Ettore BATTELLI Guido D'IPPOLITO

COMPENDIO della PRIVACY e della CYBERSICUREZZA

II Edizione
2025

Neldiritto Editore

Capitolo X
Il Data Protection Officer (DPO): il Responsabile per la Protezione dei Dati

SOMMARIO:

1. La figura del Data Protection Officer (DPO) e la normativa di riferimento

Il sistema introdotto dal RGPD fa perno sulla **prevenzione del rischio di violazione di dati personali e dei (connessi) diritti e libertà fondamentali della persona**.
Il RGPD assegna un ruolo di rilievo al **Responsabile per la Protezione dei Dati** (**RPD**), spesso indicato con la dizione inglese di ***Data Protection Officer*** (**DPO**), per quanto attiene al profilo della sicurezza dei dati, considerato dal legislatore europeo elemento chiave all'interno del nuovo sistema di *data governance* e che rappresenta un elemento fondante del principio di *accountability*.
La grande rilevanza del Regolamento non si rinviene, allora, solamente nei puntuali adempimenti prescritti dalla normativa, ma in quel **cambio di prospettiva**, per cui si passa da una disciplina generale incentrata sui **diritti dell'interessato** ad una basata sui **doveri del titolare e del responsabile del trattamento**.
Il RGPD ha attribuito ai soggetti attivi del trattamento compiti e obiettivi generali (quali la progettazione, l'attuazione e il controllo del trattamento) e, al contempo, la capacità (e l'onere) di dimostrare che il trattamento attuato è conforme alle norme (art. 5, co. 2 e 25 RGPD), **procedimentalizzando le attività** in capo a detti soggetti, **secondo un principio generale di responsabilità** (art. 24 RGPD: l'"*accountability*").
Tale impostazione consente a ciascun ente (impresa o pubblica amministrazione) di adottare misure concrete per «attuare i principi di protezione dei dati» (art. 25 – *Data protection by design* e *by default*) e «garantire un livello di sicurezza adeguato al rischio» (art. 32 – *Sicurezza del trattamento*), in modo da offrire una protezione che sia reale ed effettiva.
L'analisi deve allora partire dai principi di *accountability* e di **responsabilizzazione**, i quali congiuntamente intesi richiamano l'opportunità di creare un clima di fiducia

tra interessati e titolari del trattamento al fine di favorire realmente uno sviluppo dell'economia digitale.
Tale clima di **fiducia**, al quale interessato e titolare devono tendere nel trattamento dei dati personali, deve altresì trovar sostegno nel principio potenzialmente confliggente della trasparenza.
In questo scenario si colloca il "*Data Protection Officer*" il quale si pone quale figura strategica, fondamentale per la corretta gestione delle *privacy policy*, a garanzia di un miglioramento dell'organizzazione interna e di un adeguato livello di tutela dei cittadini.
Il DPO rappresenta un simbolo di cambiamento radicale nel modo di intendere la protezione dei dati personali.
Attraverso il d.lgs. del 10 agosto 2018, n. 101, sono state introdotte nell'ordinamento italiano, tra le «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679», anche le specifiche di riferimento che disciplinano il DPO quale **figura interna o esterna al contesto delle pubbliche amministrazioni e delle imprese**.
Il DPO è chiamato a svolgere il suo ruolo quale "Responsabile per la protezione dei dati" non solo presso tutti gli enti protagonisti nella Pubblica Amministrazione (Comuni, Regioni, Autorità di controllo, ecc.) ma anche presso soggetti privati che esercitano funzioni pubbliche (come, ad esempio, concessionari di servizi pubblici).
Il DPO è chiamato ad assicurare un **«monitoraggio regolare e sistematico».**
Ebbene, si considera "**regolare**" un monitoraggio che avviene in maniera continua o a intervalli periodici e costanti nel tempo, mentre risulta essere "**sistematico**" quando l'attività di trattamento avviene in una logica di sistema, in maniera predeterminata ed organizzata anche in un progetto complessivo di raccolta dati.
Il DPO rappresenta un vero e proprio **strumento di *accountability***, adottabile, obbligatoriamente o volontariamente, a seconda dei casi, da ciascun Ente, pubblico o privato, nel contesto delle azioni volte ad attenuare il rischio di violazione dei dati personali e dei diritti delle persone fisiche.
La **designazione del DPO** per le pubbliche amministrazioni e per le aziende private (nei casi in cui ciò sia obbligatorio) viene a rappresentare la **prima operazione necessaria per una *compliance* alla normativa europea in materia di protezione dei dati personali**.
La designazione del DPO è onere sia del titolare che del responsabile a seconda del soggetto che soddisfi i criteri relativi alla nomina ed è resa **obbligatoria** dall'art. 37 par. 1, lett. *a*, del Regolamento per ogni «**autorità pubblica ed organismo pubblico**» **–** ad esclusione delle autorità giurisdizionali **–** e per ogni **impresa privata** le cui attività principali consistano in «trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala» (art. 37 par. 1, lett. *b*), RGPD) o riguardino trattamenti «su larga scala» di categorie particolari di dati o dati giudiziari (art. 37 par. 1, lett. *c*), RGPD).
Circa la nozione di «**autorità pubblica ed organismo pubblico**» cui si riferisce la lett. *a*) dell'art. 37 del Regolamento, sono da ritenere tali le persone giuridiche così

inquadrate dal diritto interno. Non vengono specificate le dimensioni dell'organismo destinatario dell'obbligo e può essere designato anche un unico DPO per più organismi pubblici tenuto conto della loro struttura organizzativa e dimensione.
In merito ai soggetti privati tenuti alla nomina del DPO sono da prendere in considerazione le tipologie di attività intraprese dal titolare, laddove, ai sensi del considerando 97 RGPD, saranno da ritenersi **"principali"** le sole attività **"primarie"** e non anche quelle **accessorie** di trattamento dei dati personali.
Queste, poi, devono configurarsi quali trattamenti di dati comuni consistenti nel monitoraggio regolare e sistematico degli interessati, oppure come trattamenti di dati effettuati "**su larga scala"**.
Circa il concetto di **larga scala** del trattamento di **categorie particolari di dati** o **dati giudiziari**, il considerando 91 RGPD chiarisce che esso vada riferito alle attività «che mirano 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 e che potenzialmente presentano un rischio elevato».

