Torna indietro

Circolare 31 maggio 2019 - Regolamento generale sulla protezione dei dati (Regolamento UE 2016/679) - Valutazione d'impatto sulla protezione dei dati (cd. DPIA) - Istruzioni operative e modulistica

31 maggio 2019

Ministero della Giustizia
LA RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI

Al Sig. Capo di Gabinetto del Ministro
Al Sig. Capo dell'Ufficio legislativo
Alla Segreteria del Ministro
Alla Segreteria del sottosegretario di Stato Vittorio Ferraresi
Alla Segreteria del sottosegretario di Stato Jacopo Morrone
All'Ufficio stampa e informazione
Al Sig. Capo dell'Ufficio centrale degli archivi notarili
Al Sig. Direttore della Direzione generale per il coordinamento delle politiche di coesione
Al Responsabile della prevenzione della corruzione e della trasparenza
All'Organismo indipendente di valutazione della performance
Ai sig.ri Capi di Dipartimento
Dipartimento per gli affari di giustizia
Dipartimento dell'organizzazione giudiziaria, del personale e dei servizi
Dipartimento dell'amministrazione penitenziaria
Dipartimento per la giustizia minorile e di comunità
e p.c. Al Sig. Garante per la protezione dei dati personali

OGGETTO: **Regolamento generale sulla protezione dei dati (Regolamento UE 2016/679). Valutazione d'impatto sulla protezione dei dati (cd. DPIA) Istruzioni operative e modulistica**

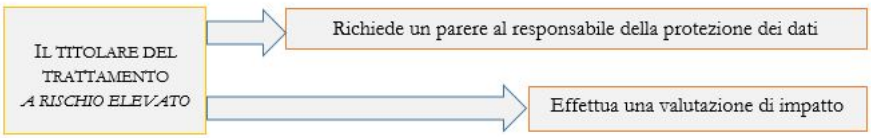
1. Valutazione d'impatto sulla protezione dei dati
"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali" (art. 35, Reg.). Lo svolgimento della valutazione d'impatto sulla protezione dei dati (DPIA) ha il fine di determinare, in particolare, l'origine, la natura, la particolarità e la gravità del rischio (Considerando n. 84).

Il regolamento UE n. 2016/679 non definisce formalmente il concetto di valutazione d'impatto sulla protezione dei dati: essa, però, può essere definita come un processo inteso 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, valutando detti rischi e determinando le misure per affrontarli (v. Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati).

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; 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 Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati (art. 35, paragrafo 3, Reg.). Infatti, rientra nei compiti del responsabile della protezione dei dati di fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento (art. 39, paragrafo 1, lett. c, Reg.). Sul valore della consultazione e del parere ci soffermeremo nel capo successivo.

Soffermandosi in questa sede sul ruolo del titolare, vanno richiamart le «**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» del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 ("WP 248, rev. 01"): esse chiariscono che la valutazione d'impatto deve essere condotta dal titolare, coadiuvato dal responsabile della protezione dei dati. La responsabilità della DPIA spetta, dunque, al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione.



La valutazione d'impatto sulla protezione dei dati è richiesta, in particolare, ove sussista: 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 (si ricorda che la valutazione d'impatto riguarda esclusivamente i dati delle persone fisiche, atteso che il regolamento 2016/679 non disciplina il trattamento dei dati personali relativi a persone giuridiche; v. Considerando n. 14); b) il trattamento, su larga scala, di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, paragrafo 1, Reg.) o di dati relativi a condanne penali e a reati (ai sensi dell'art. 10, Reg.); c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. Questo elenco non è tassativo ma meramente esemplificativo.

Per la individuazione dei trattamenti da sottoporre a DPIA, le menzionate Linee guida del Gruppo di Lavoro Articolo 29 hanno individuato nove criteri da tenere in considerazione ai fini dell'identificazione dei trattamenti che possono presentare un "rischio elevato" (il testo è disponibile al seguente link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236). Il ricorrere di due o più criteri è indice di un trattamento che presenta un rischio elevato per i diritti e le libertà degli interessati e richiede, quindi, una valutazione d'impatto sulla protezione dei dati (cfr. WP 248, rev. 01, pag. 11). Tuttavia, il titolare del trattamento può richiedere una valutazione d'impatto sulla protezione dei dati anche in presenza di uno solo di questi criteri, tenuto conto delle circostanze del caso concreto.

