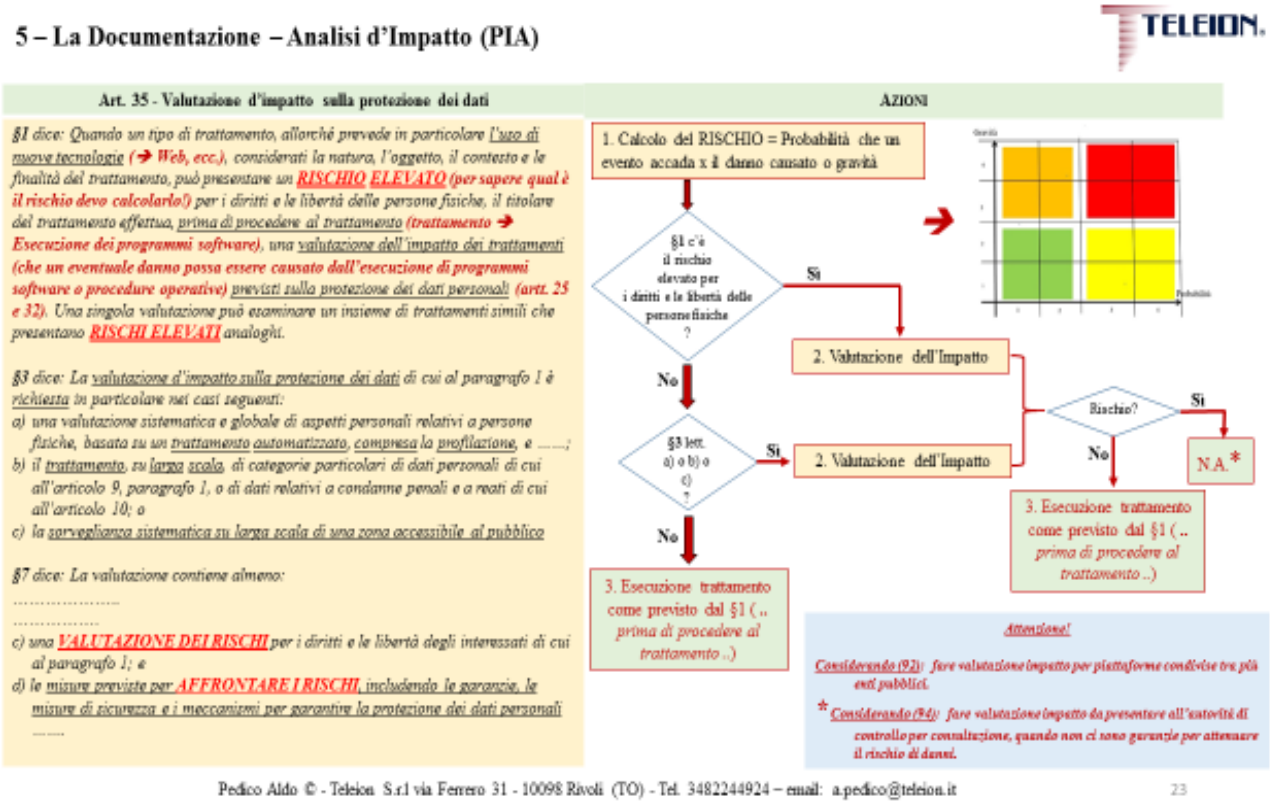
INDICAZIONI PRATICHE DI ADEGUAMENTO TECNOLOGICO AL GDPR

VALUTAZIONE D'IMPATTO-CALCOLO DEL RISCHIO (ART. 35)

CHE COSA È LA VDI?

Se esiste un rischio elevato, il TdT deve garantire la conformità alle leggi, alle normative e ai requisiti delle politiche per la privacy.

Ovvero, se sui diritti e sulle libertà delle persone fisiche, il danno impatta per quantità di pubblico oppure per entità del danno, il TdT può non eseguire il trattamento salvo autorizzazione dell'autorità di controllo, in seguito alla consultazione.



