimento di dati fuori dall'Unione Europea, i dati sono adeguatamente protetti?
  Per ogni nazione fuori dall'Unione Europea dove i dati sono archiviati e processati, indicare e descrivere se sono riconosciuti come offerenti di un livello adeguato di protezione dei dati o descrivere la fornitura di servizi concernenti il trasferimento.

RISCHI

Questa sezione permette di valutare i rischi della privacy, prendendo in considerazione controlli esistenti o pianificati.

CONTROLLI ESISTENTI O PIANIFICATI

Questa sezione permette di identificare i controlli (esistenti o pianificati) che contribuiscono alla sicurezza dei dati

- Crittografia *Descrivi i mezzi crittografici impiegati per i flussi di dati (VPN, TLS, etc.) implementati nel trattamento.*
  I mezzi implementati per **assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.).**
  Descrivi i mezzi crittografici impiegati per i flussi di dati (VPN, TLS, etc.) implementati nel trattamento.
- Anonimizzazione-
  Indicare qui se sono implementati meccanismi di anonimato, quali sono e per quali finalità
  Ricorda di distinguere tra dati anonimizzati o pseudonimi.
- Partizionamento dei dati
  Implementare il partizionamento dei dati aiuta a ridurre la possibilità che i dati personali possano essere correlati e che avvengano compromissioni dei dati.
- Controllo degli accessi
  Metodi per definire ed attribuire profili degli utenti. Specificare i mezzi di autenticazione implementati. Se applicabili specificare le regole per le password (lunghezza minima, caratteri richiesti, durata della validità, numero di tentativi prima del blocco dell'account etc.).
- Tracciabilità
  Politiche che definiscono la tracciabilità la gestione dei log.
- Archiviazione
  Se applicabile, descrivere qui i processi di gestione dell'archivio (consegna, archiviazione, consultazione etc.) sotto la tua responsabilità. Specificare i ruoli relativi all'archivio (ufficio di origine, agenzie di trasferimento etc.) e la politica di archiviazione. Stabilisci se i dati possono rientrare nel contesto degli archivi pubblici.
- Sicurezza dei documenti cartacei
  Dove sono conservati i documenti cartacei contenenti dati utilizzati durante il trattamento, indicare qui come sono stampati, archiviati, distrutti e scambiati.
- Minimizzare la quantità di dati personali
  Si possono utilizzare i seguenti metodi: filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, ridurre la natura identificativa del dato, ridurre l'accumulazione dei dati, limitare l'accesso ai dati
- Vulnerabilità
  Politiche volte a limitare la probabilità e la gravità dei rischi per le risorse utilizzate durante l'operatività e procedure operative documentali, inventario e aggiornaemnto di software e hardware, affrontare vulnerabilitO duplicare i dati, limitare l'accesso fisico al materiale etc.).
- Lotta contro il malware
  Misure per proteggere l'accesso a reti pubbliche (internet) o non controllate (di partner) nonché postazioni e server contro malware che potrebbe compromettere la sicurezza dei dati.
- Gestione postazioni
  Misure adottate per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni etc.) vengano sfruttate per danneggiare i dati personali (aggiornamenti, protezione fisica e accesso, lavoro su uno spazio di rete di backup, controlli di integritO logging etc.).
- Sicurezza dei siti web
  Implementazione delle raccomandazioni ANSSI per la sicurezza dei siti web.

