REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

# Linea Guida in materia di responsabili della protezione dei dati (DPO)

**13 dicembre 2016**

La presente costituisce una traduzione non ufficiale e di cortesia in lingua italiana della versione in lingua inglese del documento 16/EN WG243: Linea Guida in materia di responsabili della protezione dei dati (DPO) 13 dicembre 2016 del WG 29

Tale traduzione (versione n.1) è stata effettuata, nell'ottica di condivisione della conoscenza, al fine di agevolare la lettura da parte di cittadini, imprese e associazioni nell'attesa della traduzione ufficiale da parte degli organi competenti.

Non si assume alcuna responsabilità in merito alla correttezza della traduzione stessa.

*Traduzione a cura di: dott. Stefano Gorla*

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46 / CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995,

visti gli articoli 29 e 30,

visto il suo regolamento,

Ha adottato gli orientamenti presenti:

## Indice dei contenuti

## 1. Introduzione

Il Regolamento Generale sulla Protezione dei Dati (GDPR – General Data Protection Regulation)[1], che entrerà in vigore il 25 maggio 2018, fornirà un moderno quadro basato sulla responsabilità, relativo alla conformità per la protezione dei dati in Europa. I responsabili della protezione dei dati (DPO – Data Protection Officer) saranno, per molte organizzazioni, al centro di questo nuovo quadro giuridico, facilitando così il rispetto delle disposizioni del GDPR.

Per il GDPR, è obbligatorio per alcuni titolari e responsabili, designare un DPO[2]. Questo è il caso di tutte le autorità pubbliche e gli organismi (indipendentemente da quali dati elaborino), e per altre organizzazioni che - come attività principale – hanno il monitoraggio sistematico e su larga scala delle persone, o trattano particolari categorie di dati personali su larga scala.

Anche quando il GDPR non prevede esplicitamente la nomina di un DPO, le organizzazioni possono trovare utile designare, su base volontaria, un DPO. Il Gruppo di Lavoro sulla Protezione dei Dati Articolo 29 (WP29) incoraggia tali designazioni volontarie.

Il concetto di DPO non è nuovo. Anche se la direttiva 95/46 / CE[3] non obbligava nessuna organizzazione a nominare un DPO, nella pratica, la nomina del DPO si è sviluppata nel corso degli anni in vari Stati membri.

Prima dell'adozione del GDPR, il WP29 ha sostenuto che il DPO è un elemento fondamentale di responsabilità e che la nomina di un DPO possa facilitare la conformità e, inoltre, diventare un vantaggio competitivo per il business[4]. Oltre a facilitare la conformità attraverso la realizzazione di strumenti di evidenza delle responsabilità (accountability) (ad esempio facilitare o effettuare valutazioni di impatto sulla protezione dei dati e audit), i DPO fungono da intermediari tra le parti interessate (ad esempio le autorità di vigilanza, le persone interessate e le unità di business all'interno di un'organizzazione).

---

[1] *Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46 / CE (regolamento sulla protezione dei dati generali), (GU L 119, 2016/05/04).*

[2] *La nomina di un DPO è obbligatoria anche per le autorità competenti ai sensi dell'articolo 32 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali dalle autorità competenti ai fini della prevenzione, ricerca, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, e che abroga la decisione quadro 2008/977 / GAI del Consiglio (GU L 119, 4.5. 2016, p. 89-131), e la legislazione nazionale di attuazione. Mentre queste linee guida si concentrano sul DPO del GDPR, la guida è rilevante anche per quanto riguarda il DPO ai sensi della direttiva 2016/680, per quanto riguarda le loro analoghe disposizioni.*

[3] *Direttiva 95/46 / CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag . 31).*

[4] *Vedi http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf*

Il DPO non è personalmente responsabile in caso di mancato rispetto del GDPR. Il GDPR esplicita chiaramente che sono il titolare o il responsabile tenuti a garantire ed essere in grado di dimostrare che il trattamento viene eseguito in conformità con le sue disposizioni (articolo 24 (1)). Il rispetto della protezione dei dati è una responsabilità del titolare o del responsabile.

Il titolare o il responsabile hanno anche un ruolo cruciale nel consentire un efficace svolgimento dei compiti del DPO. La nomina di un DPO è un primo passo, ma il DPO deve avere sufficiente autonomia e risorse per svolgere i propri compiti in modo efficace.

Il GDPR riconosce il DPO come un attore chiave nel nuovo sistema di governance dei dati e stabilisce le condizioni per la sua nomina, la posizione e le attività. Lo scopo di queste linee guida è quello di chiarire le disposizioni pertinenti nel GDPR al fine di aiutare i titolari e responsabili al rispetto legislativo, ma anche di assistere il DPO nel proprio ruolo. Le linee guida forniscono anche raccomandazioni sulle best practises, sulla base dell'esperienza acquisita in alcuni Stati membri dell'UE. Il WP29 monitorerà l'attuazione di queste linee guida e potrà integrarle, se necessario, con ulteriori dettagli.

## 2. Designazione di un DPO

### 2.1. Designazione obbligatoria

L'articolo 37 (1) del GDPR richiede la designazione di un DPO in tre casi specifici[5]:

a) quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico[6];

b) se le attività principali del titolare o del responsabile consistono in trattamenti, che richiedono un monitoraggio regolare e sistematico, su larga scala, degli interessati;o

c) quando le attività principali del titolare o il responsabile consistono in trattamenti su larga scala di categorie particolari di dati[7] o[8] dati personali in materia di condanne penali e reati[9].

Nelle seguenti sezioni, il WP29 fornisce una guida per quanto riguarda i criteri e la terminologia utilizzate all'articolo 37(1).