NOVE CRITERI PER LA DEFINIZIONE DI UN INSIEME DI TRATTAMENTI A CUI EFFETTUARE LA VDI – WP248

Il regolamento generale sulla protezione dei dati non richiede la realizzazione di una VdI sulla protezione dei dati per ciascun trattamento che può presentare rischi per i diritti e le libertà delle persone fisiche. La realizzazione di una VdI sulla protezione dei dati è obbligatoria soltanto qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, §1, illustrato dall'art. 35, §3, e integrato dall'art. 35, §4). Essa è particolarmente importante quando viene introdotta una nuova tecnologia di trattamento dei dati.

Nei casi in cui non è chiaro se sia richiesta una VdI sulla protezione dei dati o meno, il ***WP29*** *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.*

Sebbene una VdI sulla protezione dei dati possa essere richiesta anche in altre circostanze, l'art. 35, §3, fornisce alcuni esempi 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 fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, §1, o di dati relativi a condanne penali e a reati di cui all'art. 1013; o

c) *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".*

Al fine di fornire un insieme più concreto di trattamenti che richiedono una VdI sulla protezione dei dati in virtù del loro rischio elevato intrinseco, tenendo conto degli elementi particolari di cui all'art. 35, §1 e all'art. 35, §3, lettere da a) a c), l'elenco da adottare a livello nazionale ai sensi dell'art. 35, §4, e dei cons. 71, 75 e 91, e di altri riferimenti del regolamento generale sulla protezione dei dati a trattamenti che "possono presentare un rischio elevato", si devono considerare i seguenti nove criteri.

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" (cons. 71 e 91).*
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" (art. 35, §3, lett. a)).*
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" (art. 35, §3, lett. c)).*
4. *Dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'art. 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'art. 10. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti).*
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 cons. 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:*
   a. *il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;*
   b. *il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;*
   c. *la durata, ovvero la persistenza, dell'attività di trattamento;*
   d. *la portata geografica dell'attività di trattamento;*
6. *Creazione di corrispondenze o combinazione di insiemi di dati;*
7. *Dati relativi a interessati vulnerabili (cons. 75);*
8. *Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative: ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una VdI sulla protezione dei dati.*
9. *Quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (art. 22 e cons. 91).*

CASI IN CUI NON SIA RICHIESTA LA VDI – WP248

Il ***WP29*** ritiene che una VdI sulla protezione dei dati non sia richiesta nei seguenti casi:

a) quando il trattamento non è tale da "*presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 35, §1);

b) 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.

c) quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate (cfr. III.C);

d) qualora un trattamento, effettuato a norma dell'art. 6, §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 (art. 35, §*10), a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;*

e) 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 (art. 35, §5);

f) non è necessaria una VdI sulla protezione dei dati per i trattamenti che sono stati verificati da un'autorità di controllo o dal RPD, a norma dell'art. 20 della direttiva 95/46/CE e che vengono eseguiti in maniera tale da fare sì che non si sia registrata alcuna variazione rispetto alla verifica precedente.

CARATTERISTICHE MINIME DI UNA VDI – WP248

Il regolamento generale sulla protezione dei dati definisce le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati (art. 35, §7, e cons. 84 e 90):

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

Nel valutare l'impatto di un trattamento va tenuto conto (art. 35, §8) del rispetto di un codice di condotta (art. 40). Ciò può essere utile per dimostrare che sono state scelte o messe in atto misure adeguate, a condizione che il codice di condotta sia adeguato all'operazione di trattamento interessata. Devono essere presi in considerazione anche certificazioni, sigilli e marchi al fine di dimostrare la conformità rispetto al regolamento generale sulla protezione dei dati dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento (art. 42), nonché rispetto alle norme vincolanti d'impresa.

