lexant
STUDIO LEGALE

FOCUS ON

GDPR: il Data Protection Officer (DPO)

Ruolo e poteri del DPO nel nuovo Reg. UE n. 2016/679 (GDPR)

Regolamento europeo in materia di protezione dei dati personali (GDPR – Reg. UE n. 2016/679): la nuova figura del *data protection officer* (DPO)

Il Regolamento UE 2016/679 (General Data Protection Regulation o GDPR) ha introdotto, con gli articoli 37, 38 e 39, la figura del Data Protection Officer o Responsabile della protezione dei dati personali (in seguito DPO).

Ai sensi della nuova disciplina, la nomina di un DPO assume carattere obbligatorio per i soggetti pubblici e, per i soggetti privati, qualora le attività principali svolte dal Titolare o dal Responsabile del trattamento consistano in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala oppure consistano nel trattamento su larga scala di categorie particolari di dati personali, quali quelli sensibili, genetici, biometrici, i dati relativi a condanne penali e a reati.

Il Gruppo dei Garanti (WP29), in data 13 dicembre 2016, ha approvato e pubblicato tre documenti (aggiornati e rivisitati in data 5 aprile 2017) contenenti indicazioni e raccomandazioni in merito ad alcune delle più rilevanti novità apportate dal GDPR, in vista della sua prossima applicazione da parte degli Stati membri. Le linee guida, alla cui elaborazione ha partecipato anche il Garante italiano, riguardano, oltre agli altri temi, il Responsabile per la protezione dei dati.

Allo scopo di agevolare l'interpretazione della normativa, il Gruppo dei Garanti ha innanzitutto cercato di fornire una definizione degli elementi posti dal Regolamento a fondamento dell'obbligatorietà della designazione del DPO.

Nel definire cosa si debba intendere per attività principali del Titolare o del Responsabile del trattamento, il WP29 precisa, ad esempio, che le stesse ricomprendono il trattamento dei dati personali tutte le volte in cui esso costituisca parte integrante delle attività ordinariamente svolte da tali soggetti.

Il Gruppo di Lavoro non fornisce, invece, una definizione puntuale in merito alla definizione di trattamenti su larga scala limitandosi a suggerire che, con il tempo, concentrandosi su alcune tipologie di trattamento maggiormente comuni, si riuscirà ad individuare degli standard utili in tale senso. Il WP29 ha comunque già indicato alcuni esempi delle soglie di riferimento e alcuni parametri generali cui è opportuno attenersi. Il Gruppo dei Garanti riferisce, infatti, che dovrebbero essere ricompresi nella ipotesi di trattamento su larga scala, il trattamento di dati personali effettuato da banche o compagnie di assicurazione o quello che abbia ad oggetto i dati di viaggio dei soggetti che utilizzano mezzi di trasporto pubblici, il trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food, il trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale ed il trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Al contrario, esempi di trattamento non su larga scala sono individuati nel trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario e nel trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Il WP29 raccomanda, inoltre, di considerare alcuni fattori indicativi, tra cui il numero di soggetti interessati, il volume di dati trattati, la durata delle operazioni di trattamento e l'estensione geografica di queste ultime.

Da ultimo, il monitoraggio regolare e sistematico viene definito come quella forma di monitoraggio effettuata periodicamente o in via continuativa, al cui interno è ricompresa, ad esempio, la profilazione online o il data-driven

marketing ossia quelle attività di marketing che utilizzano i dati degli interessati al fine di comprendere meglio le loro preferenze ed esigenze così da poter in seguito offrire servizi personalizzati.

Occorre rilevare che, a prescindere dai casi in cui la nomina di un DPO sia obbligatoria, tale designazione è comunque considerata dai Garanti una buona prassi e come tale viene incoraggiata anche per le aziende che ne sarebbero esenti.

Si precisa, altresì, che il Gruppo dei Garanti raccomanda, nell'ottica dell'adeguamento al principio dell'accountability (o responsabilizzazione) introdotto dal Regolamento, di documentare per iscritto le motivazioni che hanno portato alla scelta di nominare un DPO o di non provvedervi così da porsi nelle condizioni di poter eventualmente dimostrare (ove dovesse verificarsi una ispezione) di aver preso in considerazione i fattori di maggiore rilievo e delicatezza.