---

[5] *Si noti che ai sensi dell'articolo 37 (4), l'Unione o una legge dello Stato membro possono chiedere la designazione dei DPO in altre situazioni.*

[6] *Fatta eccezione per i tribunali che agiscono a titolo giudiziario.*

[7] *Ai sensi dell'articolo 9 questi includono dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici al fine di identificare in modo univoco una persona fisica, dati relativi alla salute o dati riguardanti la vita sessuale di una persona fisica o l'orientamento sessuale.*

[8] *Articolo 37 (1) (c) usa la parola 'e'. Vedere la sezione 2.1.5, di seguito, per la spiegazione sull'uso del 'o' invece di 'e'.*

[9] *Articolo 10.*

A meno della ovvietà che l'organizzazione non sia tenuta a designare un DPO, il WP29 raccomanda che i titolari ed i responsabili documentino l'analisi interna effettuata per determinare se è necessario o meno nominare un DPO, in modo da essere in grado di dimostrare che il fattori più importanti sono stati correttamente presi in considerazione[10].

Quando un'organizzazione designa una DPO su base volontaria, gli stessi requisiti di cui agli articoli da 37 a 39 si applicano alla sua nomina, alla posizione e alle attività come se la nomina fosse obbligatoria.

Ciò non impedisce ad un'organizzazione, che non vuole designare un DPO su base volontaria e non è legalmente tenuta a designare un DPO, di utilizzare comunque consulenti esperti, con compiti relativi alla protezione dei dati personali, interni od esterni. In questo caso è importante assicurare che non ci sia confusione riguardo il titolo, lo stato, la posizione e compiti. Pertanto, deve essere chiaro, in qualsiasi comunicazione all'interno ed all'esterno dell'azienda, così come con le autorità di protezione dei dati, con le persone interessate, e con il pubblico in generale, che il titolo di questa figura o consulente non è un DPO[11].

### 2.1.1. Autorità o organismo pubblico

Il GDPR non definisce cosa costituisca "un'autorità pubblica o un organismo pubblico". Il WP29 ritiene che tale nozione debba essere determinata in base al diritto nazionale. Di conseguenza, le autorità pubbliche e gli organismi comprendono le autorità nazionali, regionali e locali, ma il concetto, ai sensi delle leggi nazionali applicabili, di solito include anche una serie di altri organismi di diritto pubblico[12]. In tali casi, la designazione di un DPO è obbligatoria.

Un'attività pubblica può essere effettuata, e la pubblica autorità esercitata[13], non soltanto da autorità o enti pubblici, ma anche da altre persone fisiche o giuridiche di diritto pubblico o privato, in settori quali, secondo la normativa nazionale di ciascuno Stato membro, servizi di trasporto pubblico, fornitura di acqua ed energia, infrastrutture stradali, servizio pubblico di radiodiffusione, edilizia residenziale pubblica o organi disciplinari per le professioni regolamentate.

In questi casi, le persone interessate possono trovarsi in una situazione molto simile a quella in cui i propri dati vengono trattati da un'autorità pubblica o da un organismo. In particolare, i dati possono essere trattati per scopi simili e gli individui hanno spesso poca o nessuna scelta, su se e come i loro dati saranno trattati, e pertanto possono richiedere la protezione aggiuntiva che la nomina di un DPO può garantire.

---

[10] *Si veda l'articolo 24(1).*

[11] *Questo è importante anche per i chief privacy officer (CPO) o altri professionisti privacy già attivi oggi in alcune aziende, che non possono sempre soddisfare i criteri del GDPR, per esempio, in termini di disponibilità di risorse o garanzie per l'indipendenza e quindi non possono essere considerati e indicati come DPO.*

[12] *Si veda, ad esempio, la definizione di organismo del settore pubblico e organismo di diritto pubblico di cui all'articolo 2 (1) e (2), della direttiva 2003/98 / CE del Parlamento europeo e del Consiglio del 17 novembre 2003, relativa al riutilizzo delle informazioni del settore pubblico (GU L 345 del 31.12.2003, pag. 90).*

[13] *Articolo 6 (1) (e).*

Anche se non vi è alcun obbligo in questi casi, il WP29 raccomanda, come buona pratica, che:

- organizzazioni private incaricate di fornire servizi o esercitare l'autorità pubblica designino un DPO e che
- tale attività di DPO dovrebbe coprire tutti i trattamenti effettuati, compresi quelli che non sono legati all'esecuzione di un compito pubblico o esercizio del dovere ufficiale (ad esempio, la gestione di un database dei dipendenti).

### 2.1.2. Attività principali

L'articolo 37 (1) (b) e (c) del GDPR si riferisce alle attività principali del titolare o del responsabile. Il considerando 97 specifica che le attività principali di un titolare si riferiscono ad "attività primarie e non si riferiscono al trattamento dei dati personali come attività accessorie". Le attività principali possono essere quindi considerate come le operazioni chiave necessarie per raggiungere gli obiettivi del titolare o del responsabile.

Tuttavia, le attività fondamentali non devono essere interpretate come escludenti le attività in cui il trattamento dei dati costituisce una parte inscindibile di attività del titolare o del responsabile. Ad esempio, l'attività principale di un ospedale è di fornire assistenza sanitaria. Tuttavia, un ospedale non ha può fornire l'assistenza sanitaria in modo sicuro ed efficace senza il trattamento dei dati relativi alla salute, come ad esempio le cartelle cliniche dei pazienti. Pertanto, il trattamento di questi dati deve essere considerato come una delle attività principali di ogni ospedale, pertanto questi, devono designare il DPO.

Un altro esempio potrebbe essere quello di una società di sicurezza privata che svolge la sorveglianza di un certo numero di centri commerciali privati e spazi pubblici. La sorveglianza è l'attività principale della società, che a sua volta è indissolubilmente legata al trattamento dei dati personali. Pertanto, questa società deve designare un DPO.

D'altra parte, tutte le organizzazioni svolgono diverse attività, ad esempio, pagano i loro dipendenti o hanno attività standard IT. Si tratta di funzioni di supporto necessarie per svolgere l'attività principale dell'organizzazione o per raggiungere il business. Anche se queste attività sono necessarie o essenziali, di solito sono considerate funzioni accessorie, rispetto all'attività principale.