- Backup
  Politiche e mezzi implementati per assicurare la disponibilità o l'integrità dei dati personali, mentre si mantiene la loro confidenzialità,
- Manutenzione
  Esistenza di una politica di manutenzione fisica dell'attrezzatura, specificando l'eventuale ricorso al subappalto. Dovrà inquadrare la manutenzione remota se è autorizzata e specificare i metodi di gestione dei materiali difettosi.
- Contratti di trattamento
  Regolare i rapporti di approvvigionamento (es. responsabile trattamento dati, responsabile protezione dei dati, servizi cloud, ecc) tramite un contratto firmato intuitu personae
  - Richiedere al fornitore di inoltrare la sua politica di sicurezza dei sistemi informativi insieme a tutti i documenti di supporto delle sue certificazioni di sicurezza delle informazioni e allegare tali documenti al contratto. Garantire che le misure siano conformi alla propria politica di sicurezza ed alle raccomandazioni dell'autorità garante.
  - Determinare e fissare in modo preciso, su base contrattuale, le operazioni che il responsabile del trattamento potrà eseguire sui dati personali:
  1) I dati a cui avrà accesso o che gli saranno trasmessi.
  2) Le operazioni che deve eseguire sui dati.
  3) La durata per la quale può memorizzare i dati.
  4) Tutti i destinatari a cui il responsabile del trattamento potrà trasmettere i dati.
  5) Le operazioni da eseguire al termine del servizio (cancellazione permanente dei dati o restituzione dei dati nel contesto della reversibilità quindi distruzione di dati).
  6) Gli obiettivi di sicurezza stabiliti dal titolare del trattamento.
  - Determinare, su base contrattuale, la ripartizione delle responsabilità in merito ai processi legali volti a consentire agli interessati di esercitare i propri diritti.
  Esplicitamente vietare o regolare l'utilizzo di fornitori di secondo livello.
  - Chiarire nel contratto che il rispetto degli obblighi di protezione dei dati è un requisito vincolante del contratto.
- Sicurezza della rete
  A seconda del tipo di rete sulla quale il trattamento è effettuato (isolata, privata o internet), Specificare il firewall, le sonde di rilevamento intrusione o altri dispositivi (attivi o passivi) che sono responsabili di garantire la sicurezza della rete.
- Controllo degli accessi fisici
  Politiche per assicurare la sicurezza fisica (zonizzazione, accompagnamento, uso di tornelli, porte chiuse e così via). Indicare se sono in atto procedure di avviso in caso di irruzione.
- Monitoraggio dell'attività della rete
  Esistenza di misure messe in atto per essere in grado di rilevare tempestivamente incidenti relativi a dati personali e di disporre elementi utilizzabili per studiarli o fornire elementi di prova nel contesto delle indagini (politica di registrazione eventi, rispetto degli obblighi di protezione dei dati etc.)
- Sicurezza dell'hardware
  Esistenza delle misure adottate per ridurre la possibilità che le caratteristiche delle apparecchiature (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovibili etc.) vengano utilizzate per danneggiare i dati personali (inventario, compartimentalizzazione, ridondanza, limiti per l'accesso etc.)
- Evitare le fonti di rischio
  Esistenza di misure per prevenire le fonti di rischio, umane o no numane, che possono essere incontrate a scapito dei dati personali (merci pericolose, aree geografiche pericolose, trasferimento dati al di fuori dell'UE etc.)
- Protezione contro fonti di rischio non umane
  Esistenza di misure per ridurre o evitare i rischi connessi a fonti non umane (fenomeni climatici, incendio, danni provocati dall'acqua, incidenti interni o esterni, animali, etc.) che potrebbero influire sulla sicurezza dei dati personali (misure preventive, rilevamento, protezione etc.)

- Organizzazione
  Esistenza di un'organizzazione in grado di dirigere e controllare la protezione dei dati personali all'interno dell'organizzazione (designazione di un DPO, creazione di un organo di monitoraggio, etc.)
- Politiche
  Il titolare del trattamento dei dati deve disporre di una banca dati documentale che formalizzi gli obiettivi e le regole da applicare nel campo della protezione dei dati (rischi, principi chiave da seguire, obiettivi, regole da applicare, ecc., revisione periodica della politica IT etc.)
- Gestione dei rischi sulla privacy
  Esistenza di una politica che definisce i processi volti a controllare i rischi che i trattamenti dell'organizzazione pongono sui diritti e le libertà delle persone interessate (censimento del trattamento dei dati personali, quali dati sono, valutazione del rischio, determinare misure esistenti o previste etc.)
- Integrare la protezione della privacy nei progetti
  Esistenza di procedure che descrivono i metodi per tenere conto della protezione dei dati personali in qualsiasi nuovo trattamento (etichette di fiducia, norme, gestione del rischio per la persona interessata secondo una metodologia etc.)
- Gestire le violazioni dei dati personali
  Esistenza di un'organizzazione oeprativa per rilevare e gestire eventi che possono influire sulle libertà e sulla privacy delle persone interessate (definizione delle responsabilità a piano di reazione, caratterizzazione delle violazioni etc.)
- Gestione del personale
  Esistenza di un piano che inquadra lemisure di sensibilizzazione adottate sull'arrivo di una persona nella sua funzione e una procedura che descrive lemisure prese per l'accesso ai dati .
- Relazioni con terze parti
  Esistenza di una procedura per ridurre i rischi che l'accesso legittimo ai dati da parte di terzi possa porre alle libertà della vita privata delle persone interessate (identificazione dei terzi, contratto di suappalto, convenzione etc.)
- Supervisione
  Esistenza di misure per fornire una visione globale e aggiornata dello stato di protezione dei dati e conformità on il GDPR (per monitorare la conformità di trattamenti, obiettivi e indicatori, responsabilità ,etc).

