La figura del Data Protection Officer (DPO) in base al GDPR 2016/679

Autore: Dott.ssa Stefania Tonutti - Professionista BLS Compliance
In: Diritto penale

Di cosa si tratta?

Stiamo parlando del Regolamento (UE) 2016/679 (più comunemente noto come GDPR) concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati. Il Regolamento è entrato in vigore il 24 maggio 2016 e diventerà direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018. Nello specifico si tratterà, in sintesi, la figura del Data Protection Officer, alla luce delle ultime Linee Guida emanate dal Gruppo 29.

Il GDPR[1] prevede una figura particolare e molto importante, che si aggiunge a quelle "classiche privatistiche" quali titolare e responsabile del trattamento: quella del Data Protection Officer (DPO). Una persona fisica, una sorta di figura ibrida fra il ruolo di vigilanza dei processi interni alla struttura (del titolare e del responsabile, che lo devono nominare, obbligatoriamente in taluni casi previsti per legge), ed il ruolo di consulenza; funge inoltre da "ponte di contatto" e super partes con l'Autorità Garante nazionale.

Quali sono i requisiti?[2]

Il Responsabile della protezione dei dati, nominato dal titolare o dal responsabile del trattamento, dovrà:

1. possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;

2. adempiere alle sue funzioni in piena indipendenza ed in assenza di conflitti di interesse;

3. operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di

servizio.

Diritto & Diritti ISSN 1127-8579

Il titolare o il responsabile dovranno mettere a disposizione del DPO le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

Quali sono i suoi compiti?[3]

Il DPO dovrà:

a) informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;

c) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;

d) fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;

e) fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

In sintesi, il DPO effettua sia un'attività interna alla struttura del preponente, sia un'attività esterna, in quanto punto di contatto fra la struttura e l'Autorità Garante.

Da un lato le sue competenze sembrerebbero molto ampie (effettuare una valutazione dei rischi; trovare soluzioni giuridiche al problema; conoscere sia il diritto nazionale sia quello comunitario; svolgere verifiche, coordinare i lavori in caso di incidenti/violazioni informatiche, etc.). Dall'altro, invece, non è ben chiara la definizione, anzi, il collocamento, del suo ruolo.

Ecco allora che, visti i dubbi e le incertezze capillarmente diffusi a livello europeo sulle caratteristiche ed i compiti del DPO, il Gruppo dei Garanti Europei (WP 29) ha emanato, lo scorso dicembre, delle Linee Guida in cui viene data un'interpretazione puntuale di quanto elencato negli articoli 37, 38 e 39 del GDPR: in particolare, chiariscono quali dovranno essere i requisiti soggettivi e oggettivi di questa nuova figura

Diritto & Diritti ISSN 1127-8579

professionale.

Casi di nomina obbligatoria del DPO

In base al Regolamento, il DPO dovrebbe essere nominato quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico: il WP29 dà un'interpretazione estensiva di organismo pubblico e raccomanda, come una buona pratica, la nomina del DPO anche da parte delle organizzazioni private che svolgono funzioni pubbliche o che esercitano pubblici poteri. La sua attività dovrebbe coprire tutte le operazioni di trattamento, comprese quelle che non sono legate alla esecuzione di un compito pubblico o esercizio del dovere ufficiale (ad esempio la gestione di un database dei dipendenti).

Ancora, la nomina dovrebbe essere obbligatoria quando le attività principali (cd. core business) del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati. Per "attività core" si intende un'operazione necessaria per raggiungere lo scopo, appunto, del titolare o responsabile.[4] Infine, terzo ed ultimo punto di designazione obbligatoria del DPO: nel caso di trattamento, su larga scala, di speciali categorie di dati personali o di dati relativi a reati e condanne penali. Il concetto di "larga scala" dev'essere valutato sulla base di alcuni specifici criteri: quali, ad esempio, il numero di interessati coinvolti nel trattamento, la durata del trattamento e la sua estensione geografica (tra i trattamenti effettuati su larga scala, in particolare, rientrano la geo-localizzazione, per finalità statistiche, dei clienti di una certa attività, ad esempio catene di ristoranti; il trattamento dei dati bancari dei propri clienti da parte di una compagnia assicurativa; il trattamento, da parte di un motore di ricerca, dei dati personali degli utenti per l'invio di pubblicità mirata). Tra i trattamenti non su larga scala, invece, sono ricompresi: il trattamento dei dati di un proprio paziente da parte del medico di famiglia ed il trattamento dei dati personali di natura penale da parte di un avvocato.