### 2.1.3. Larga scala

Articolo 37 (1) (b) e (c), richiede la nomina del DPO per il trattamento dei dati personali effettuato su larga scala. Il GDPR non fornisce una definizione di larga scala, anche se il considerando 91 illustra alcune indicazioni[14].

[14] *Secondo il considerando, 'le operazioni di trattamento su larga scala che mirano a elaborare una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che possano interessare un gran numero di persone interessate e che sono suscettibili di causare un alto rischio' dovrebbero essere incluse. D'altra parte, il considerando prevede espressamente che il trattamento dei dati personali non dovrebbe essere considerato su larga scala se il trattamento riguarda dati personali provenienti da pazienti o clienti da parte di un singolo medico, o altro operatore sanitario o avvocato. È importante considerare che, mentre il considerando fornisce esempi agli estremi della scala (elaborazione da parte di un singolo medico contro trattamento di dati di un intero paese o in Europa), c'è una grande zona grigia tra questi due estremi. Inoltre, va tenuto presente che questo considerando fa riferimento alle valutazioni d'impatto sulla protezione dei dati. Ciò implica che alcuni elementi potrebbero essere specifici per quel contesto e non necessariamente si applicano alla designazione dei DPO esattamente allo stesso modo.*

Infatti, non è possibile dare un numero preciso sia per quanto riguarda la quantità di dati elaborati o il numero di persone interessate, che sia applicabile a tutte le situazioni. Ciò non esclude la possibilità, tuttavia, che nel corso del tempo, possa svilupparsi una pratica standard, per specificare in termini oggettivi e quantitativi ciò che costituisce il trattamento su larga scala di alcuni tipi di attività comuni. Il WP29 prevede inoltre al contributo, attraverso la condivisione e la pubblicazione di esempi di soglie rilevanti per la designazione di un DPO, a questo sviluppo.

In ogni caso, il WP29 raccomanda che, in particolare, i seguenti fattori devono essere presi in considerazione per determinare se il trattamento è effettuato o meno su larga scala:

- Il numero di persone interessate - sia come un numero specifico o come percentuale della popolazione in questione
- Il volume di dati e / o la gamma di differenti elementi di dati in elaborazione
- La durata, o la permanenza, l'attività di elaborazione dei dati
- L'estensione geografica dell'attività del trattamento

Esempi di trattamenti su larga scala includono:

- l'elaborazione dei dati del paziente nel corso normale delle attività di un ospedale
- trattamento dei dati di viaggio di persone che utilizzano il sistema di trasporto pubblico di una città (ad esempio, il monitoraggio tramite schede di viaggio)
- l'elaborazione dei dati in tempo reale di geo-localizzazione di clienti di una catena di fast food internazionale a fini statistici da parte di un responsabile specializzato nella fornitura di questi servizi
- trattamento dei dati dei clienti nel normale corso di attività da una compagnia di assicurazioni o di una banca
- trattamento dei dati personali (profilazione) per la pubblicità di un motore di ricerca
- trattamento dei dati (contenuti, il traffico, la posizione) da parte dei fornitori di servizi telefonici o Internet

Esempi che non costituiscono l'elaborazione su larga scala sono:

- trattamento dei dati dei pazienti da parte di un singolo medico
- trattamento di dati personali relativi a condanne penali e reati da parte di un singolo avvocato.

### 2.1.4. Monitoraggio regolare e sistematico

La nozione di un monitoraggio regolare e sistematico degli interessati, non è definito nel GDPR, ma il concetto di monitorare il comportamento degli interessati è menzionato nel considerando 24[15] e comprende in modo chiaro tutte le forme di monitoraggio e profilatura su internet, anche per i fini della pubblicità comportamentale.

[15] *'Al fine di determinare se un'attività può essere considerata di monitoraggi del comportamento degli interessati, occorre verificare se le persone fisiche sono tracciate su Internet compreso il potenziale utilizzo successivo di tecniche di elaborazione dei dati personali che consistono nel profilare una persona fisica, in particolare al fine di prendere decisioni in materia di lei o di lui o per l'analisi e la previsione di lei o di lui delle sue preferenze personali, comportamenti e atteggiamenti'.*

Tuttavia, il concetto di monitoraggio deve essere considerato soltanto come un esempio di monitoraggio del comportamento degli interessati[16].

WP29 interpreta come definizione di “regolare” il verificarsi di uno o più dei seguenti elementi:

- in corso o che si verificano a intervalli specifici per un determinato periodo
- ricorrente o ripetuto ad orari prestabiliti
- costantemente o periodicamente svolto

WP29 interpreta la definizione di “sistematico” il verificarsi di uno o più dei seguenti elementi:

- il verificarsi in base ad un sistema
- pre-organizzato, organizzato o metodico
- che si svolge nell'ambito di un piano generale per la raccolta dati
- eseguito come parte di una strategia

Esempi: operatori di una rete di telecomunicazioni; fornitura di servizi di telecomunicazione; e-mail retargeting; profilazione e scoring ai fini della valutazione del rischio (ad esempio a scopo di recupero crediti, istituzione di premi assicurativi, la prevenzione delle frodi, l'individuazione di riciclaggio di denaro); tracciabilità della posizione, programmi di fidelizzazione; pubblicità legata ai comportamenti (profilazione); monitoraggio di benessere, fitness e salute dati tramite dispositivi indossabili; televisione a circuito chiuso; dispositivi collegati a contatori intelligenti, macchine intelligenti, domotica, ecc.

#### 2.1.5. Categorie particolari di dati e dati relativi a condanne penali e reati

L’articolo 37 (1) (c) affronta il trattamento di categorie particolari di dati ai sensi dell'articolo 9, e dati personali relativi a condanne penali e reati di cui all'articolo 10. Anche se la dicitura usa la parola 'e', non vi è alcuna ragione per cui i due criteri debbano essere applicati contemporaneamente. Il testo dovrebbe quindi essere letto come 'o'.

