Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo II

Il Ruolo del Data Protection Officer

Avv. Michele Iaselli

M2.1 La figura del Responsabile della Protezione dei dati (RPD | DPO)

Tra le maggiori novità del Regolamento Europeo sulla protezione dei dati personali rientra sicuramente la previsione del Data Protection Officer (DPO) o responsabile della protezione dei dati, figura di indubbio rilievo le cui competenze, per la verità, non sono state ancora chiarite nel modo migliore dagli organi comunitari.

In effetti l'art. 37 del Regolamento prevede che quando:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali, oppure
b) 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, oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9 (dati sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10
il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati (c.d. data protection officer).

Qualora, poi, il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

Il DPO è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai propri compiti. Tale figura, di alto livello professionale, può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure adempiere ai suoi compiti in base a un contratto di servizi e quindi può essere un libero professionista.

Il DPO deve essere prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali sia dal titolare del trattamento che dal responsabile del trattamento e gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal Regolamento.

Il DPO deve godere di ampia autonomia e non riceve alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti. Inoltre il Regolamento specifica (art. 38) che il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti, ma riferisce direttamente ai massimi superiori gerarchici del titolare del trattamento o del responsabile del trattamento.

Quali sono i compiti del DPO? (art. 39 del Regolamento)

a) 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 Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) 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;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento;

d) cooperare con l'autorità di controllo;

e) 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 del Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nonostante tali precisazioni il DPO rimane una figura controversa che è stata molto discussa in seno alla Commissione Europea. E' sicuramente un'importante figura professionale fortemente voluta i cui compiti e responsabilità, però, non sono particolarmente chiari, specialmente avuto riferimento ai rapporti con il titolare del trattamento. E' indubbio però che il responsabile della protezione dei dati sia una figura chiave nell'ambito del trattamento automatizzato dei dati personali.

Linee-guida sui responsabili della protezione dei dati (RPD) del WP 29 adottate il 16 dicembre 2016 ed emendate in data 5 aprile 2017

Proprio per i motivi suesposti il WP 29 istituito dalla Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 ha adottato delle linee guida al fine di chiarire quali debbano essere i requisiti ed i compiti di un Data Protection Officer e quale dovrà essere in concreto il suo apporto nel campo della protezione dei dati personali di un'unità organizzativa.

Innanzitutto le linee guida chiariscono che alcuni titolari e responsabili del trattamento sono tenuti a nominare un DPO in via obbligatoria. Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali (dati sensibili).

Inoltre si suggerisce che ove il Regolamento non imponga in modo specifico la designazione di un DPO, può risultare utile procedere a tale designazione su base volontaria.

La figura del DPO non costituisce una novità assoluta. La direttiva 95/46/CE non prevedeva alcun obbligo di nomina di un DPO, ma in molti Stati membri questa è divenuta una prassi nel corso degli anni (v. ad esempio la Germania)

Il WP29 ha sempre sostenuto che questa figura rappresenti un elemento fondante ai fini della responsabilizzazione, e che la nomina del DPO possa facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese. Oltre a favorire l'osservanza attraverso strumenti di *accountability (per esempio, supportando o svolgendo valutazioni di impatto e audit in materia di protezione dei dati), i DPO fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente.*

Le linee guida chiariscono un altro aspetto molto importante e cioè che i DPO non rispondono personalmente in caso di inosservanza del Regolamento. Quest'ultimo chiarisce che spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del Regolamento stesso (articolo 24, primo paragrafo). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare o sul responsabile.
Inoltre, al titolare o al responsabile del trattamento spetta il compito fondamentale di consentire lo svolgimento efficace dei compiti cui il DPO è preposto. La nomina di un DPO è solo il primo passo, perché il DPO deve disporre anche di autonomia e risorse sufficienti a svolgere in modo efficace i compiti cui è chiamato.

M2.2 Chi deve designare il DPO

Le linee guida suggeriscono ai titolari e responsabili di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un DPO, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti.

Nel Regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Il WP29 ritiene che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico.

In tale ambito il WP29 formula le seguenti raccomandazioni in termini di buone prassi:
- gli organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri dovrebbero nominare un DPO; e
- le attività del DPO nominato nei termini sopra indicati dovrebbero estendersi a tutti i trattamenti svolti, compresi quelli che non sono connessi all'espletamento di funzioni pubbliche o all'esercizio di pubblici poteri quali, per esempio, la gestione di un database del personale.