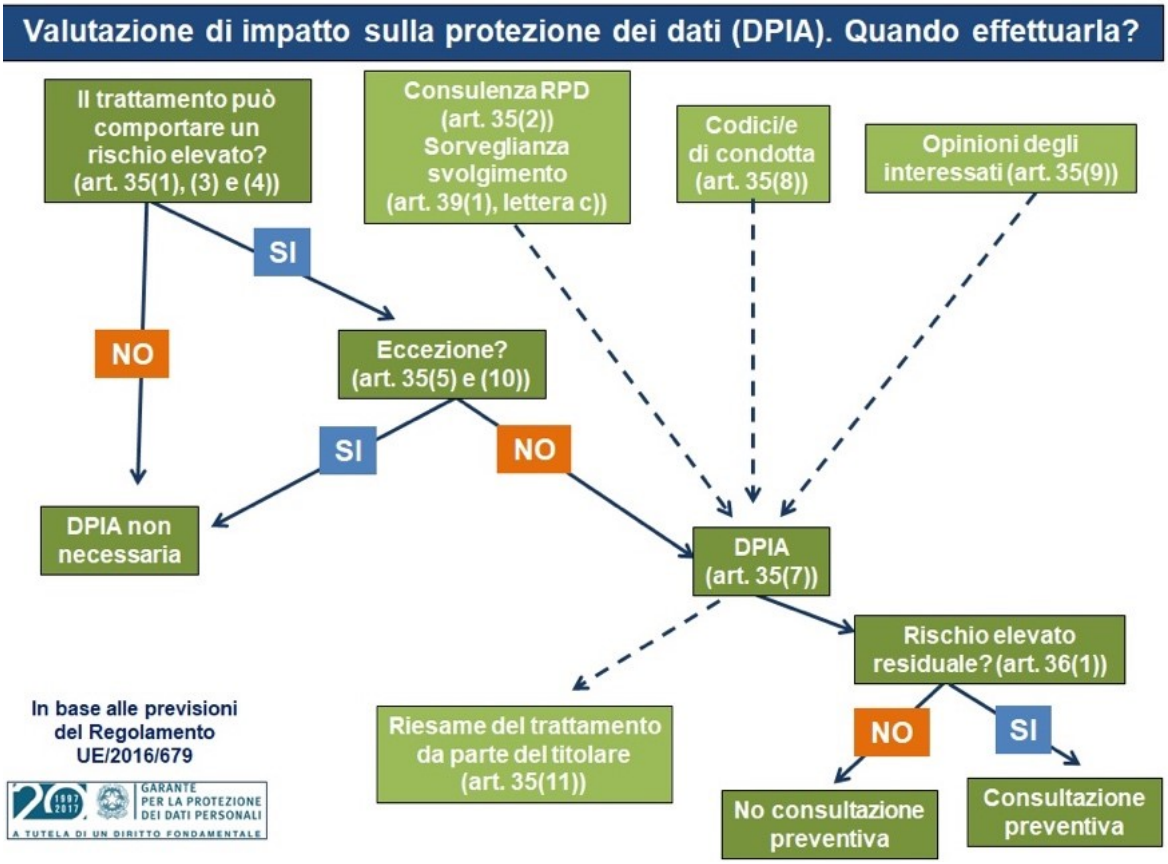
Il Garante per la protezione dei dati personali, con **provvedimento dell'11 ottobre 2018, ha introdotto un elenco delle tipologie di trattamenti** soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, par. 4, del Reg.: questo elenco è stato predisposto sulla base del WP 248, rev. 01, allo scopo di specificarne ulteriormente il contenuto e a complemento dello stesso
(https://www.garanteprivacy.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazio dd65-df86-fed4-df3c3570f59d?version=1.11).

Il Garante, ai sensi dell'art. 35, par. 5, Reg., potrebbe redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una DPIA. Allo stato, non è stato redatto e/o comunicato alcun elenco del genere.

E' opportuno ricordare che la valutazione d'impatto sulla protezione dei dati non è obbligatoria per ciascun trattamento ma solo per quello che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (articolo 35, par. 1, Reg.). Il riferimento a «diritti e libertà» degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si deve consultare il Garante per la protezione dei dati personali. In particolare, come emerge dai Considerando 94 – 96 del Regolamento UE n. 679 del 2016, la consultazione preventiva è necessaria nel caso in cui le misure tecniche e organizzative individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti (cioè quando il rischio residuale per i diritti e le libertà degli interessati resti elevato).

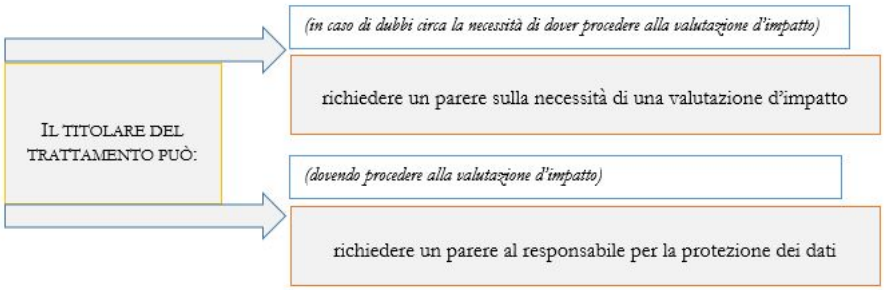
Il procedimento delineato dalla normativa unionale è, in sintesi, il seguente. Se il trattamento può comportare un rischio elevato e non ricorrono ipotesi che lo escludano, il titolare del trattamento deve procedere a fare una valutazione d'impatto, previa acquisizione del parere del responsabile per la protezione dei dati. Se, all'esito della DPIA, residua un rischio elevato, il titolare del trattamento deve procedere a consultazione preventiva (ex art. 36 Reg.).