Tutti i requisiti pertinenti stabiliti nel regolamento generale sulla protezione dei dati offrono un quadro ampio e generico per la progettazione e lo svolgimento di una VdI sulla protezione dei dati.

Il cons. 90 del regolamento generale sulla protezione dei dati delinea una serie di elementi costitutivi della VdI sulla protezione dei dati che si sovrappone a elementi ben definiti della gestione del rischio.

In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:

1. stabilendo il contesto: *"tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio";*
2. valutando i rischi: *"valutare la particolare probabilità e gravità del rischio";*
3. trattando i rischi: *"attenuando tale rischio*" e "*assicurando la protezione dei dati personali*", e "*dimostrando la conformità al presente regolamento*".

PUBBLICAZIONE DI UNA VDI – WP248

La pubblicazione di una VdI non è un requisito giuridico sancito dal Regolamento Generale sulla protezione dei dati, è una decisione del TdT procedere in tal senso. Tuttavia, i TdT dovrebbero prendere in considerazione la pubblicazione di almeno alcune parti, ad esempio di una sintesi o della conclusione della loro VdI.

CRITERI PER UNA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI ACCETTABILE – WP248

Il ***WP29*** 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:

a) <u>una descrizione sistematica del trattamento è fornita</u> (art. 35, §7, lett. a)):

1. la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (cons. 90);
2. vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
3. viene fornita una descrizione funzionale del trattamento;
4. sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);
5. si tiene conto del rispetto dei codici di condotta approvati (art. 35, §8);

b) <u>la necessità e la proporzionalità sono valutate (art. 35, §7, lett. b)):</u>

1. sono state determinate le misure previste per garantire il rispetto del regolamento (art. 35, §7, lett. d) e cons. 90):
   - ❖ misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
     - Ψ finalità determinate, esplicite e legittime (art. 5, §1, lett. b));
     - Ψ liceità del trattamento (art. 6);
     - Ψ dati personali adeguati, pertinenti e limitati a quanto necessario (art. 5, §1, lett. c));
     - Ψ limitazione della conservazione (art. 5, §1, lett. 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 (art. 28);
  - garanzie riguardanti trattamenti internazionali (capo V);
  - consultazione preventiva (art. 36).

c) i rischi per i diritti e le libertà degli interessati sono gestiti (art. 35, §7 lett. c)):

1. l'origine, la natura, la particolarità e la gravità dei rischi (cfr. cons. 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 (cons. 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 (cons. 90);
2. sono determinate le misure previste per gestire tali rischi (art. 35, §7, lett. d) e cons. 90);

d) le parti interessate sono coinvolte:

1. si consulta il responsabile della protezione dei dati (art. 35, §2);
2. si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (art. 35, §9).

VANTAGGI PER EFFETTUARE UNA VDI

Questo standard internazionale fornisce una guida che può essere adattata a una vasta gamma di situazioni in cui PII viene elaborato. Tuttavia, in generale, una VdI può essere effettuata allo scopo di:

a) identificare gli impatti, i rischi e le responsabilità sulla privacy;
b) fornire input per progettare per la tutela della privacy (art. 25);
c) revisionare i rischi per la privacy di un nuovo sistema di informazione e di valutarne l'impatto e la probabilità;
d) fornire la base per la fornitura di informazioni sulla privacy per i principali PII su qualsiasi azione di mitigazione;
e) mantenere gli aggiornamenti successivi con funzionalità aggiuntive;
f) condividere e mitigare i rischi con le parti interessate; fornendo le informazioni relative alla conformità.

*NOTA. Una VdI è a volte indicata con altri termini: "**Privacy Review**"; "**VdI**".*

I costi di modifica di un progetto in fase di pianificazione di solito è una frazione di quelle sostenute in seguito.

Se l'impatto è inaccettabile, il progetto può essere annullato del tutto.

Tuttavia, una VdI aiuta a identificare i problemi precocemente e ridurre i costi del tempo di gestione, le spese legali e potenziali mediatici o d'interesse pubblico, prendendo in considerazione i problemi in anticipo.

