# Il DPO: stato dell'arte e considerazioni operative nel contesto normativo italiano

30 April 2024

**AUTORE**

Aurora Agostini
Partner

lexia.it

## Introduzione

Il *Data Protection Officer (DPO)*, noto in Italia anche come Responsabile della Protezione dei Dati (RPD), è una figura professionale istituita dal Regolamento Generale sulla Protezione dei Dati (GDPR, Regolamento UE 2016/679), precisamente all'Articolo 37. Questo ruolo è cruciale per garantire che le organizzazioni trattino i dati personali rispettando i diritti e le libertà fondamentali degli individui: il DPO ha il compito di supervisionare la strategia e l'attuazione delle pratiche di protezione dei dati all'interno di un'azienda, assicurando che queste siano conformi alle normative del GDPR.

## Chi deve nominare un DPO?

L'obbligo di nominare un DPO è specificato per determinate tipologie di enti, come indicato dall'Articolo 37, paragrafi 1, lettere b) e c) del GDPR. Questo include organizzazioni il cui *core business* implica trattamenti di dati che necessitano di un monitoraggio regolare e sistematico degli interessati su larga scala, o il trattamento su larga scala di categorie particolari di dati personali. Gli stati membri dell'UE possono imporre ulteriori requisiti per la designazione di un DPO, ed è in questo senso che il Garante per la Protezione dei Dati Personali italiano fornisce attraverso le sue FAQ ulteriori chiarimenti sull'obbligo di designare un DPO.

Le FAQ del Garante sottolineano che il DPO deve essere coinvolto in tutte le questioni relative alla protezione dei dati personali, a prescindere dal fatto che il trattamento sia effettuato dal titolare o dal responsabile del trattamento;

inoltre, chiariscono che il DPO dovrebbe avere un'adeguata conoscenza della normativa e delle pratiche di protezione dei dati, comprensiva delle operazioni di trattamento svolte dall'ente e delle misure di sicurezza implementate.

Il Garante mette in evidenza che, oltre ai casi espressamente menzionati dal GDPR, altri scenari possono richiedere la designazione di un DPO, tra cui:

- Concessionari di servizi pubblici (es. trasporto, gestione acqua, raccolta rifiuti)
- Istituti di credito e imprese assicurative
- Società di informazione creditizia e finanziarie
- Società di revisione contabile e di recupero crediti
- Istituti di vigilanza, partiti politici, sindacati
- Operatori nel settore delle utilities e delle telecomunicazioni
- Società nel campo della sanità e della prevenzione/diagnostica
- Call center e fornitori di servizi IT e televisivi a pagamento

## Caratteristiche professionali

Il ruolo del DPO, oltre a garantire il rispetto del GDPR, richiede una combinazione di competenze giuridiche, tecniche e di comunicazione che lo rendono un pilastro fondamentale all'interno delle organizzazioni. Secondo le FAQ del Garante per la Protezione dei Dati Personali italiano, il DPO deve possedere una conoscenza approfondita delle leggi sulla protezione dei dati applicabili e delle prassi operative, sia a livello nazionale che europeo. Deve essere in grado di interpretare e applicare la normativa in vari contesti aziendali, che possono includere settori altamente regolamentati come la sanità, il settore finanziario o i servizi pubblici.

Essendo spesso chiamato a lavorare a stretto contatto con gli uffici IT per assicurare che le misure tecniche e organizzative adottate per la protezione dei dati siano appropriate, il DPO necessita anche di solidi fondamenti in ambito tecnologico. Questo può includere la comprensione di sistemi di crittografia, sicurezza delle reti e software di gestione dati.

Un'altra competenza fondamentale è la capacità di comunicazione efficace. Il DPO deve saper spiegare complessi requisiti legali e tecnici a diverse parti interessate, che possono variare da membri del consiglio di amministrazione a dipendenti tecnici, in modo chiaro e comprensibile. È altresì incaricato di promuovere una cultura della protezione dei dati all'interno dell'organizzazione, fungendo da punto di riferimento per i dipendenti su questioni relative alla *privacy* e protezione dei dati.

Infine, l'indipendenza è un requisito chiave per questa posizione: il DPO deve agire senza ricevere istruzioni dirette da altri dipartimenti, garantendo una supervisione imparziale e obiettiva delle pratiche relative al trattamento dei dati. Questa autonomia, come sottolineato nelle FAQ, è essenziale per

mantenere la fiducia di tutte le parti interessate e per garantire una governance dei dati trasparente e responsabile.

## Sanzioni per la mancata designazione del DPO

La mancata designazione di un DPO, nei casi in cui è obbligatoria, può esporre l'ente a sanzioni significative. L'Articolo 83, paragrafo 4 del GDPR prevede che le sanzioni possono arrivare fino a 10 milioni di euro o al 2% del fatturato annuale totale dell'esercizio finanziario precedente, a seconda di quale importo sia maggiore.

Inoltre, se un'analisi preliminare mostra che la nomina di un DPO non è necessaria, è comunque importante documentare accuratamente le motivazioni di questa decisione per dimostrare la conformità con il GDPR in caso di eventuali ispezioni o audit.

## La valutazione della necessità del DPO

In conclusione, la designazione di un DPO non è solo una disposizione normativa, ma una misura prudente per affrontare con consapevolezza le complessità della protezione dei dati personali. La decisione di nominare o meno un DPO non dovrebbe essere presa alla leggera, né essere vista come un mero adempimento burocratico: ogni organizzazione dovrebbe valutare attentamente le proprie operazioni di trattamento dei dati, considerare i rischi potenziali per la privacy degli interessati e ponderare l'eventualità di nomina di un DPO come un'opportunità per rafforzare la fiducia e la trasparenza con i propri utenti e clienti.

Nonostante il GDPR definisca chiaramente gli scenari in cui la designazione di un DPO è obbligatoria, vi sono molte situazioni borderline in cui una valutazione approfondita diventa cruciale. In questi casi, non solo si dovrebbe esaminare la scala e la natura dei dati trattati, ma anche la frequenza e la complessità delle attività di trattamento. La scelta di dotarsi di un DPO può diventare un vantaggio competitivo, evidenziando l'impegno dell'ente nella salvaguardia dei diritti degli interessati.

L'assenza di un DPO può non solo portare a sanzioni significative ma può anche riflettere una mancanza di governance interna sul trattamento dei dati, che oggi rappresenta sempre più un aspetto critico della strategia aziendale. Il DPO, quindi, non è semplicemente una figura di conformità, ma un vero e proprio consulente strategico che guida l'ente nella gestione oculata dei dati, nella mitigazione dei rischi e nell'instaurare una cultura del rispetto della privacy che permea ogni livello organizzativo.

In ultima analisi, la presenza di un DPO può essere vista come un simbolo di eccellenza e di serietà nell'approccio alla protezione dei dati personali, rassicurando tutte le parti interessate che i dati sono trattati con la massima cura e attenzione. Quindi, è fondamentale per le organizzazioni valutare non solo la necessità legale ma anche il valore aggiunto che un DPO può portare nel lungo termine.

## LEXIA'S DATA & TECHNOLOGY INNOVATION TEAM


**Aurora Agostini**
Partner

**Giulietta Minucci**
Counsel

**Jessica Giussani**
Associate

**Giorgia Rastrelli**
Associate