### 2.2. DPO del responsabile

L'articolo 37 si applica sia ai titolari[17] che ai responsabili[18] per quanto riguarda la designazione di un DPO. A seconda di chi soddisfa i criteri sulla designazione obbligatoria, cioè in alcuni casi solo il titolare o solo il responsabile, oppure in altri casi, sia il titolare e il responsabile sono tenuti a nominare un DPO (che dovrebbero quindi cooperare tra loro).

---

[16] *Si noti che il considerando 24 si concentra sulla applicazione extraterritoriale del GDPR. Inoltre, vi è anche una differenza tra la dicitura “monitorare il loro comportamento” (articolo 3 (2) (b)), e “monitoraggio regolare e sistematico delle persone interessate” (articolo 37 (1) (b)), che potrebbe quindi essere visto come parte di una diversa nozione.*

[17] *Il titolare è definito dall'articolo 4 (7) come la persona fisica o giuridica, che determina le finalità e gli strumenti del trattamento.*

[18] *Il responsabile è definito dall'articolo 4 (8) come la persona fisica o giuridica, che elabora i dati per conto del titolare.*

E’ importante sottolineare che anche se il titolare soddisfa i criteri per la designazione obbligatoria, il suo responsabile non è necessariamente tenuto a nominare un DPO. Questo può, tuttavia, però essere una buona prassi.

Esempi:

- Una piccola azienda familiare attiva nella distribuzione di elettrodomestici in un unico comune, utilizza i servizi di un responsabile la cui attività principale consiste nel fornire servizi di analisi di siti web e di assistenza con pubblicità mirata e marketing. Le attività dell'azienda di famiglia e dei suoi clienti non generano l'elaborazione di dati su larga scala, considerando il piccolo numero di clienti e le attività relativamente limitate. Tuttavia, le attività del responsabile (una PMI), che possiede in tal modo molti clienti, presi insieme, possono configurarsi come trattamenti su larga scala. Il responsabile deve quindi nominare un DPO ai sensi dell'articolo 37 (1) (b). Allo stesso tempo, l'azienda di famiglia in sé non ha l'obbligo di designare un DPO.
- una società di produzione di piastrelle di medie dimensioni subappalta i servizi di medicina del lavoro ad un responsabile esterno, che possiede un gran numero di clienti simili. Il responsabile designa un DPO ai sensi dell'articolo 37 (1) (c) a condizione che il trattamento sia su larga scala. Tuttavia, il produttore non è necessariamente obbligato a nominare un DPO.

Come buona prassi, il WP29 raccomanda che il DPO, designato da un responsabile, dovrebbe anche supervisionare le attività svolte dall'organizzazione in qualità di titolari del trattamento vero e proprio (ad esempio risorse umane, IT, logistica).

### 2.3. Facilmente raggiungibile da ogni stabilimento

Articolo 37 (2) permette ad un gruppo di imprese di designare un unico DPO a condizione che questi sia facilmente raggiungibile da ogni stabilimento. Il concetto di accessibilità si riferisce ai compiti del DPO come un punto di contatto rispetto agli interessati[19], all’autorità di controllo[20] ma anche internamente all'organizzazione, considerando che uno dei compiti del DPO è informare e consigliare, dei loro obblighi ai sensi della presente Regolamento[21], il titolare, il responsabile e i dipendenti che svolgono trattamenti.

Al fine di garantire che il DPO, interno o esterno, sia accessibile e contattabile è importante garantire che il suo indirizzo di contatto sia disponibile in conformità con i requisiti del GDPR[22].

Il DPO deve essere in grado di comunicare in modo efficiente con gli interessati[23] e cooperare[24] con le autorità di vigilanza. Questo significa anche che tale comunicazione

[19] *L'articolo 38 (4): gli interessati possono contattare il responsabile della protezione dei dati per quanto riguarda tutte le questioni relative al trattamento dei propri dati personali e per l'esercizio dei loro diritti ai sensi del presente regolamento.*

[20] *L'articolo 39 (1) (e): ‘fungere da punto di contatto per l'autorità di controllo su questioni relative al trattamento, tra cui la consultazione preliminare di cui all'articolo 36, e di consultare, se del caso, in relazione a qualsiasi altra questione'.*

[21] *L'articolo 39 (1) (a).*

[22] *Vedi anche la sezione 2.5.*

deve avvenire nella lingua o nelle lingue utilizzate dalle autorità di controllo e delle persone interessate.

Ai sensi dell'articolo 37 (3), un singolo DPO può essere designato per più autorità o enti pubblici, tenendo conto della loro struttura e dimensione organizzativa. Le stesse considerazioni valgono per quanto riguarda le risorse e la comunicazione. Dato che il DPO è responsabile di una serie di compiti, il titolare deve garantire che un singolo DPO sia in grado di eseguire in modo efficiente ed efficace questi compiti, pur essendo responsabile di diversi enti pubblici ed enti.

La disponibilità personale di un DPO (sia fisicamente negli stessi locali come dipendenti, attraverso un numero verde o altro mezzo di comunicazione sicuro) è essenziale per garantire che gli interessati siano in grado di contattare il DPO. Il DPO è tenuto al segreto o alla riservatezza relativa al rendimento dei suoi compiti, in conformità con il diritto dell'Unione o Stato membro (articolo 38 (5)). Tuttavia, l'obbligo del segreto / riservatezza non vieta il che il DPO possa contattare e chiedere un parere all'autorità di vigilanza.

### 2.4. Competenze e capacità del DPO

Articolo 37 (5), prevede che il DPO 'è designato in base alla qualità professionali e, in particolare, conoscenza approfondita del diritto alla protezione dei dati, delle pratiche e la capacità di svolgere i compiti di cui all'articolo 39'. Il considerando 97 prevede che il livello necessario di conoscenze specialistiche deve essere determinato in base ai trattamenti dei dati effettuati e la loro protezione.

