

## Il Data Protection Officer (DPO)

### | Chi è il DPO |

Il **Data Protection Officer (DPO)** è una **figura introdotta** dal **Regolamento generale sulla protezione dei dati 2016/679 | GDPR**, pubblicato sulla Gazzetta Ufficiale Europea L. 119 il 4 maggio 2016.

Il DPO (figura storicamente già presente in alcune legislazioni europee) è una professionalità con un **ruolo aziendale** con **competenze giuridiche, informatiche, di risk management** e di **analisi dei processi**. Può essere sia interno che esterno all'azienda: in ogni caso deve godere di autonomia decisionale e quindi non essere sottoposto a pressioni da parte dell'azienda. Il suo compito è quello di osservare, **valutare** e **organizzare** la **gestione del trattamento di dati personali** (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati **nel rispetto delle normative sulla privacy** comunitarie e nazionali.

Questo soggetto è già conosciuto nel mondo anglosassone con il termine di Chief Privacy Officer (CPO), Privacy Officer, Data Protection Officer o Data Security Officer. In Italia assume il nome di Responsabile Protezione dei Dati (RPD).

## | Cosa fa il DPO |

*Il DPO ha un **ruolo consultivo**. È una figura che va ad affiancare il Titolare/Responsabile nella gestione delle problematiche relative al trattamento dei dati personali. In tal modo si garantisce che un soggetto qualificato si occupi della materia della protezione dei dati personali, aggiornandosi sui rischi e le misure di sicurezza, in considerazione della crescente importanza e complessità del settore.*

L'art. 39 del Regolamento Europeo sulla Protezione dei Dati Personali elenca i principali compiti del DPO (Data Protection Officer):

- 1. Informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento** in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- 2. Sorvegliare l'osservanza del Regolamento**, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati **nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento** in materia di protezione dei dati personali, **compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale** che partecipa ai trattamenti e alle connesse attività di controllo;
- 3. Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;**
- 4. Cooperare con l'autorità di controllo;**
- 5. Fungere da punto di contatto per l'autorità di controllo** per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il Responsabile della Protezione dei Dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

## | Quali realtà possono nominare il DPO |

Il **DPO** è **designato** (art. 37) dal Titolare o dal Responsabile del trattamento, in base ad un **contratto**. Tale **designazione** dovrà essere **comunicata** all'**Autorità** di controllo nazionale.

Devono **nominare obbligatoriamente** un DPO tutte le pubbliche amministrazioni ed enti pubblici, eccetto le autorità giudiziarie. L'obbligo riguarda anche tutti i soggetti (**enti e imprese**) che nelle loro **attività principali trattano su larga scala**:

**1. Dati sensibili:** le **attività** principali del **Titolare** del trattamento o del **Responsabile** del trattamento consistono nel **trattamento**, su larga scala, di **categorie particolari di dati personali** di cui all'articolo 9 (dati particolari, sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10.

L'articolo 9 del Regolamento al comma 1 definisce quelle che sono le categorie particolari di dati personali (ex **dati sensibili**): "che rivelino l'**origine razziale** o **etnica**, le **opinioni politiche**, le **convinzioni religiose** o **filosofiche**, o l'**appartenenza sindacale**, nonché trattare **dati genetici**, dati **biometrici** intesi a identificare in modo univoco una persona fisica, dati relativi alla **salute** o alla **vita sessuale** o all'**orientamento sessuale** della persona".

**2.** Le **attività** principali 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 **su larga scala** (*in base a numero interessati coinvolti, quantità dati trattati, diverse tipologie dati trattati, durata trattamento, portata geografica trattamento*).

Le imprese, che non ricadono invece nell'obbligo di legge, possono comunque decidere di dotarsi ugualmente di un Data Protection Officer.