APPROFONDIMENTO

La Proposta di Regolamento conteneva una previsione secondo la quale l'obbligo di nomina sarebbe stato da imporre alle aziende con più di 250 dipendenti, ma fu rilevato come quello della dimensione della struttura non fosse un criterio adatto a stabilire l'effettiva necessità di un "*professionista della privacy*", in quanto organizzazioni con meno di 250 dipendenti che trattassero ingenti quantità di dati o compissero trattamenti altamente rischiosi, avrebbero potuto necessitare di un DPO ancor più di una grande impresa le cui attività di trattamento fossero del tutto marginali.

Dunque, i titolari che effettuino trattamenti di tale portata su **categorie particolari di dati** (art. 9) o **dati giudiziari** (art. 10), oppure attraverso meccanismi qualificabili come «monitoraggio regolare e sistematico», saranno soggetti all'obbligo *ex* art. 37, par. 1, del Regolamento di nominare un DPO mentre, al di fuori di tali ipotesi, la nomina resta una facoltà riconosciuta ai soggetti attivi del trattamento che, se esercitata, ne dimostra in concreto l'*accountability*.

Caso pratico
Si pensi ad una struttura sanitaria.
L'attività principale di un ospedale è rappresentata dall'assistenza sanitaria da erogare ai cittadini attraverso il trattamento dei dati idonei a rivelare lo stato di salute dei pazienti.
Il personale medico, infermieristico e gli altri operatori sanitari, nell'espletamento delle proprie funzioni istituzionali, proprio ai fini di un diligente svolgimento della loro opera sono autorizzati ad accedere e consultare la cartella clinica e/o il dossier sanitario elettronico dei pazienti, dovendo conoscere ogni informazione utile, compresi quindi dati c.d. "*super sensibili*", proprio al fine di rendere all'assistito una diagnosi seria e completa.

Nessun dubbio, allora, che proprio per la delicatezza dell'attività di trattamento dei dati sanitari, la rilevanza del rischio e il trattamento su "larga scala", l'individuazione di un DPO sia obbligatoria.

L'art. 2-*sexiesdecies* del Codice privacy, inserito dal d.lgs. n. 101/2018, ha esteso l'obbligatorietà della nomina del DPO anche «ai trattamenti di dati personali effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni», ipotesi espressamente esclusa dal novero delle circostanze obbligatorie dell'art. 37 par.1, lett. *a*, del Regolamento.

2. La formazione del DPO e i requisiti per la nomina o designazione

Affinché le misure adottate risultino efficaci è necessario che esse vengano individuate da ciascun Ente autonomamente, in rapporto alle peculiarità del caso specifico, ponendo attenzione particolare al rischio inerente alla natura e al trattamento dei dati da proteggere.
A questo fine, il DPO deve essere considerato come un *manager* del cambiamento digitale e deve possedere **conoscenze multidisciplinari** per poter garantire in piena autonomia l'assistenza necessaria ai titolari e ai responsabili del trattamento nella costruzione di adeguati modelli organizzativi sia di *data protection by design* sia di *data protection by default*.
Al DPO, infatti, è attribuito il compito di assistere il titolare/responsabile del trattamento «nel controllo del rispetto del […] regolamento» (considerando 97 RGPD) svolgendo la propria funzione ("mista" di consulenza, vigilanza e controllo) in assoluta **autonomia e indipendenza** (art. 38, par. 3 e 6, RGPD), quale terzo rispetto al titolare o responsabile del trattamento che lo designa.
In ragione della complessità del ruolo e delle funzioni attribuitegli, il DPO dovrebbe: (a) essere un **professionista esperto, dotato di competenze multidisciplinari e specialistiche** in materia di protezione dei dati personali, con particolare riferimento alla conoscenza della normativa e delle prassi specifiche (art. 37, par. 5, RGPD); (b) possedere essenziali **requisiti di indipendenza** (considerando 97) e, a questo fine, nel contesto dell'ente designante, deve **essere collocato in una posizione tale da riferire al più alto livello gerarchico** (art. 38, par. 3, RGPD) e (c) da **non dare adito a un conflitto di interessi** (art. 38, par. 6, RGPD).
Con riferimento specifico alle (a) capacità e alle competenze del DPO, l'art. 37, par. 5, RGPD specifica che la sua designazione avviene «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'art. 39» e il considerando 97 prevede che l'adeguato livello di conoscenza della normativa sul corretto trattamento dei dati personali dovrebbe essere determinato in base ai tipi di trattamenti effettuati dal titolare o dal responsabile e alla protezione richiesta per i dati personali che ne sono oggetto.
Nella sostanza, quindi, l'art. 37, par. 5 del RGPD non specifica in maniera inequivocabile quali requisiti debba possedere il DPO, limitandosi ad affermare che