Il WP29 si è chiesto se il DPO sia responsabile in prima persona dell'implementazione della privacy in azienda (coincidendo quindi con il Privacy Officer o il Compliance Manager) o se sia invece una figura di controllo (necessariamente distinta dalle precedenti, per evitare di controllare sé stesso) ed ha infine preso posizione a favore della seconda ipotesi. Già nell'introduzione si legge, infatti, "i DPO non sono personalmente responsabili in caso di mancato rispetto del GDPR. Il GDPR rende chiaro che è il Titolare o il Responsabile che è tenuto a garantire ed essere in grado di dimostrare che il trattamento viene eseguito in conformità con le sue disposizioni".

Con riferimento alle mansioni, è opportuno precisare che al DPO sono affidate, contestualmente, attività di consulenza e controllo, la verifica dell'applicazione del GDPR, della disciplina nazionale e delle policy interne, il compito di informare e consigliare il Titolare del trattamento, interloquire con le Autorità di controllo e con gli interessati, aiutare il Titolare nell'implementazione di attività quali il registrare le attività di trattamento, garantire la sicurezza del trattamento e notifica e comunicare eventuali data breach.

Un posto di rilievo viene inoltre assegnato anche alla confidentiality (ai sensi dell'art. 38 punto 5 GDPR) secondo cui il DPO è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti. La riserbatezza è difatti necessaria e indispensabile per il corretto e fisiologico espletamento delle funzioni del DPO dal momento che il suo venir meno comporterebbe una mancanza di fiducia da parte dei lavoratori che potrebbero così non comunicare con il DPO.

Il Garante della Privacy ha, peraltro, precisato che, considerata l'importanza del suo ruolo, la scelta di tale figura dovrà essere effettuata con particolare attenzione, verificando il possesso di competenze ed esperienze specifiche e multidisciplinari e non ci si potrà limitare a designare un qualsiasi dipendente già impiegato all'interno dell'azienda. Nell'ipotesi in cui, dopo aver compiuto una puntuale valutazione, alcuna delle figure presenti all'interno della singola struttura possieda le necessarie qualità sarà, infatti, possibile e consigliabile avvalersi di soggetti esterni.

I requisiti fondamentali del Data Protection Officer possono, in sintesi, indicarsi nella conoscenza della normativa e delle best practices esistenti in materia di protezione dei dati, nella conoscenza specialistica del settore in cui opera l'organizzazione, nella autorevolezza e nell'indipendenza.

In particolare, uno degli elementi cardine della nuova figura del DPO si individua proprio nella necessità che il medesimo rivesta una posizione di indipendenza e autonomia. Ciò significa che, nel caso di nomina interna, la persona individuata quale DPO non dovrà rivestire un ruolo che gli consenta di determinare finalità e modalità del trattamento. Pertanto, non sarà possibile, ad esempio, nominare quale DPO l'IT manager dell'azienda, in quanto i relativi compiti sono verosimilmente incompatibili con quelli propri del DPO, che finirebbe in pratica per controllare sé stesso, verificando se le

proprie attività di IT manager siano conformi alla normativa in materia di data protection. Parimenti, potrebbero sussistere situazioni di conflitto all'interno dell'organizzazione del Titolare o del Responsabile per chi ricopre ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane) ma anche per chi ricopre posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento.

Nella scelta tra designare un dipendente già impiegato all'interno dell'azienda e delegare ad un fornitore esterno specializzato (con la precisazione che dovrà in ogni caso trattarsi di una persona fisica, supportata, laddove necessario, da un team ma non potrà essere una persona giuridica) è opportuno valutare la dimensione dell'organizzazione, l'esistenza delle competenze richieste all'interno, la tipologia di dati trattati e di trattamenti e così via.

Infine può essere utile ricordare che il paragrafo 3 dell'art. 38 del GDPR stabilisce che il Titolare del trattamento e il Responsabile del trattamento si assicurino che il Responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti, che il DPO non possa essere rimosso o penalizzato dal Titolare del trattamento o dal Responsabile del trattamento per l'adempimento dei propri compiti e che debba riferire direttamente al vertice gerarchico del Titolare del trattamento o del Responsabile del trattamento.

Avv. Simona Cardillo