- **Livello di esperienza**

Il livello richiesto di competenza non è strettamente definito ma deve essere commisurato con la sensibilità, la complessità e la quantità di dati dei processi organizzativi. Ad esempio, quando un trattamento è particolarmente complesso, o se comporta una grande quantità di dati sensibili, per il DPO potrebbe essere necessario un più elevato livello di competenza e di supporto. C'è anche una differenza a seconda che l'organizzazione trasferisca sistematicamente dati personali al di fuori dell'Unione Europea o se tali trasferimenti siano occasionali. Il DPO dovrebbe quindi essere scelto con cura, tenendo conto delle questioni relative alla protezione dei dati che sorgono all'interno dell'organizzazione.

- **Qualità professionali**

Anche se l'articolo 37 (5) non specifica le qualità professionali che devono essere considerate quando si designa un DPO, è importate il fatto che il DPO debba avere esperienza sulla legislazione relativa alla protezione dei dati personali sia nazionale che europea, sulle prassi e debba avere una conoscenza approfondita del GDPR. Risulta utile che le autorità di controllo promuovano una formazione adeguata e regolare per i DPO.
Risulta utile la conoscenza del settore di business delle imprese e dell'organizzazione del titolare. Il DPO dovrebbe anche avere una conoscenza sui processi di trattamento dei dati

---

[23] *L'articolo 12 (1): Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.*

[24] *L'articolo 39 (1) (d): a cooperare con l'autorità di controllo.*

e sulle operazioni effettuate, nonché sui sistemi informativi, le esigenze di sicurezza dei dati e la protezione dei dati del titolare.
Nel caso di un ente pubblico o di un organismo, il DPO dovrebbe anche avere una buona conoscenza delle regole e delle procedure amministrative dell'organizzazione.

- **Capacità di svolgere i suoi compiti**

La capacità di soddisfare i compiti del DPO deve essere interpretata sia in riferimento alle sue qualità personali e alla conoscenza, ma anche in riferimento alla sua posizione all'interno dell'organizzazione. Le qualità personali dovrebbero includere, per esempio: integrità e alta etica professionale; la preoccupazione primaria del DPO dovrebbe essere di garantire la conformità al GDPR. Il DPO svolge un ruolo chiave nella promozione di una cultura della protezione dei dati all'interno dell'organizzazione e aiuta ad implementare gli elementi essenziali del GDPR, come ad esempio i principi di trattamento dei dati[25], diritti degli interessati[26], la protezione dei dati fin dalla progettazione e per default[27], la registrazione delle attività[28], la sicurezza dei trattamenti[29], la notifica e la comunicazione dei dati breach[30].

- **DPO sulla base di un contratto di servizio**

La funzione del DPO può essere esercitata anche sulla base di un contratto di servizio stipulato con una persona o un'organizzazione esterna all'organizzazione del titolare / responsabile. In quest'ultimo caso, è essenziale che ogni membro dell'organizzazione che esercita le funzioni di DPO soddisfi tutti i requisiti relativi alla sezione 4 della GDPR (ad esempio, è essenziale che nessuno abbia un conflitto di interessi). E' altrettanto importante che ogni membro sia protetto dalle disposizioni del GDPR (ad esempio senza la cessazione abusiva di contratto di servizio per attività come DPO, ma anche nessun licenziamento senza giusta causa di un singolo membro dell'organizzazione durante lo svolgimento dei compiti di DPO). Allo stesso tempo, le singole abilità e capacità possono essere combinate in modo che diverse persone, che lavorano in team, possano servire più efficacemente i clienti.
Per motivi di chiarezza giuridica e di buona organizzazione si raccomanda di avere una chiara ripartizione dei compiti e ruoli all'interno del team del DPO e assegnare ad una singola persona il ruolo di riferimento univoco di contatto e di responsabile per ogni cliente. Sarebbe generalmente utile anche specificare questi punti nel contratto di servizio.

### 2.5. Pubblicazione e comunicazione delle informazioni di contatto del DPO

L'articolo 37 (7) del GDPR richiede al titolare o al responsabile:

- di pubblicare i dati di contatto del DPO e
- di comunicare i dati di contatto alle autorità di controllo competenti.

L'obiettivo di questi requisiti è quello di garantire che gli interessati (sia all'interno che all'esterno dell'organizzazione) e le autorità di controllo possono facilmente, direttamente

[25] *Capitolo II.*
[26] *Capitolo III.*
[27] *Articolo 25.*
[28] *Articolo 30.*
[29] *Articolo 32.*
[30] *Articoli 33 e 34.*

ed in maniera riservata contattare il DPO senza dover contattare un'altra parte dell'organizzazione.

I dati di contatto del DPO dovrebbero includere informazioni che consentano alle persone interessate e alle autorità di controllo di raggiungere il DPO in modo semplice (un indirizzo postale, un numero di telefono dedicato, e un indirizzo di posta elettronica dedicato). Se necessario, ai fini della comunicazione con il pubblico, possono anche essere previsti altri mezzi di comunicazione, per esempio, un numero verde dedicato o un modulo di contatto dedicato rivolti al DPO, magari sul sito web dell'organizzazione.

L'articolo 37 (7) non richiede che i dati di contatto pubblicati debbano includere il nome del DPO. Anche se includere il nome può essere una buona prassi, è il titolare e il DPO che possono decidere se ciò sia necessario, o utile in circostanze particolari[31].

Il WP29 raccomanda che l'organizzazione informi l'autorità di controllo e i dipendenti del nome e dei recapiti del DPO. Ad esempio, il nome e i recapiti del DPO potrebbero essere pubblicati internamente sulla rete Intranet dell'organizzazione, o sull'elenco telefonico interno e negli organigrammi.

## 3. Posizione del DPO

### 3.1. Il coinvolgimento del DPO in tutte le questioni relative alla protezione dei dati personali

L'articolo 38 del GDPR prevede che il titolare e il responsabile assicurino che il DPO sia coinvolto, correttamente e in modo tempestivo, in tutte le questioni che riguardano la protezione dei dati personali.

