LO STUDIO DEL CONSULENTE DEL LAVORO

GDPR - CYBER SICUREZZA - LEGAL

News

CDL

Analisi dei rischi nello studio D.P.I.A.

SINERGIA
RISK MANAGEMENT

2023

Consulenti del lavoro e privacy: analisi dei rischi e DPIA

L'Analisi dei rischi costituisce uno strumento indispensabile per far fronte all'obbligo, di cui all'art. 32 del GDPR, relativo alla sicurezza dei dati personali. Tale analisi ha lo scopo di:

- formalizzare, razionalizzare e finalizzare le proprie strategie in materia di sicurezza;

- definire opportune strategie per l'informazione e la formazione dei soggetti che trattano i dati sotto la propria autorità;

- determinare la necessità di una valutazione d'impatto sui trattamenti e, se del caso, effettuare la valutazione d'impatto stessa.

Un valido supporto per l'esecuzione dell'analisi dei rischi può essere costituito dalle linee guida 2016 dell'Enisa per le PMI, il cui approccio alla valutazione del rischio si basa su quattro fasi:

- definizione dell'operazione di trattamento e del suo contesto;

- comprensione e valutazione dell'impatto;

- definizione di possibili minacce e valutazione della loro probabilità (probabilità di occorrenza della minaccia);

- valutazione del rischio (data dalla combinazione tra la probabilità di accadimento della minaccia e l'impatto).

Qualora i trattamenti possano presentare in generale un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento dovrebbe inoltre svolgere una valutazione d'impatto sulla protezione dei dati (DPIA) per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio, per poi prenderne in considerazione l'esito nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali è conforme a quanto previsto dal GDPR.

Come nel caso della nomina del DPO, la valutazione d'impatto è richiesta in alcuni casi specifici.

Tra quelli che potrebbero riguardare l'attività svolta dal CdL ci sono i trattamenti su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati che mirino al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati.

Anche in questo caso, può in generale considerarsi esclusa la larga scala nel caso un trattamento riguardi dati personali di clienti da parte di un unico professionista. Maggiori approfondimenti sull'applicabilità

del concetto di larga scala al proprio contesto organizzativo sono invece d'obbligo nel caso di svolgimento congiunto dell'attività professionale.

Come noto, l'approccio metodologico proposto dal Regolamento UE 2016/679 (di seguito anche "GDPR") ha rivoluzionato il ruolo dei Titolari del trattamento rendendoli, ancor più, soggetti attivi e propositivi della propria compliance privacy. In particolar modo, tale cambiamento è stato accelerato dal principio di responsabilizzazione (cd. accountability) che ha posto in capo al Titolare del trattamento l'onere di "auto valutarsi" al fine di determinare, in maniera autonoma, come porre in essere i trattamenti di dati personali. Molte delle incertezze riguardano, ad oggi, la Valutazione di Impatto Privacy (di seguito anche "V.I.P."), nuovo adempimento inserito all'art. 35 del GDPR e che è frutto, principalmente, di una valutazione del rischio che rilevi un rischio rilevante.

L'adempimento in cui si esplica maggiormente questo approccio è l'analisi del rischio e la conseguente adozione di misure, sia tecniche che organizzative, adeguate, ovvero calibrate alle attività di trattamento dati concretamente svolte. La novità rispetto alle misure di sicurezza minime dell'All. B del Codice privacy ante-riforma del 2018 è di rilievo. Tuttavia, come si suole dire, "da grandi poteri derivano grandi responsabilità" ed è così che molti Titolari del trattamento si sono trovati spaesati, senza più quel "minimo" punto di riferimento dato dall'All. B del vecchio Codice Privacy.

La V.I.P. è una procedura prevista dall'art. 35 del GDPR attraverso la quale si descrive un trattamento di dati, col fine di valutarne la necessità e la proporzionalità, nonché, i relativi rischi e di approntare le misure idonee ad affrontarli.

La V.I.P. fornisce un approccio sistematico che consente di comprendere, con efficacia, i profili di rischio e le "remediations", permette al Titolare del trattamento di valutare, a priori, l'impatto nella protezione dei dati personali e l'adeguatezza delle misure di sicurezza tecnico/organizzative che, di conseguenza, si possono adottare.

E' uno strumento principe dell'accountability in quanto, da un lato supporta il Titolare nel rispettare le prescrizioni del GDPR, e dall'altro consente di dimostrare la conformità dei trattamenti stessi.

Oggetto della V.I.P. possono essere o un singolo trattamento di dati personali oppure più trattamenti, purché simili tra loro per natura, ambito di applicazione, contesto, finalità e rischi.

L'articolo 35 del GDPR stabilisce che, qualora un trattamento possa 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 di impatto dei trattamenti previsti sulla protezione dei dati personali.

La V.I.P. è richiesta, in particolare, qualora si ricada in una di queste ipotesi:

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'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

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

Si ricorda che, la mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa (articolo 35, paragrafi 1, 3 e 4), l'esecuzione in maniera errata di detta valutazione (articolo 35, paragrafi 2 e da 7 a 9) oppure la mancata consultazione dell'autorità di controllo laddove richiesto (articolo 36, paragrafo 3, lettera e)), possono comportare una sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di EUR oppure, nel caso di un'impresa, pari a fino al 2% del fatturato annuo globale dell'anno precedente, a seconda di quale dei due importi sia quello superiore.