Il DPO, in sostanza, è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa in materia di protezione dei dati e può essere tanto un dipendente del titolare del trattamento o del responsabile del trattamento quanto un libero professionista che opera in forza di un contratto di servizi.

Tuttavia, in merito a questo punto, il Regolamento sottolinea che i suoi compiti e le sue funzioni non

Diritto & Diritti ISSN 1127-8579

devono dar adito a possibili conflitti di interessi. L'assenza del conflitto di interessi è strettamente legata alla necessità di agire in modo indipendente: ciò comporta, in particolare, che il DPO non può mantenere una posizione all'interno dell'organizzazione che lo portino a determinare le finalità e gli strumenti del trattamento dei dati personali. Appare evidente, scrive il WP29, che, a causa della specifica struttura organizzativa in ogni realtà, questo deve essere considerato caso per caso.[5]

Anche se l'art. 37 del Regolamento non specifica le qualità professionali che dovrebbero essere considerate quando si designa un DPO, è chiaro che, come affermato in precedenza, il responsabile della protezione dei dati dovrebbe avere esperienza sulla legislazione relativa alla protezione dei dati personali sia nazionale che europea. Per il WP29 risulta utile che le autorità di controllo promuovano una formazione adeguata e regolare per il DPO.

Indubbiamente è utile anche che il DPO abbia la conoscenza del settore di business delle imprese e dell'organizzazione del titolare e, nel caso di un ente pubblico, dovrebbe anche avere una buona conoscenza delle regole e delle procedure dell'organizzazione amministrativa.

In conclusione: la figura del DPO risulta ancora "nebbiosa" e controversa, soprattutto in Italia, e questo è aggravato anche dal fatto che l'Autorità Garante non si è ancora espressa sul tipo di certificazione a cui dovrebbe fare riferimento per svolgere la sua attività, e sulla tipologia di contratto che dovrebbe stipulare con il titolare ed il responsabile.

Non resta che aspettare ulteriori chiarimenti e, nel frattempo, non farsi trovare impreparati.

Visita la sezione del Portale dedicata alla PRIVACY

[1] Agli articoli 37, 38 e 39;

Diritto & Diritti ISSN 1127-8579

[2] Per i requisiti ed i compiti si veda la scheda riassuntiva proposta dall'Autorità Garante per la Protezione dei Dati Personali (di seguito Garante Privacy o Autorità Garante) al seguente link;

[3] Anche qui come la nota precedente, i compiti descritti sono una sintesi degli articoli 37 e 39 del GDPR;

[4] Nelle Linee Guida si fa riferimento, come esempio, agli ospedali: il core business è sicuramente provvedere alla cura delle persone, e il trattamento dei loro dati è un aspetto imprescindibile

[5] Nelle Linee Guida si suggerisce: «A seconda delle attività, le dimensioni e la struttura dell'organizzazione, può essere buona pratica per responsabili o titolari:

- individuare le posizioni che sarebbero incompatibile con la funzione di DPO
- elaborare un regolamento interno al fine di evitare conflitti di interesse
- includere una spiegazione più generale su conflitti di interesse
- dichiarare che il DPO scelto ha alcun conflitto di interessi per quanto riguarda la sua funzione
- includere nelle norme interne di organizzazione le garanzie ed assicurare che il il contratto di servizio è sufficientemente preciso e dettagliato»

https://www.diritto.it/la-figura-del-data-protection-officer-dpo-in-base-al-gdpr-2016679/

Diritto & Diritti ISSN 1127-8579