E' fondamentale che il DPO sia coinvolto il prima possibile in tutte le questioni relative alla protezione dei dati. In relazione alle valutazioni di impatto sulla protezione dei dati il GDPR prevede esplicitamente il precoce coinvolgimento del DPO e specifica che il titolare deve chiedere il parere del DPO nello svolgimento di tale valutazione di impatto[32].

Risulta importante garantire che il DPO sia informato e consultato, in via preliminare, in modo da facilitare il rispetto del GDPR, inoltre garantire il rispetto di un approccio "privacy by design" attraverso una procedura standard adottata all'interno dell'organizzazione. Inoltre, è importante che il DPO possa essere visto come un interlocutore all'interno dell'organizzazione e che sia parte dei gruppi di lavoro che si occupano di attività di trattamento dei dati all'interno dell'organizzazione.

Di conseguenza, l'organizzazione deve garantire, ad esempio, che:

- il DPO sia invitato a partecipare regolarmente alle riunioni di dirigenti e quadri.
- la sua presenza è raccomandata in tutti i casi in cui vengono prese le decisioni con implicazioni sulla protezione dei dati. Tutte le informazioni pertinenti devono essere

[31] *E' da notare che l'articolo 33 (3) (b), che descrive le informazioni che devono essere fornite alle autorità di controllo e alle persone interessate, in caso di una violazione dei dati personali, a differenza dell'articolo 37 (7), in particolare richiede che siano comunicati anche il nome (e non solo i dati di contatto) del DPO.*

[32] *Articolo 35 (2).*

trasmesse al DPO in modo tempestivo al fine di consentirgli di fornire consulenza adeguata.
- al parere del DPO deve essere sempre dato il giusto peso. In caso di disaccordo, il WP29 raccomanda, come buona pratica, di documentare le ragioni per le quali non si ritiene opportuno seguire il consiglio del DPO.
- il DPO deve essere tempestivamente consultato nel caso di violazione dei dati o nel caso in cui si verifichi un altro tipo di incidente.

Quando necessario, il titolare o il responsabile può elaborare delle linee guida sulla protezione dei dati o dei programmi che stabiliscono quando il DPO debba essere consultato.

### 3.2. Risorse necessarie

L'articolo 38 (2) del GDPR richiede che l'organizzazione, per sostenere il DPO, 'fornisca le risorse necessarie per svolgere [suoi] compiti e l'accesso ai dati personali ed operazioni di trattamento, e di mantenere la sua conoscenza specialistica. In particolare, sono da considerare i seguenti elementi:

- Sostegno attivo della funzione del DPO da parte della direzione (ad esempio dall'alta Direzione).
- Tempo sufficiente per il DPO per adempiere ai suoi doveri. Ciò è particolarmente importante nel caso in cui il DPO è nominato su base part-time o quando il lavoratore svolge la protezione dei dati in aggiunta ad altri compiti. In caso contrario, dei conflitti di priorità potrebbero comportare che le funzioni del DPO vengano trascurate. Avere un tempo sufficiente da dedicare ai compiti del DPO è di primaria importanza. Si tratta di buona prassi stabilire una percentuale di tempo per la funzione di DPO dove questa non venga eseguita a tempo pieno. E' anche buona pratica determinare il tempo necessario per svolgere la funzione, il livello appropriato di priorità per le funzioni del DPO, e per il DPO (o l'organizzazione) di elaborare un piano di lavoro
- Sostegno adeguato in termini di risorse finanziarie, infrastrutture (locali, strutture, attrezzature) e del personale, se del caso.
- Comunicazione ufficiale della designazione del DPO a tutto il personale al fine di garantire che la sua esistenza e la funzione sia conosciuta all'interno dell'organizzazione.
- Necessario accesso ad altri servizi, quali le risorse umane, legale, IT, sicurezza, ecc, in modo che i DPO possano ricevere supporto essenziale, input e informazioni da questi altri servizi.
- Formazione continua. Al DPO dovrebbe essere data la possibilità di rimanere aggiornato in materia di protezione dei dati. L'obiettivo dovrebbe essere quello di aumentare costantemente il livello di competenza del DPO e dovrebbe essere incoraggiato a partecipare a corsi di formazione sulla protezione dei dati e altre forme di sviluppo professionale, come la partecipazione in privacy forum, workshop, ecc
- Date le dimensioni e la struttura dell'organizzazione, può essere necessario allestire una squadra di DPO (un DPO e il suo staff). In questi casi, la struttura interna della squadra e dei compiti e delle responsabilità di ciascuno dei suoi membri dovrebbe essere chiaramente redatta. Allo stesso modo, quando la funzione del DPO è

esercitata da un fornitore esterno, un gruppo di persone, che lavorano per questa entità, possono efficacemente svolgere i compiti di un DPO come una squadra, sotto la responsabilità di un responsabile di contatto designato per il cliente.

In generale maggiori sono i trattamenti e la loro complessità o i trattamenti sensibili, maggiori devono essere le risorse allocate per il DPO. La funzione di protezione dei dati deve essere efficace e sufficientemente costruita in relazione ai trattamenti dei dati in corso.

### 3.3. Istruzioni e "agire in modo indipendente"

L'articolo 38 (3) stabilisce alcune garanzie di base per contribuire a garantire che il DPO sia in grado di svolgere i suoi compiti con un sufficiente grado di autonomia all'interno dell'organizzazione. In particolare, il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il considerando 97 aggiunge che il DPO 'anche se non è un dipendente del titolare, dovrebbe essere in grado di svolgere le sue funzioni e compiti in modo indipendente '.