Per quanto riguarda la nomina di un DPO, l'art. 37 del Regolamento non distingue fra titolari e responsabili del trattamento in termini di sua applicabilità. A seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare ovvero il solo responsabile, oppure sia l'uno sia l'altro a dover nominare un DPO; questi ultimi saranno poi tenuti alla reciproca collaborazione.

Vale la pena di evidenziare che anche qualora il titolare sia tenuto, in base ai criteri suddetti, a nominare un DPO, il suo eventuale responsabile del trattamento non è detto sia egualmente tenuto a procedere a tale nomina – che però può costituire una buona prassi.

Esempi

Una piccola azienda a conduzione familiare operante nel settore della distribuzione di elettrodomestici in una città si serve di un responsabile del trattamento la cui attività principale consiste nel fornire servizi di tracciamento degli utenti del sito web oltre all'assistenza per attività di pubblicità e marketing mirati. Le attività svolte dall'azienda e dai clienti non generano trattamenti di dati "su larga scala", in considerazione del ridotto numero di clienti e della gamma relativamente limitata di attività. Tuttavia, il responsabile del trattamento, che conta numerosi clienti come questa piccola azienda familiare, svolge, nel suo complesso, trattamenti su larga scala. Ne deriva che il responsabile deve nominare un DPO ai sensi dell'art. 37, primo paragrafo, lettera b); al contempo, l'azienda in quanto tale non è soggetta all'obbligo di nomina del DPO.

Un'azienda di medie dimensioni che produce rivestimenti in ceramica incarica un responsabile esterno della gestione dei servizi di salute occupazionale; tale responsabile ha un numero elevato di clienti con caratteristiche analoghe. Il responsabile è tenuto a nominare un DPO ai sensi dell'art. 37, primo paragrafo, lettera b), poiché svolge trattamenti su larga scala. Tuttavia, l'azienda non è tenuta necessariamente allo stesso adempimento.

M2.3 Come definire l'attività principale

L'articolo 37, paragrafo 1, lettere b) e c) del Regolamento contiene un riferimento alle "*attività principali del titolare del trattamento o del responsabile del trattamento".*

Nel considerando 97 si afferma che le attività principali di un titolare del trattamento "riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria".

Con "attività principali" si possono intendere: le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento.

Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare o dal responsabile. Per esempio, l'attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente.

M2.4 Larga scala e monitoraggio regolare e sistematico
M2.5 Cosa fare nel caso di gruppi di imprese

In base all'articolo 37, paragrafo 1, lettere b) e c) del Regolamento, occorre che il trattamento di dati personali avvenga su larga scala per far scattare l'obbligo di nomina di un DPO. Nel Regolamento non si dà alcuna definizione di trattamento su larga scala, anche se il considerando 91 fornisce indicazioni in proposito ("*trattamenti su larga scala, 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*").

Il WP29 raccomanda di tenere conto, in particolare, di alcuni fattori al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Esempi di trattamento su larga scala:
- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di *fast food;*
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Esempi di trattamento non su larga scala:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Il monitoraggio regolare e sistematico

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del Regolamento; tuttavia, il considerando 24 menziona il "*monitoraggio del comportamento di detti interessati" ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale.*
Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati.

L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del WP29:
- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del WP29:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Alcuni esempi:
- curare il funzionamento di una rete di telecomunicazioni;
- la prestazione di servizi di telecomunicazioni;
- il reindirizzamento di messaggi di posta elettronica;
- profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio);
- tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili;
- programmi di fidelizzazione;
- pubblicità comportamentale;
- monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili;
- utilizzo di telecamere a circuito chiuso;
- dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

M2.6 Le competenze
M2.7 Esperienza

In base all'articolo 37 del Regolamento, 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*". Nel considerando 97 si prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.

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. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il DPO avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche distinguere in base all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea.

M2.8 Qualità professionali

L'articolo 37, paragrafo 5, non specifica le qualità professionali da prendere in considerazione nella nomina di un DPO; tuttavia, sono pertinenti al riguardo la conoscenza da parte del DPO della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del Regolamento. Proficua anche la promozione di una formazione adeguata e continua rivolta ai DPO da parte delle Autorità di controllo.

E' utile la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare; inoltre, il DPO dovrebbe avere sufficiente familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare.

Nel caso di un'autorità pubblica o di un organismo pubblico, il DPO dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili.

La norma UNI 11697

Di recente è stata emanata la norma UNI 11697 che definisce i profili professionali relativi al trattamento e alla protezione dei dati personali coerentemente con le definizioni fornite dall'EQF e utilizzando gli strumenti messi a disposizione dalla UNI 11621-1 "Metodologia per la costruzione di profili professionali basati sul sistema e-CF".

