Le imprese e la riservatezza. Gli adempimenti legati al debutto del nuovo Regolamento europeo il prossimo 25 maggio

Privacy, rischi da valutare subito

Il documento d'impatto va redatto prima dell'utilizzo dei dati e per i trattamenti in corso

PAGINA A CURA DI
Daniele Colombo

Sono tenuti a redigere la «valutazione di impatto privacy» (la sigla inglese è Dpia: *data privacy impact assessment*) i datori di lavoro che:

- sono in possesso di dati sensibili di lavoratori (ad esempio dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale) «su larga scala»;
- conservano dati personali di soggetti vulnerabili (minori, soggetti in condizioni di minorata capacità fisica o psichica e così via).

È un adempimento previsto dal Regolamento europeo sulla rivacy (Gdpr) che, dal 25 maggio, sostituirà nel nostro ordinamento, definitivamente, le attuali norme sulla privacy.

L'articolo 35 del Regolamento Ue/2016/679 definisce la valutazione di impatto privacy come una procedura che mira a descrivere un trattamento di dati per valutarne la necessità, la proporzionalità e i relativi rischi, per adottare misure idonee a gestirli.

La Dpia è uno strumento di estrema importanza per le aziende, perché aiuta il titolare dei dati a rispettare le norme del nuovo Regolamento e a garantire l'adozione di misure idonee ad attuare le prescrizioni qui contenute.

IL RAGGIO D'AZIONE
Scatta l'obbligo per le aziende che trattano informazioni sensibili su larga scala o di persone vulnerabili

La Dpia deve essere condotta prima di procedere al trattamento e non può essere un documento "statico", ma "dinamico", in continua evoluzione e riesame. Questo comporta la necessità di una rivisitazione della valutazione a intervalli regolari e continuativi.

Ai trattamenti di dati personali già in corso si applica la nuova normativa oppure no? Su questo punto si sono espressi i Garanti della privacy a livello europeo (il cosiddetto gruppo di lavoro «Articolo 29») nelle Linee guida in materia di valutazione di impatto privacy emanate il 4 ottobre 2017, affermando che è necessaria la Dpia anche per i trattamenti già in corso, se c'è stata una variazione dei rischi, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

La Dpia può essere effettuata sia dal titolare dei dati sia da soggetti interni o esterni all'organizzazione. La responsabilità resta comunque al titolare del trattamento. Nello svolgere l'attività di valutazione, il titolare si consulta con il responsabile della protezione dei dati, qualora sia stato nominato (il cosiddetto Dpo, *data protection officer*) e con i responsabili del trattamento.

La valutazione di impatto privacy è obbligatoria? L'articolo 35 del Regolamento Ue 679/2016 afferma che la Dpia è obbligatoria ogni qualvolta il trattamento dei dati comporta rischi elevati per i diritti e le libertà dei soggetti.

Non c'è l'obbligo di redigere il documento, invece, se i trattamenti dei dati personali:

1. non presentano rischi rilevanti per i diritti e le libertà delle persone;
2. sono già stati sottoposti a verifica da parte delle autorità di controllo;
3. sono compresi nell'elenco facoltativo o fanno riferimento a norme o regolamenti per la cui definizione è stata condotta una Dpia.

Come deve essere redatta la Dpia? Il regolamento generale sulla protezione dei dati (articolo 35, paragrafo 7 e considerando 84 e 90) stabilisce che il documento in questione dovrà contenere:

1. la descrizione dei trattamenti previsti e delle relative finalità;
2. la valutazione della necessità e proporzionalità del trattamento;
3. la valutazione dei rischi per i diritti e le libertà delle persone fisiche e le misure previste per la gestione di questi rischi.

L'azienda dovrà inoltre dimostrare la conformità dei trattamenti rispetto al Gdpr.

Non è prevista quindi una metodologia uniforme di redazione del documento. Spetta al titolare scegliere quella che risulta conforme al Regolamento europeo.

Esiste un obbligo di rendere pubblica la Dpia? Secondo le linee guida del 4 ottobre 2017 non c'è un obbligo generale di pubblicazione. La decisione spetterà, dunque, anche in questo caso, ai titolari dei dati. In ogni caso, la pubblicazione della Dpia (anche per stralcio) è consigliata, sia per ragioni di trasparenza e responsabilizzazione, sia perché, rendendo noto il documento, le persone riporranno più fiducia sul corretto trattamento dei loro dati.

LA PAROLA CHIAVE

Data protection officer

È il responsabile della protezione dei dati, una figura obbligatoria, secondo il nuovo Regolamento europeo sulla privacy, in tre casi:
- se il trattamento di dati personali è effettuato da un'autorità o da un organismo pubblici;
- quando le attività principali dell'organizzazione consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- quando le attività principali dell'organizzazione consistono nel trattamento su larga scala di dati sensibili o giudiziari.