## | **Obblighi del titolare o responsabile verso il DPO** |

Vi sono numerosi obblighi che il Titolare (o il Responsabile) ha verso il Responsabile per la Protezione dei Dati (se nominato):

- 1. Supportare il DPO** nell'esecuzione dei suoi compiti;
- 2. Fornire le risorse necessarie** per l'esecuzione dei suoi compiti;
- 3. Consentire l'accesso ai dati e alle operazioni di trattamento;**
- 4. Assicurare l'accesso del DPO ai massimi livelli manageriali dell'azienda;**
- 5. Assicurarsi** che gli altri compiti del DPO non interferiscano con la sua responsabilità primaria quale DPO;
- 6. Non fornire alcuna istruzione al DPO sui suoi compiti;**
- 7. Non penalizzare o licenziare il DPO per l'esecuzione dei suoi compiti.**

## | Il Dpo in Microdata |

Il **Garante italiano** ha **precisato** che **non esiste** alcun obbligo di nominare quale DPO dei soggetti che abbiano attestati o con partecipazione a corsi di formazione, né esiste **alcun albo professionale**, quanto piuttosto necessita l'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Secondo l'**autorità italiana** di controllo è opportuno **privilegiare soggetti** che dimostrino **qualità professionali adeguate** alla complessità del compito da svolgere, casomai con esperienze di master o corsi di studio.

Come si può notare, è raro che una **azienda** di piccole o medie dimensioni abbia l'obbligo di **nominare un DPO**, ma è anche vero che oggi esistono aziende di piccole dimensioni che comunque **trattano grandissime quantità di dati**, grazie a strumenti informatici. Gli esempi possono essere parecchi, come un call center, oppure un centro commerciale che ha un impianto di videosorveglianza.

**Microdata**, pur non ricadendo nell'obbligo di nomina di un DPO, **ha scelto di dotarsi di questa figura** in modo da garantire una tutela sempre maggiore dei dati in quanto Responsabile del trattamento nelle lavorazioni svolte per i propri clienti.

**Microdata ha scelto come proprio DPO Partners4Innovation: P4I** - Partners4Innovation è la società del **Gruppo Digital360** che offre servizi di Advisory e Coaching a supporto dell'Innovazione Digitale e Imprenditoriale ad imprese e Pubbliche Amministrazioni.



Per informazioni e contatti consultare la privacy policy di Microdata riportata sul sito [www.microdatagroup.it](http://www.microdatagroup.it)

## | Il valore aggiunto del DPO esterno |

Il **ruolo** può essere **affidato**, secondo la normativa europea, a un **dipendente dell'azienda** o a un **professionista esterno**, che può essere una **persona fisica** o un'**organizzazione**. Può anche essere nominato un **unico DPO** per un **intero gruppo di imprese**.

Il GDPR stabilisce che il Titolare e il Responsabile del trattamento debbano assicurarsi che il **DPO** sia sempre **tempestivamente** e **adeguatamente coinvolto** in **tutte le questioni inerenti al trattamento**. In più il DPO è **totalmente indipendente** e non deve ricevere istruzioni da nessuno per l'assolvimento dei propri doveri.

È **decisamente più opportuno** nominare un **DPO esterno**: in modo da assicurare il principio di **imparzialità** e **scongiurare** ogni eventuale ipotesi di **conflitto d'interessi**. Se il DPO fosse un dipendente svolgendo altre mansioni all'interno dell'azienda potrebbe risultare autore di un possibile conflitto di interessi con quelle proprie dell'altro incarico (e difficilmente all'interno dell'Azienda è presente una figura con i requisiti richiesti dalla normativa, necessari per legge).

Il **DPO** deve essere una **figura indipendente** e al di **sopra** delle **parti**, un soggetto specifico ed esperto in materia, che si occupi esclusivamente della protezione dei dati personali. Egli necessita di una **preparazione specialistica**, una **formazione continua** e di un'**esperienza** concreta acquisita **sul campo** nel corso del tempo, in modo da essere in grado di supportare adeguatamente le organizzazioni nell'ambito di un mercato unico digitale europeo.

## | Fonti consultate |

Informazioni sul Dpo:

- Asso Dpo (associazione Data protection officer) <https://www.assodpo.it/it/chi-e-il-dpo/>
- Protezione dati personali.it  
<https://protezionedatipersonali.it/data-protection-officer>
- Federprivacy.org  
<https://federprivacy.org/informazione/primo-piano/item/176-data-protection-officer-requisiti-compiti-e-certificazioni>
- Frareg  
<https://www.frareg.com/it/legge-sulla-privacy/d-p-o-data-protection-officer-chi-e-e-cosa-deve-fare/>
- Dmep.it  
<https://www.dmep.it/inboundmarketing/perch%C3%A8-affidarsi-ad-un-dpo-esterno>