Livello	Titolo di studio	Formazione specifica	Esperienza lavorativa	Equipollenza
Responsabile protezione dati	Laurea che includa discipline almeno in parte afferenti alle conoscenze del professionista privacy, legali o tecnico / informatiche[1)].	Corso di almeno 80 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[2)].	Minimo 6 anni di esperienza lavorativa legata alla privacy di cui almeno 4 anni in incarichi di livello manageriale[3)].	Se in possesso di laurea magistrale l'esperienza lavorativa si riduce a 4 anni di cui 3 in incarichi di livello manageriale. Se in possesso di diploma di scuola media superiore minimo 8 anni di esperienza lavorativa di privacy di cui almeno 5 anni in incarichi di livello manageriale.
Manager privacy	Laurea che includa discipline almeno in parte afferenti alle conoscenze del professionista privacy, legali o tecnico / informatiche[1)].	Corso di almeno 60 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[2)].	Minimo 6 anni di esperienza lavorativa legata alla privacy di cui almeno 3 anni in incarichi di livello manageriale[3)].	Se in possesso di laurea magistrale l'esperienza lavorativa si riduce a 4 anni di cui 2 in incarichi di livello manageriale. Se in possesso di diploma di scuola media superiore minimo 8 anni di esperienza lavorativa di privacy di cui almeno 4 anni in incarichi di livello manageriale.
Specialista privacy	Diploma di scuola media superiore.	Corso di almeno 24 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[2)].	Minimo 4 anni di esperienza lavorativa legata alla privacy.	Se in possesso di laurea l'esperienza lavorativa si riduce a 2 anni.
Valutatore privacy	Diploma di scuola media superiore.	Corso di almeno 40 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[2)].	Minimo 6 anni di esperienza lavorativa continuativa legata alla privacy di cui almeno 3 anni in incarichi di audit.	Se in possesso di laurea l'esperienza lavorativa si riduce a 4 anni di cui 2 in incarichi di audit. Se in possesso di Laurea Magistrale minimo 3 anni di esperienza lavorativa di cui 2 in incarichi di audit.

1) Un laureato con laurea non afferente alle conoscenze del professionista privacy, legali o tecnico / informatiche è da considerarsi equiparato a un diplomato di scuola media superiore.

2) È ammissibile la riduzione delle ore di formazione richieste fino a un massimo del 10% (30% per il Valutatore Privacy) in caso di possesso di certificazioni professionali riconosciute come attinenti alle conoscenze richieste al professionista privacy in questione.

3) gli incarichi di livello manageriale possono includere anche attività rilevante svolta nell'ambito di attività di consulenza o di prestazione d'opera condotta nell'ambito dell'esecuzione di ingaggi professionali.

M2.9 Capacità di svolgere i propri compiti

Per capacità di assolvere i propri compiti si deve intendere sia quanto è legato alle qualità personali e alle conoscenze del DPO, sia quanto 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 dovrebbe perseguire in via primaria l'osservanza delle disposizioni del Regolamento.

Il DPO svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, e contribuisce a dare attuazione a elementi essenziali del Regolamento quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali.

M2.10 DPO interno ed esterno
M2.11 Attività

Il ruolo di DPO può essere ricoperto da un dipendente del titolare o del responsabile (non in conflitto di interessi) che conosca la realtà operativa in cui avvengono i trattamenti; l'incarico può essere anche affidato a soggetti esterni, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento (UE) 2016/679 assegna a tale figura. Il responsabile della protezione dei dati scelto all'interno andrà nominato mediante specifico atto di designazione, mentre quello scelto all'esterno, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un contratto di servizi. Tali atti, da redigere in forma scritta, dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento.

In particolare nel caso di un contratto di servizi è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante quale DPO soddisfi tutti i requisiti applicabili come fissati nella Sezione 4 del Regolamento; per esempio, è indispensabile che nessuno di tali soggetti versi in situazioni di conflitto di interessi.

Pari importanza riveste il fatto che ciascuno dei soggetti in questione goda delle tutele previste dal Regolamento: per esempio, non è ammissibile la risoluzione ingiustificata del contratto di servizi in rapporto alle attività svolte in quanto DPO, né è ammissibile l'ingiustificata rimozione di un singolo appartenente alla persona giuridica che svolga funzioni di DPO.

Le linee guida suggeriscono, al fine di favorire una corretta e trasparente organizzazione interna, di procedere a una chiara ripartizione dei compiti all'interno del gruppo di lavoro DPO e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi.

Inoltre si ricorda che l'articolo 37, settimo paragrafo, del Regolamento impone al titolare o al responsabile del trattamento
- di pubblicare i dati di contatto del DPO, e
- di comunicare i dati di contatto del DPO alle pertinenti autorità di controllo.