Ciò significa che, nell'adempimento dei suoi compiti di cui all'articolo 39, il DPO non deve essere istruito su come affrontare una questione, per esempio, quale risultato dovrebbe essere raggiunto, come indagare su una denuncia o se è necessario consultare l'autorità di controllo. Inoltre i DPO, non devono ricevere indicazioni su come avere un particolare punto di vista in merito ad un problema relativo alla legge sulla protezione dei dati, per esempio, una particolare interpretazione della legge.

L'autonomia dei DPO, tuttavia, non significa che essi hanno poteri decisionali che si estendono oltre i loro compiti di cui all'articolo 39.

Il titolare o il responsabile rimangono responsabili per il rispetto della normativa sulla protezione dei dati e devono essere in grado di dimostrarne la conformità[33]. Se il titolare o il responsabile prende decisioni che sono incompatibili con il GDPR e con il parere del DPO, al DPO deve essere data la possibilità di rendere chiara la propria opinione dissenziente a coloro che devono prendere le decisioni.

### 3.4. Licenziamento o penali per l'esecuzione di attività del DPO

L'articolo 38 (3) richiede anche che il DPO dovrebbe 'non essere licenziato o subire penali o richiami dal titolare o responsabile per l'esecuzione dei [suoi] compiti'.

Questo requisito rafforza anche l'autonomia dei DPO e aiuta a garantire che essi possano agire in modo indipendente e godere di una protezione sufficiente nello svolgimento delle loro attività di protezione dei dati.

Le sanzioni sono vietate, secondo il GDPR, solamente se sono inflitte a seguito del fatto che il DPO svolga o abbia svolto le sue funzioni come DPO. Ad esempio può succedere ch un DPO consideri che un particolare trattamento è suscettibile di provocare un rischio elevato e consigliare il titolare o il responsabile di effettuare una valutazione d'impatto sulla protezione dei dati, e che il titolare o il responsabile non sia d'accordo con la valutazione

[33] *Articolo 5 (2).*

del DPO. In una tale situazione, il DPO non può essere licenziato per aver fornito questo consiglio.

Le sanzioni possono assumere una varietà di forme e possono essere dirette o indirette. Esse potrebbero consistere, ad esempio, nella assenza o nel ritardo della promozione; prevenzione da avanzamento di carriera; rifiuto da benefici che altri dipendenti ricevono. Non è necessario che tali sanzioni siano effettivamente eseguite, una semplice minaccia è sufficiente fintanto che vengono utilizzate per penalizzare il DPO per motivi legati alla sua o alle sue attività in qualità di DPO.

Come normale regola di gestione e come sarebbe il caso per qualsiasi altro dipendente o imprenditore, o soggetto a contratto nazionale applicabile o del lavoro e del diritto penale, un DPO potrebbe ancora essere licenziato legittimamente per motivi diversi a quelli legali all'esecuzione dei suoi compiti (per esempio, in caso di furto, molestie fisiche, psicologiche o sessuali o simili atti di colpa grave).

In questo contesto, va notato che il GDPR non specifica come e quando un DPO può essere licenziato o sostituito da un'altra persona. Tuttavia, più stabile è il contratto di DPO, o esistono maggiori garanzie contro il licenziamento ingiusto, più è probabile che sarà in grado di agire in modo indipendente. Pertanto, il WP29 accoglierebbe con favore gli sforzi delle organizzazioni in tal senso.

### 3.5. Conflitto d'interessi

L'articolo 38 (6) permette al DPO di 'compiere altri compiti e mansioni'. Si richiede, tuttavia, che l'organizzazione assicuri che 'tali compiti e dei doveri non diano luogo ad un conflitto di interessi'.

L'assenza di conflitto di interessi è strettamente legata alla necessità di agire in modo indipendente. Anche se il DPO è autorizzato ad avere altre funzioni, possono essergli affidati solo altri compiti che non diano luogo a conflitti di interesse. Ciò comporta, in particolare, che il DPO non può tenere una posizione all'interno dell'organizzazione che porta a determinare le finalità e gli strumenti del trattamento di dati personali. Questo deve essere considerato caso per caso in funzione della specifica struttura organizzativa in ogni organizzazione[34].

A seconda delle attività, delle dimensioni e della struttura dell'organizzazione, può essere utile per i titolari o responsabili:

- individuare le posizioni che sarebbero incompatibili con la funzione di DPO
- elaborare il regolamento interno al fine di evitare conflitti di interesse
- includere una spiegazione più generale sui conflitti di interesse
- dichiarare che il DPO non ha alcun conflitto di interessi per quanto riguarda la sua funzione di DPO, in modo da aumentare la consapevolezza su questo requisito
- includere le garanzie, nelle regole interne dell'organizzazione, e garantire che l'avviso di posto vacante per il posto di DPO o per il contratto di servizio sia

[34] *Come regola generale, le posizioni contrastanti possono includere posizioni di senior management (come amministratore delegato, direttore operativo, direttore finanziario, capo ufficiale medico, capo del dipartimento di marketing, capo delle risorse umane o capo di reparti IT), ma anche altri ruoli più in basso nella struttura organizzativa se tali posizioni o ruoli portano alla determinazione delle finalità e modalità del trattamento.*

sufficientemente preciso e dettagliato, al fine di evitare un conflitto di interessi. In questo contesto, va anche tenuto presente che i conflitti di interesse possono assumere forme diverse a seconda che il DPO sia assunto internamente o esternamente.

## 4. Compiti del DPO

### 4.1. Controllo del rispetto del GDPR

L'articolo 39 (1) (b) affida al DPO, tra gli altri compiti, il compito di controllare il rispetto del GDPR. Il considerando 97 specifica inoltre che il DPO 'dovrebbe aiutare il titolare o il responsabile al monitoraggio della compliance interna del rispetto del presente regolamento'.

Come parte di questi compiti per controllare la compliance, i DPO possono, in particolare:

- raccogliere informazioni per identificare le attività di trattamento,
- analizzare e verificare la conformità delle attività di trattamento, e
- informare, consigliare ed emettere raccomandazioni al titolare o al responsabile.

