

L'identikit dell'iter (Dpia)

CHE COSA È LA «DPIA»

Procedura per prevenire rischi

La valutazione d'impatto sulla protezione dei dati personali (in inglese *data protection impact assesment, Dpia*) è una procedura attraverso la quale l'azienda può valutare i rischi cui sono sottoposti i trattamenti dei dati, per poter mettere a punto tutte le misure necessarie ad attenuare questi rischi

A CHE COSA SERVE

Conformità alle regole Ue

Lo scopo della Dpia è valutare se il trattamento dei dati da parte del titolare è conforme al nuovo Regolamento europeo sulla Privacy, in vigore dal 25 maggio. Vista l'utilità della procedura, il gruppo di lavoro europeo dei Garanti della privacy suggerisce di valutarne l'adozione per tutti i trattamenti dei dati (non solo nei casi in cui il Regolamento ne prevede l'obbligatorietà)

QUANDO FARLA

Pesa la variazione del rischio

La valutazione deve essere eseguita prima di ogni trattamento di dati. Per i trattamenti che siano già in corso, la procedura è necessaria solo se variano i rischi cui sono sottoposti i dati, tenendo conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento

CHI DEVE FARLA

Responsabilità al titolare

La valutazione di impatto privacy ricade sotto la responsabilità del titolare del trattamento dei dati personali, che può farsi aiutare anche da consulenti esterni all'azienda o da organismi esperti di informatica all'interno dell'impresa stessa (ad esempio il responsabile It dell'azienda). La responsabilità della procedura comunque è del titolare

OBBLIGATORIETÀ

Trattamenti da valutare

La Dpia è obbligatoria quando il trattamento può comportare un rischio elevato per i diritti delle persone coinvolte. I garanti della Privacy hanno individuato una serie di situazioni-chiave (trattamento di dati su larga scala, monitoraggio continuo, trattamento di dati sensibili o giudiziari o di natura strettamente personale) in presenza di almeno due delle quali la Dpia è da fare

CONSEGUENZE

Sanzione fino a 10 milioni

La mancata esecuzione della valutazione di impatto privacy nei casi di obbligatorietà o l'errata valutazione possono comportare l'applicazione di una sanzione pari nel massimo a 10 milioni di euro oppure, nel caso dell'impresa, fino al 2% del fatturato globale dell'anno precedente, in base a quale dei due importi sia quello superiore (articolo 83 paragrafo 4 lettera a del Regolamento 679/2016)