Privacy: i tre volti del Data Protection Officer

Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Una delle novità più rilevanti del GDPR è rappresentata dalla figura del Responsabile della Protezione dei Dati (RPD), ossia il Data Protection Officer. Il DPO ha il compito di sorvegliare l'osservanza del GDPR, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità. Il DPO, inoltre, deve essere in grado di adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. Forte l'impatto sul sistema organizzativo delle realtà aziendali dove tale figura si presenta con un profilo a tre volti: quali?

Il **GDPR** offre un quadro di riferimento in termini di **compliance per la protezione dei dati** in Europa aggiornato e fondato sul principio di responsabilizzazione (accountability). I Responsabili della Protezione dei Dati (RPD), altrimenti noti come **Data Protection Officer** (DPO), si trovano esattamente al centro di questo nuovo quadro giuridico e sono chiamati a facilitare l'osservanza delle disposizioni.

Chi è tenuto a designare un DPO

Secondo il GDPR, alcuni titolari e responsabili del trattamento sono tenuti a nominare un DPO. In base all'Articolo 37, paragrafo 1, del GDPR, questo vale, in particolare:

- per tutte le **amministrazioni** e gli enti pubblici, indipendentemente dai dati oggetto di trattamento (fatta eccezione per le autorità giudiziarie)

- per quei soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono un **monitoraggio regolare e sistematico degli interessati** su larga scala

- per tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di **dati sensibili**, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche ove il Regolamento non imponga in modo specifico la designazione di un DPO, può risultare utile procedere alla **nomina su base volontaria**. In tal caso, troveranno applicazione tutti i requisiti di cui agli Articoli 37-39 per quanto concerne la nomina stessa, lo status e i compiti del DPO.

L'Articolo 37 non distingue fra titolari del trattamento e responsabili del trattamento in termini di applicabilità: a seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare del trattamento, ovvero il solo responsabile del trattamento, oppure sia l'uno sia l'altro, a dover nominare un DPO. Questi ultimi saranno poi tenuti alla reciproca collaborazione.

Il Paragrafo 2 consente a un **gruppo imprenditoriale** di nominare un unico DPO a condizione che quest'ultimo sia "facilmente raggiungibile da ciascuno stabilimento".

Il concetto di raggiungibilità si riferisce ai compiti del DPO in quanto punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente. Infatti, il DPO, se necessario con il supporto di un team di collaboratori, deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo coinvolte. Ciò

significa che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa.

Analogamente, ai sensi dell'Articolo 37, Paragrafo 3, è ammessa la **designazione di un unico DPO** per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

Per garantire l'accessibilità del DPO (soprattutto da parte di chi deve esercitare i suoi diritti) è raccomandata la sua collocazione **nel territorio dell'Unione Europea**, indipendentemente dall'esistenza di uno stabilimento del titolare o del responsabile in tale sede. Tuttavia, non si può escludere che, in alcuni specifici casi, un DPO sia in grado di adempiere ai propri compiti con maggiore efficacia operando al di fuori dell'UE.

La figura del DPO ...

In base all'Articolo 37, Paragrafo 5, il DPO "è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'Articolo 39".

Il livello di **conoscenza specialistica** richiesto non trova una definizione tassativa; piuttosto, deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento. Inoltre, non sono specificate le qualità professionali da prendere in considerazione nella nomina di un DPO. Tuttavia, sono pertinenti, al riguardo, la conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, anche in termini di misure tecniche e organizzative, nonché un'approfondita conoscenza del GDPR.

Non sono richieste **attestazioni formali** o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio o professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.

Per "capacità di assolvere i propri compiti", poi, si deve intendere sia tutto ciò che è legato alle qualità personali e alle conoscenze del DPO, sia ciò che dipende dalla posizione del DPO all'interno dell'azienda o dell'organismo.

Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici.

Il DPO, inoltre, deve essere in grado di adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che non può trattarsi di un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali.

Il DPO dovrà operare alle dipendenze del titolare o del responsabile del trattamento dati, oppure sulla base di un **contratto di servizio**.

In quest'ultimo caso, il DPO sarà esterno e le sue funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica.

… e i compiti

I compiti stabiliti per il DPO potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale "responsabile" per il singolo cliente. In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale DPO soddisfi tutti i requisiti fissati nel GDPR. Per favorire efficienza e correttezza, e prevenire **conflitti di interesse** a carico dei componenti del team, è opportuno procedere ad una chiara ripartizione dei compiti e prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente.

L'Articolo 39, Paragrafo 1, lettera b), affida al DPO, fra gli altri, il compito di **sorvegliare l'osservanza del GDPR**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità. Il titolare del trattamento (o il responsabile del trattamento), infatti, dovrebbe essere assistito dal DPO nel controllo del

rispetto a livello interno del regolamento.

Fanno parte di questi compiti di controllo svolti dal DPO, in particolare, la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità e l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

In secondo luogo, il DPO svolge un ruolo di primo piano nella collaborazione con il titolare del trattamento per quanto riguarda la conduzione di una valutazione di impatto sulla protezione dei dati (DPIA).

L'Articolo 35, Paragrafo 2, prevede in modo specifico che il titolare si consulti con il DPO quando svolge una DPIA. A sua volta, l'Articolo 39, Paragrafo 1, lettera c) affida al DPO il compito di "fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'Articolo 35".

In particolare, la consultazione dovrebbe avvenire sulle seguenti tematiche:

1) se condurre o meno una DPIA

2) quale metodologia adottare nel condurre una DPIA

3) se condurre la DPIA con le risorse interne ovvero esternalizzandola

4) quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate

5) se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte siano conformi al GDPR.

Con riferimento al ruolo di "**facilitatore" attribuito al DPO**, ricordiamo inoltre che egli deve fungere da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti attribuiti.

Deve, inoltre, informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e dalle altre disposizioni dettate in materia.

Infine, il DPO è chiamato a supportare il titolare/responsabile in ogni attività connessa al trattamento dei dati personali, inclusa quella relativa alla realizzazione di un registro contenente tutte le attività di trattamento svolte.

Considerazioni finali

Il DPO è una figura completamente nuova che ha un forte impatto anche sul sistema organizzativo di una realtà. Già il fatto che debba essere un soggetto che non sia in posizione di conflitto di interessi, libero e non "istruito", lo rende un elemento molto particolare all'interno di un'azienda o di un ente.

Si presenta, poi, come un profilo a tre volti. Un volto è diretto verso i **vertici dell'azienda**, in quanto il DPO diventa il consulente del titolare. Un secondo volto è verso il Garante, perché il DPO è non solo il punto di contatto con cui dialoga l'autorità di controllo in caso di bisogno ma anche un **presidio del sistema normativo** dentro l'attività di trattamento dei dati affinché sia garantita la corretta applicazione del Regolamento. Infine, un terzo volto è orientato **verso gli interessati**, che possono esercitare i loro diritti dialogando con il DPO. Una funzione "una e trina" che, nella pratica, riserverà non poche sorprese.

Il nuovo regolamento UE sulla privacy GDPR entra in vigore dal 25 maggio 2018.