Il controllo del rispetto non significa che il DPO sia personalmente responsabile nel caso in cui vi sia una non conformità. Il GDPR rende chiaro che è il titolare, non il DPO, che è tenuto ad 'attuare misure tecniche e organizzative per garantire e per essere in grado di dimostrare che il trattamento viene eseguito in conformità del presente regolamento' (articolo 24 (1)). il rispetto della protezione dei dati è una responsabilità aziendale del titolare del trattamento, non del DPO.

### 4.2. Il ruolo del DPO in una valutazione d'impatto sulla protezione dei dati

Ai sensi dell'articolo 35 (1), è compito del titolare, non del DPO, effettuare, quando necessario, una protezione dei dati di valutazione dell'impatto (DPIA- Data Protection Impact Assessment). Tuttavia, il DPO può svolgere un ruolo molto importante e utile per supportare il titolare. Seguendo il principio della protezione dei dati "by design", l'articolo 35 (2) richiede espressamente che il titolare 'deve chiedere il parere' del DPO nello svolgimento di un'attività di DPIA. L'articolo 39 (1) (c), a sua volta, cita tra i compiti del DPO quello di 'fornire consulenza ove richiesto per quanto riguarda il [DPIA] e monitorare le sue prestazioni'.

Il WP29 raccomanda che il titolare chieda, tra gli altri, il parere del DPO, sui seguenti temi[35]:

- effettuare o meno un DPIA
- metodologia da seguire nello svolgimento di un'attività di DPIA
- se effettuare un DPIA in-house o se esternalizzare
- quali garanzie (comprese le misure tecniche e organizzative) da applicare per mitigare gli eventuali rischi per i diritti e gli interessi delle persone interessate
- se la valutazione dei dati di impatto di protezione è stata effettuata correttamente e se le sue conclusioni e pianificazioni sono conformi al GDPR.

[35] *L'articolo 39 (1) cita i compiti del DPO e indica che il DPO deve avere "almeno" i seguenti compiti. Pertanto, nulla impedisce al titolare di assegnare al DPO altri compiti diversi da quelli esplicitamente menzionati all'articolo 39 (1), o specificando i compiti in modo più dettagliato.*

Se il titolare non è d'accordo con la consulenza fornita dal DPO, la documentazione del DPIA dovrebbe specificamente giustificare per iscritto il motivo per cui il consiglio non è stato preso in conto[36].

Il WP29 raccomanda inoltre che il titolare deve delineare con chiarezza, ad esempio, nel contratto del DPO, ma anche nelle informazioni fornite ai dipendenti (e altre parti interessate, se del caso), la gestione, i compiti precisi e la loro portata del DPO, in particolare per quanto riguarda la realizzazione del DPIA.

### 4.3. Approccio risk-based

L'articolo 39 (2) richiede che il DPO 'deve tenere debitamente in conto del rischio associato alle operazioni di trattamento, tenuto conto della natura, la portata, il contesto e le finalità del trattamento' cioè è necessaria una valutazione corretta dei rischi.

Questo articolo richiama un principio di senso più generale e comune, che può essere rilevante per il lavoro quotidiano del DPO. In sostanza, si richiede ai DPO di dare la priorità alle attività e concentrare i gli sforzi su questioni che presentino un rischio più elevato di protezione dei dati. Questo non significa che essi debbano trascurare il controllo del rispetto dei dati di operazioni che hanno un livello relativamente più basso di rischio di trattamento, ma indica che essi dovrebbero concentrarsi, in primo luogo, sulle aree a più alto rischio.

Questo approccio selettivo e pragmatico dovrebbe aiutare il DPO a consigliare al titolare quale metodologia utilizzare nello svolgimento di un DPIA, quali settori dovrebbero essere oggetto di un controllo di protezione dei dati sia interni che esterni, quali attività di formazione interna sia necessario fornire al personale o al management per le attività di trattamento dei dati.

### 4.4. Il ruolo del DPO nella tenuta dei registri

Ai sensi dell'articolo 30 (1) e (2), è il titolare o il responsabile, non il DPO, che è tenuto a 'mantenere un registro delle operazioni di trattamento sotto la propria responsabilità' o 'di mantenere un registro di tutte le categorie di attività di trattamento svolte per conto di un titolare'.

In pratica, i DPO spesso creano degli inventari e tengono un registro dei trattamenti sulla base delle informazioni ricevute dai vari reparti in merito al trattamento dei dati personali. Questa pratica è stata stabilita in rispetto a molte leggi nazionali vigenti e in base alle norme sulla protezione dei dati applicabili alle istituzioni e organismi UE[37].

L'articolo 39 (1), prevede un elenco dei compiti che il DPO deve avere come minimo. Pertanto, nulla impedisce al titolare o al responsabile di assegnare al DPO il compito di mantenere il registro delle operazioni di trattamento, sotto la responsabilità del titolare. Tale registro dovrebbe essere considerato come uno degli strumenti che permettono al

[36] *Articolo 24 (1), prevede che 'tenuto conto della natura, la portata, il contesto e le finalità del trattamento, nonché i rischi delle variazioni della probabilità e la gravità per i diritti e le libertà delle persone fisiche, il titolare deve attuare misure tecniche ed organizzative al fine di garantire e di essere in grado di dimostrare che il trattamento viene eseguito in conformità del presente regolamento. Tali misure sono riviste e aggiornate, ove necessario '.*

[37] *Articolo 24 (1) (d), del regolamento (CE) 45/2001.*

DPO di svolgere i suoi compiti di controllo della conformità, informando e consigliando il titolare o il responsabile.

In ogni caso, il registro di cui è necessaria la conservazione a norma dell'articolo 30, dovrebbe essere visto come uno strumento che consenta il controllo, su richiesta da parte dell'autorità di controllo, e di avere una panoramica di tutte le attività di trattamento dei dati personali che un’organizzazione sta svolgendo. È quindi un prerequisito per la conformità, e come tale, risulta una misura di accountability.