Esso può anche aiutare un'organizzazione a evitare costosi errori e imbarazzanti sulla privacy.

Anche se una VdI dovrebbe essere più di un semplice controllo di conformità, comunque contribuisce a dimostrare la conformità di un'organizzazione ai pertinenti requisiti di privacy e protezione dei dati in caso di un'indagine successiva denuncia, controllo della privacy o la conformità. In caso di rischio per la privacy o violazione che si verifica, il rapporto VdI può fornire la prova che l'organizzazione ha agito in modo appropriato nel tentativo di prevenire il verificarsi. Questo può aiutare a ridurre o addirittura eliminare ogni responsabilità, pubblicità negativa e la perdita di reputazione.

Una VdI aumenta un processo decisionale informato ed espone le lacune di comunicazione interna o ipotesi nascoste su questioni di privacy in merito al progetto.

Una VdI permette all'organizzazione di conoscere in anticipo le insidie alla privacy di un processo, di un sistema informatico o un programma, piuttosto che avere i suoi revisori dei conti o concorrenti che glieli facciano notare.

Una VdI può aiutare:

1. un'organizzazione a guadagnare la fiducia del pubblico e la fiducia che la privacy è stata costruita nella progettazione di un processo, di un sistema informatico o di un programma;
2. ad anticipare e rispondere alle preoccupazioni del pubblico sulla privacy.

OBIETTIVI DELLE SEGNALAZIONI VDI

L'obiettivo di segnalazione VdI è quello di comunicare i risultati della valutazione alle parti interessate e di soddisfare le loro aspettative.

I seguenti esempi sono tipici di un'aspettativa delle parti interessate:

a) PII principale – VdI è uno strumento per consentire soggetti di PII per avere la certezza che la loro privacy è protetto.

b) Gestione – diversi punti di vista si applicano con:

1. la VdI come strumento per gestire i rischi per la privacy, creare consapevolezza e stabilire responsabilità; visibilità oltre l'elaborazione PII all'interno dell'organizzazione, e possibili rischi, impatti dello stesso;
2. effettuare la VdI nelle prime fasi del progetto garantisce che i requisiti di privacy sono inclusi nei requisiti funzionali e non, sono realizzabili, sono vitali e vengono tracciati attraverso il cambiamento e la gestione dei rischi; lo sforzo per classificare e gestire progetti PII dovrebbe essere finanziato come linea di investimento separata e quantificata in un bilancio di progetto;
3. la VdI è uno strumento per comprendere i rischi per la privacy a / progetto / livello di unità la funzione; il consolidamento dei rischi; Ingresso ai meccanismi di progetto e di applicazione sulla Privacy; ingressi per i processi di privacy re–Engineering.

c) Regolatore – VdI è uno strumento che contribuisce a fornire elementi di prova per la conformità con i requisiti legali applicabili. È in grado di fornire la prova di atti dovuti adottati dall'organizzazione in caso di violazione, non conformità, denuncia, etc.

d) Cliente – VdI è un mezzo per valutare come il processore PII o il titolare PII sta gestendo PII e fornisce la prova che segue gli obblighi contrattuali.

La segnalazione di VdI dovrebbe svolgere due funzioni fondamentali.

1. Inventario: mantiene i soggetti specifici informati delle entità colpite, l'ambiente interessato e i rischi sul ciclo di vita delle entità colpite.
2. Voci di azione: è un meccanismo di monitoraggio sulle azioni/attività che migliorano e/o risolvono i rischi identificati. La sensibilità per la distribuzione e la divulgazione delle informazioni di segnalazione deve essere chiaramente valutata e classificata (privato, confidenziale, pubblico, ecc.).