2. Responsabile per la protezione dei dati

Nell'ipotesi in cui si debba procedere a valutazione d'impatto, il parere del responsabile della protezione dei dati (RPD) è un adempimento necessario; ciò emerge più chiaramente nel testo inglese del Regolamento, in cui l'art. 35 utilizza l'espressione "the controller shall seek the advice of the data protection officer" là dove "shall" indica un comportamento dovuto ("deve") e "advice" indica "parere" (espressione più chiara rispetto a quella italiana "si consulta"). Gli articoli 35 e 39 del Regolamento UE n. 679 del 2016, pertanto, devono essere interpretati nel senso che il titolare del trattamento a rischio elevato è tenuto a richiedere un parere al responsabile della protezione dei dati personali dovendo procedere a valutazione d'impatto. Più in particolare, l'art. 35, par. 2, Reg., là dove prevede che il titolare "si consulta" intende richiamare il "parere" menzionato dall'art. 39, par. 1, lett. c), Reg.

La richiesta di parere al responsabile per la protezione dei dati presuppone che il titolare ritenga che il trattamento possa presentare un rischio elevato e sia quindi necessaria una valutazione d'impatto. Ciò nondimeno, il "parere" che il RPD rende al titolare può includere anche il fatto che, in concreto, effettivamente sia necessaria (o non) una valutazione d'impatto (atteso che, comunque, il RPD ha compiti di consulenza in generale, ex art. 39, par. 1, lett. a Reg.). Pertanto, sono plausibili due distinte ipotesi: la prima, che il titolare sia incerto circa la necessità di una DPIA e a tal fine consulti il responsabile; la seconda, che il titolare sia già convinto che la valutazione sia necessaria e allora richieda il parere previsto dagli artt. 35, 39 Reg. Ebbene, in tale ultimo caso, il RPD non è vincolato al giudizio svolto dal titolare e ben potrebbe ritenere che, in realtà, nel caso sottoposto, la DPIA non è necessaria oppure osservare che è necessaria ma per motivi diversi da quelli indicati dal titolare. Il rapporto tra titolare e responsabile, al cospetto della valutazione d'impatto, è di tipo dialogico/cooperativo in quanto finalizzato a garantire una protezione effettiva dei dati personali e, pertanto, devono essere scongiurate interpretazioni che introducano formalismi non previsti dalla normativa primaria ed eurounitaria o che siano incompatibili con la ratio perseguita dalle disposizioni legislative di riferimento. Ciò vuol dire che, anche prima di una formale richiesta, sono ipotizzabili contatti al fine di verificare se il parere debba essere effettivamente richiesto. Ciò nondimeno, nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati, il WP29 raccomanda di effettuarla comunque, «in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento» al fine di «rispettare la legge in materia di protezione dei dati».



Il parere del responsabile della protezione dei dati non è vincolante per il titolare il quale può discostarsi dalle indicazioni ricevute: tuttavia, in casi del genere, il RPD conserva il potere di sorveglianza che l'art. 39, par. 1, lett. b) Reg. gli riconosce. In ogni caso, il parere ricevuto dal titolare del trattamento deve essere documentato all'interno della DPIA.

E' pacifico – perché normativamente previsto (art. 39, par. 1, lett. c, Reg.) - che il RPD deve sorvegliare lo svolgimento del procedimento che si conclude con la valutazione d'impatto (nella versione inglese "to monitor", ossia controllare, monitorare, verificare l'andamento). Ciò vuol dire che il titolare del trattamento deve aggiornare periodicamente il responsabile delle fasi della procedura, delle scelte poste in essere, dei risultati man mano raggiunti. Ad esempio, se il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto (art. 35, par. 9, Reg.), ne informa il RPD. In questa fase esecutiva, il RPD – in virtù di quel dialogo cooperativo di cui si è detto – può offrire supporto, dare indicazioni, esprimere pareri. L'intervento del RPD può anche appuntarsi sui

contenuti della valutazione (v. art. 35, par. 7, Reg.).

3. Modulistica
Per semplificare il dialogo cooperativo tra titolare e responsabile per la protezione dei dati, questo RPD ha predisposto la modulistica allegata alla presente nota, auspicando che gli uffici la adottino in base alle istruzioni offerte. Si tratta dei seguenti tre moduli, messi a disposizione in formato word e PDF: Modello n. 1 - Richiesta del parere al responsabile per la protezione dei dati personali; Modello n. 2 - Valutazione d'impatto; Modello n. 3 - Comunicazione degli aggiornamenti al responsabile per la protezione dei dati personali.

Modello n. 1 - Richiesta del parere al responsabile per la protezione dei dati personali (word - pdf)

Modello n. 2 - Valutazione d'impatto (word - pdf)

Modello n. 3 - Comunicazione degli aggiornamenti al responsabile per la protezione dei dati personali (word - pdf)

Roma, 31 maggio 2019

La Responsabile per la protezione dei dati personale
Doris Lo Moro