Valutazione d'impatto sulla protezione dei dati – applicazione dell'art. 35 del Regolamento europeo n. 679 del 27 aprile 2016 in materia di protezione dei dati personali

Redazione	Validazione
Il Segretario	Il DPO

1. SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO

L'Art. 35 del Regolamento europeo n. 679 del 27 aprile 2016 in materia di protezione dei dati personali introduce la **valutazione preventiva dell'impatto** dei trattamenti previsti sulla protezione dei dati personali.

Più specificamente, l'art. 35 prescrive che:

- Comma 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*".

- Comma3: "*La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:*
  - *una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*
  - *il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;*
  - *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*".

- Comma 7: "*La valutazione contiene almeno:*
  - *una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;*
  - *una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;*
  - *una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;*
  - *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*".

Il presente documento contiene i registri delle attività di trattamento e la relativa valutazione preventiva dell'impatto dei trattamenti previsti sulla protezione dei dati personali, redatta dai Responsabili del trattamento dell'Unione Colline Matildiche e validata dal Responsabile della Protezione dei dati (DPO); i registri delle attività di trattamento informatizzati e la valutazione d'impatto sono conservati in forma controllata dai Responsabili del trattamento.

I Responsabili del trattamento procedono ad un riesame almeno annuale di tale valutazione d'impatto.

2. LA METODOLOGIA ADOTTATA PER LA VALUTAZIONE D'IMPATTO

Come evidenziato, la valutazione d'impatto è richiesta in alcuni casi specifici ma è comunque –in coerenza con il principio di adeguatezza che permea il Regolamento - applicabile per ogni tipologia di trattamento.

In fase di prima applicazione del Regolamento europeo, i Responsabili di trattamento hanno reputato opportuno sottoporre alla valutazione d'impatto un numero molto più significativo di trattamenti, al fine di evitare che una interpretazione troppo riduttiva potesse portare, soprattutto in presenza di dati personali ritenuti di una certa rilevanza- ad una pericolosa sottostima del rischio di violazione dei dati; la selezione dei trattamenti da sottoporre a valutazione d'impatto è stata effettuata in sede di compilazione del registro delle attività di trattamento.

La metodologia adottata si rifà alla norma UNI ISO 31000:2010 "Gestione del rischio", che prevede che per valutare quanto un rischio è elevato si deve tener conto di **due variabili indipendenti** che caratterizzano un evento (in questo caso la violazione dei dati personali che può ledere i diritti e le libertà degli interessati):

- La **probabilità potenziale** che la violazione abbia luogo
- Nel caso in cui abbia luogo, **l'impatto di tale violazione** in termini di riservatezza, integrità e disponibilità.

L'indice di rischio è il prodotto di tali variabili e può essere preso come riferimento per la sua entità.

A supporto dell'analisi del rischio possono essere adottate **scale percettive** quali ad esempio la valutazione **Alto/Medio/Basso** utilizzando una **scala numerica 0->3** sia per la probabilità che per l'impatto, come quella di seguito presentata.

La matrice a supporto della valutazione del rischio

		IMPATTO		
		A =3	M =2	B =1
PROBABILITA'	A =3	A = 9	MA =6	M = 3
	M =2	MA =6	M =4	MB = 2
	B =1	M = 3	MB = 2	B =1

Da un punto di vista metodologico, al fine di garantire una omogeneità di valutazione, nel **ponderare la probabilità** di violazione i responsabili hanno tenuto conto dei seguenti elementi caratteristici del trattamento:

- La modalità di gestione o archiviazione dei dati
- La presenza di procedure e modalità operative a supporto della gestione dei dati o della loro tracciabilità
- Il rispetto di eventuali codici di condotta approvati
- La presenza di eventuali certificazioni (inerenti il tema della protezione dei dati) in possesso di chi tratta i dati
- Il valore presunto di tali dati anche da un punto di vista commerciale.

Nel **ponderare l'impatto** i responsabili del trattamento hanno invece tenuto conto dei seguenti elementi caratteristici del trattamento:

- La tipologia di dati personali gestiti
- La presenza di dati concernenti soggetti vulnerabili (minori, disabili, ecc.)
- Il numero di interessati coinvolti
- Se il rischio concerne la divulgazione non autorizzata o l'accesso piuttosto che la potenziale distruzione, perdita o modifica dei dati personali trattati.

Sia per valori elevati dell'indice di rischio che nei casi in cui l'indice di rischio è superiore alla soglia di accettabilità, è stata pianificata una strategia tesa a **mitigare il rischio**, fino a eliminarlo o renderlo accettabile; nella valutazione sono indicate le **misure** che si prevede di mettere in atto a tal fine, da avviare a cura del Responsabile del trattamento in oggetto, tenendo conto anche della necessità e proporzionalità dei trattamenti in relazione alle finalità.

Laddove una valutazione d'impatto sulla protezione dei dati riveli la presenza di **rischi residui elevati**, il responsabile si confronterà con il titolare del trattamento che sarà tenuto a richiedere la **consultazione preventiva** dell'autorità di controllo in relazione al trattamento in oggetto.

I Responsabili del trattamento conservano in forma controllata le valutazioni d'impatto dei trattamenti considerati meritevoli di tale verifica, con evidenza –per ogni trattamento:

- della finalità del trattamento stesso
- della stima di probabilità e impatto della potenziale violazione dei dati
- della determinazione dell'indice di rischio di violazione del trattamento
- della stima dell'adeguatezza delle misure organizzative e tecniche attualmente in essere
- dell'individuazione delle eventuali misure ulteriori previste per affrontare i rischi.