LA RESPONSABILITÀ DI CONDURRE UNA VDI

In genere, la responsabilità di assicurare che una VdI è stata intrapresa dovrebbe, in primo luogo, se ce n'è uno, il responsabile della protezione PII, altrimenti con il responsabile del progetto di sviluppo della nuova tecnologia, del servizio o di un'altra iniziativa che possa impattare sulla privacy.

Quando la VdI viene eseguita direttamente dall'organizzazione, le associazioni degli utenti finali o agenzie governative possono richiedere di avere l'adeguatezza della VdI verificata da un revisore indipendente.

L'organizzazione deve garantire che vi sia la responsabilità e l'autorità per la gestione dei rischi, compresa l'attuazione e il mantenimento del processo di gestione del rischio e per garantire l'adeguatezza e l'efficacia dei controlli.

Questo può essere agevolato da:

a) specificare chi è responsabile per lo sviluppo, l'implementazione e la manutenzione del quadro di gestione del rischio; e

b) specificare i proprietari del rischio per l'attuazione del trattamento del rischio, mantenendo i controlli della privacy e la comunicazione delle informazioni rilevanti il rischio.

METODOLOGIA PER L'ESECUZIONE DELLA VALUTAZIONE D'IMPATTO

L'ambito di una VdI, i dettagli specifici di ciò che copre e come si è condotto tutti bisogno di essere adattata alla dimensione dell'organizzazione, la competenza territoriale e il programma specifico, il sistema di informazioni o di un processo che è oggetto della VdI.

L'organizzazione conducendo un processo VdI può desiderare di adattare direttamente la guida processo seguito per la sua specifica scala VdI e di scopo o come una possibile alternativa per selezionare un adeguato sistema di gestione basato sui rischi, come ISO/IEC 27001, e integrare in modo appropriato elementi atti della guida sotto, compreso l'uso del rapporto VdI per il trattamento della privacy rischia identifica.

Nella presente norma internazionale, il termine "conducendo una VdI" viene utilizzato per coprire sia una VdI iniziale in cui vengono selezionati i passi e le azioni necessarie per soddisfare il requisito particolare VdI; e un aggiornamento a una VdI esistente in cui vengono effettuati solo i passi e le azioni necessarie per l'aggiornamento.

L'allegato C fornisce ulteriori indicazioni sulla comprensione dei termini utilizzati nella presente norma internazionale.

NOTA Per sostenere le PMI nel processo della VdI, associazioni di categoria o enti di piccole e medie imprese dovrebbero essere incoraggiati a redigere codici di condotta fornendo linee guida preziose, e le PMI dovrebbero essere incoraggiati a partecipare a queste attività. I codici di condotta ragionevoli dovrebbero rispettare i valori di cui al presente lnternational standard e potrebbe ottenere approvato da autorità per la protezione dei dati.

Di seguito si elencano i passi metodologici per il raggiungimento dell'obiettivo.

a) Costituzione del gruppo VdI e fornire loro la direzione;
b) Preparazione di un piano VdI e determinazione delle risorse per condurre l'assessment;
c) Descrivere ciò che è in corso di valutazione;
d) Identificazione degli stakeholder;
e) Stabilire un piano di consultazione;
f) Consultarsi con gli stakeholder;
g) Identificare il flusso delle informazioni PII;
h) Analizzare le implicazioni dei casi in uso;
i) Determinare e salvaguardare i requisiti di privacy;
j) Identificazione delle minacce e calcolo dei rischi;
k) Minacce generiche;
l) Minacce derivabili dal trattamento dei dati personali nella Sanità;
m) Calcolo dei livelli del danno o della gravità e della probabilità;
n) Valutazione della priorità dei rischi;
o) Classificazione del rischio;
p) Scegliere le azioni di trattamento dei rischi;
q) Determinare i controlli;
r) Creare i piani di trattamento dei rischi;
s) VdI;
t) Risoluzione.

La risoluzione della VdI deve basarsi sui risultati del processo di gestione del rischio che è stato eseguito, nonché sui rischi residui e la decisione di accettare i rischi o non accettarli.