ACCESSO ILLEGITTIMO AI DATI

Analizzare le cause e le conseguenze di accesso illegittimo ai dati, e stimare la gravità e la probabilità,

- ⇨ Quale potrebbe essere l'impatto sui soggetti interessati se il rischio si dovesse realizzare?
- ⇨ Quali sono le principali minacce che potrebbero concretizzare il rischio?
- ⇨ Quali sono le fonti di rischio?
- ⇨ Quali dei controlli identificati contribuiscono a gestire il rischio?
- ⇨ Come stimeresti la gravità del rischio, specialmente riguardo i potenziali impatti e i controlli pianificati?

  (Indefinito) Trascurabile Limitato Importante Massimo
- ⇨ Come stimeresti la probabilità del rischio, specialmente riguardo le minacce, fonti di rischio e i controlli pianificati?

  (Indefinito) Trascurabile Limitato Importante Massimo

MODIFICHE INDESIDERATE DEI DATI

Analizzare le cause e le conseguenze di modifiche indesiderate ai dati, e stimare la gravità la probabilità dell'evento.

- ⇨ Quali impatti ci sarebbero sui soggetti interessati se il rischio si dovesse concretizzare?
- ⇨ Quali sono le principali minacce che possono portare al rischio?
- ⇨ Quali sono le fonti di rischio?
- ⇨ Quali dei controlli identificati contribuiscono a gestire il rischio?
- ⇨ Come stimeresti la gravità del rischio, in particolare riguardo l'impatto potenziale e i controlli pianificati?

  (Indefinito) Trascurabile Limitato Importante Massimo
- ⇨ Come stimeresti la probabilità del rischio, specialmente riguardo minacce, fonti di rischio e controlli pianificati?

  (Indefinito) Trascurabile Limitato Importante Massimo

SCOMPARSA DI DATI

Analizzare le cause e le conseguenze della perdita di dati e stimare la gravità, la probabilità dell'evento.

⇨ Quale potrebbe essere l'impatto sui soggetti interessati se il rischio dovesse realizzarsi?

⇨ Quali sono le minacce che potrebbero portare al rischio?

⇨ Quali sono le fonti di rischio?

⇨ Quali dei controlli identificati contribuisce a gestire il rischio?

⇨ Come stimeresti la gravitàel rischio, specialmente riguardo il potenziale impatto e i controlli pianificati?

(Indefinito) Trascurabile Limitato Importante Massimo

⇨ Come stimeresti la probabilità del rischio, specialmente rispetto le minacce, fonti di rischio e i controlli pianficati?

(Indefinito) Trascurabile Limitato Importante Massimo

PANORAMICA DEL RISCHIO

Questa visualizzazione permette di avere una visuale globale e sintetica degli effetti dei controlli sui rischi che gestiscono.

MAPPATURA DEL RISCHIO

Questa visualizzazione permette di comparare il posizionamento del rischio prima e dopo l'applicazione dei controlli complementari.

PIANO D'AZIONE

Pianificare in dettaglio l'implementazione di controlli aggiuntivi identificati durante il PIA.

PARERI DI DPO E SOGGETTI INTERESSATI

Presentare l'opinione delle persone responsabili della protezione dei dati e dei problemi di privacy (o eventuali delegati). Presentare anche le opinioni dei soggetti interessati o di loro rappresentanti.