Un'applicazione efficace / sistema intelligente sarà considerata soddisfacente dal responsabile del sistema una volta che il processo VdI è stato completato con rischi rilevanti individuati e opportunamente trattati per garantire l'assenza di rischi residui inaccettabili per le persone, e al fine di soddisfare i requisiti di conformità, con appropriate revisioni interne ed approvazioni.

Le seguenti soluzioni possono essere previste al termine del processo VdI:

1. Un sistema di rete intelligente o applicazione già in produzione:
   - ✓ VdI positiva: *le relazioni VdI devono essere registrate e conservate dal RPD dell'organizzazione e tenuti a disposizione dell'autorità per la protezione dei dati.*
   - ✓ VdI negativa: *un ulteriore esame sarà necessario con un piano di azioni correttive specifiche da sviluppare tra cui una proposta di controlli più efficienti o nuovi, e una nuova VdI da completare al fine di determinare se l'applicazione ha raggiunto uno stato approvabile.*
2. Un sistema di rete intelligente o applicazione ancora in fase di progettazione:
   - ✓ VdI positiva: *i rischi sono stati valutati e i controlli riguardanti tali rischi correttamente definiti e messi a punto. I rischi residui sono stati segnalati e non sono stati individuati ulteriori controlli e / o sono stati accettati alcuni rischi. Il rapporto VdI dovrebbe includere le date future per il controllo del sistema quando sarà in produzione.*
   - ✓ VdI negativa: *oltre a prevedere ulteriori controlli per l'ottenimento di un nuovo e soddisfacente livello di rischi residui, la relazione dovrebbe anche raccomandare quando possibile, le nuove azioni di progetto per l'applicazione seguendo il principio della Privacy by Design.*

È importante notare che la soluzione finale dovrebbe essere una decisione di gestione basata sui risultati delle valutazioni effettuate, rispecchiando l'interesse sociale relativo allo sviluppo della rete intelligente.

FOLLOW UP DELLA VDI

Questo processo conclude l'iter metodologico svolto all'interno del gruppo dei processi per valutazione d'impatto.

Di seguito si fornisce l'elenco delle attività che compongono il Follow Up della VDI.

A. *Preparazione del report*

B. *Pubblicazione*

C. *Attuazione dei piani di trattamento dei rischi*

D. *Review e/o audit della VdI*

E. *Affrontare le modifiche al processo*

F. *Documentazione per la VdI*

Questa punto fornisce indicazioni sul contenuto della relazione VdI.

I contenuti del rapporto VdI dipenderanno fortemente dal tipo e dalla sensibilità di PII essere processi, la sua natura e la portata e objectiv.es della VdI condotta. Così questa guida dovrebbe essere interpretato nel contesto del progetto specifico.

Alcuni dei dettagli del rapporto VdI possono essere riservate. Essi possono risolvere i problemi di business che non dovrebbero essere resi pubblici. Essi possono affrontare le opzioni di trattamento che possono rivelare dettagli sufficienti sui rischi residui per aumentare il rischio di compromissione del sistema.

L'organizzazione dovrebbe determinare il pubblico appropriato e contenuti della relazione VdI e il suo grado di riservatezza. Una relazione di fiducia a un revisore indipendente o ad una autorità di protezione dei dati può contenere più informazioni rispetto a quello fornito alle parti interessate o al pubblico.

L'organizzazione dovrebbe considerare affrontare le seguenti problematiche e prendere in considerazione le indicazioni fornite di seguito.

a) La struttura del documento.
b) La portata della valutazione; i requisiti di privacy; la valutazione del rischio.
c) Il piano di trattamento del rischio.
d) La conclusione e le decisioni prese sulla base del risultato della VdI.
e) Una sintesi pubblica VdI adatto ad essere utilizzato per informare i principali PII circa il livello di rischio associato al programma, sistema informativo, e il processo di attuazione in cui la loro PII sarà coinvolto.

STRUTTURA DEL DOCUMENTO

Il rapporto VdI dovrebbe essere adattata alle circostanze specifiche.

Normalmente indicati:

a) *nella sua pagina di copertina:*
   1. il nome del processo;
   2. il sistema informatico o un programma;
   3. il nome e l'indirizzo del responsabile PII e dell'organizzazione che svolge la VdI;
   4. la persona di contatto con i dettagli di contatto;
   5. il numero di versione per il controllo dei documenti;
   6. la data del rapporto VdI; e
   7. anche nominare coloro che possono affrontare qualsiasi domanda se diversi dalla persona che ha condotto la VdI;
   8. se il rapporto VdI è lungo, esso dovrebbe includere una sintesi indicando le principali conclusioni e raccomandazioni della VdI e che le parti interessate sono state consultate, una breve descrizione del programma, del sistema informativo, di processo o di altra iniziativa, che è stata oggetto della VdI;
   9. il motivo per cui la VdI è stato intrapreso

b) *Introduzione*
L'introduzione dovrebbe indicare il motivo per cui una VdI è stata condotta, quando è stata condotta, che è stato coinvolto nella conduzione della VdI e i termini di riferimento della VdI. Essa dovrebbe fornire alcune informazioni sul processo, sistema informatico o di un programma di valutazione. Si dovrebbe introdurre le linee guida impiegate nella VdI (ad esempio, la decisione di coinvolgere le parti interessate). L'introduzione dovrebbe fornire tutte le informazioni contestuali sull'organizzazione e il suo ambiente che potrebbe essere necessaria al fine di comprendere la motivazione della VdI. L'introduzione potrebbe anche fare riferimento alla politica sulla privacy

dell'organizzazione o al codice di condotta, nonché gli obblighi dell'organizzazione ai suoi stakeholder (azionisti e, se del caso), così come la sua conformità con la legislazione pertinente.

c) *Informazioni sui requisiti di sistema*
d) *Informazioni dell'architettura di sistema*
e) *Piani operativi e procedure*
f) *Criteri di rischio*
g) *Risorse e persone coinvolte*
h) *Consultazione delle parti interessate*
i) *Requisiti della Privacy*
j) *Piano di trattamento del Rischio*
k) *Conclusioni e Decisioni*

PUBBLICAZIONE

Al fine di fornire per gli utenti informazioni sui rischi della privacy, siano essi principi PII esterni o dipendenti, per sostenere il consenso, una sintesi pubblica della VdI può avere bisogno di essere preparati dal report principale VdI.
Se necessario, la sintesi dovrebbe rimuovere informazioni commercialmente sensibili che potrebbero essere presenti nel rapporto completo VdI e lasciare solo gli aspetti chiave rilevanti per i principali PII.

Il rapporto di sintesi VdI pubblico deve contenere:

a) i vantaggi del programma, del sistema di informazione o di processo;
b) i tipi di PII per essere elaborati e raccolti;
c) le giurisdizioni legali in cui viene realizzato il trattamento PII;
d) una sintesi delle analisi delle conformità;
e) un elenco delle eventuali misure per conformarsi ai requisiti di privacy o per il trattamento di rischio per la privacy che gli intenti dell'organizzazione per adottare o abbia adottato;
f) le misure che i principali PII si raccomanda di prendere;
g) l'organizzazione responsabile della VdI e del programma, il sistema di informazione o di processo;
h) i dati di contatti del titolare responsabile; e
i) i dettagli di ogni utente rilevati da help desk o da una struttura di supporto degli utenti messe in atto per il programma, il sistema di informazione o di processo.

Quando la sintesi degli indirizzi pubblica della VdI si rivolge a i principali PII come membri del pubblico in generale, essi dovrebbero rappresentare tutte le informazioni di cui sopra e tutte le ulteriori informazioni in modo trasparente, chiaro e comprensibile.