Queste sono disposizioni che mirano a garantire che tanto gli interessati (all'interno o all'esterno dell'ente/organismo titolare o responsabile) quanto le autorità di controllo possano contattare il DPO in modo facile e diretto senza doversi rivolgere a un'altra struttura operante presso il titolare/responsabile.

M2.12 Requisiti minimi del DPO

Coinvolgimento del DPO sulle questioni riguardanti la protezione dei dati personali

Ai sensi dell'articolo 38 del Regolamento, il titolare e il responsabile assicurano che il DPO sia "*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*".

E', difatti, essenziale che il DPO sia coinvolto quanto prima possibile in ogni questione attinente la protezione dei dati. Per quanto concerne le valutazioni di impatto sulla protezione dei dati, il regolamento prevede espressamente che il DPO vi sia coinvolto fin dalle fasi iniziali e specifica che il titolare ha l'obbligo di consultarlo nell'effettuazione di tali valutazioni.

Assicurare il tempestivo e immediato coinvolgimento del DPO, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del Regolamento e il rispetto del principio di privacy (e protezione dati) fin dalla fase di progettazione; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del titolare/responsabile. Inoltre, è importante che il DPO sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento.

Ciò significa che occorrerà garantire, per esempio:
- che il DPO sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello;
- la presenza del DPO ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il DPO deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;
- che il parere del DPO riceva sempre la dovuta considerazione. In caso di disaccordi, il WP29 raccomanda, quale buona prassi, di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal DPO;
- che il DPO sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Risorse necessarie

L'articolo 38, secondo paragrafo, del Regolamento obbliga il titolare o il responsabile del trattamento a sostenere il DPO "*fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*".

E' quindi necessario:

Supporto attivo delle funzioni del DPO da parte del *senior management (per esempio, a livello del consiglio di amministrazione).*

Tempo sufficiente per l'espletamento dei compiti affidati al DPO. Ciò riveste particolare importanza se il DPO viene designato con un contratto part-time, oppure se il dipendente si occupa di protezione dati oltre a svolgere altre incombenze. In caso contrario, il rischio è che le attività cui il DPO è chiamato finiscano per essere trascurate a causa di conflitti con altre priorità.

Supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale.

Comunicazione ufficiale della nomina del DPO a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'azienda/dell'organismo.

Accesso garantito ad altri servizi (risorse umane, ufficio giuridico, IT, sicurezza, ecc.) così da fornire al DPO supporto, informazioni e input essenziali.

Formazione permanente. I DPO dovrebbero avere la possibilità di curare il proprio aggiornamento con riguardo agli sviluppi nel settore della protezione dati. Ciò mira, in ultima analisi, a consentire un incremento continuo del livello di competenze proprio dei DPO, che dovrebbero essere incoraggiati a partecipare a corsi di formazione su materie attinenti alla protezione dei dati e ad altre occasioni di professionalizzazione (forum in materia di privacy, workshop, ecc.).

Alla luce delle dimensioni e della struttura della singola azienda/del singolo organismo, può risultare necessario costituire un ufficio o un gruppo di lavoro DPO (formato dal DPO stesso e dal rispettivo personale). In casi del genere, è opportuno definire con precisione la struttura interna del gruppo di lavoro nonché i compiti e le responsabilità individuali. Analogamente, se la funzione di DPO viene esercitata da un fornitore di servizi esterno all'azienda/all'organismo, potrà aversi la costituzione di un gruppo di lavoro formato da soggetti operanti per conto di tale fornitore e incaricati di svolgere le funzioni di DPO sotto la direzione di un responsabile che funga da contatto per il cliente.

Indipendenza del DPO

L'articolo 38, terzo paragrafo, del Regolamento fissa alcune garanzie essenziali per consentire ai DPO di operare con un grado sufficiente di autonomia all'interno dell'organizzazione del titolare/responsabile. In particolare, questi ultimi sono tenuti ad assicurare che il DPO "*non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti*".

Il considerando 97 aggiunge che i DPO "*dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente*".

Ciò significa che il DPO, nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Si ricorda, però, che il titolare o il responsabile mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza.

Se il titolare o il responsabile assumono decisioni incompatibili con il Regolamento e le indicazioni fornite dal DPO, quest'ultimo dovrebbe avere la possibilità di manifestare il proprio dissenso ai decisori.

Rimozione o penalizzazione del DPO

L'articolo 38, terzo paragrafo, del Regolamento prevede, inoltre, che il DPO "*non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti*".

Le penalizzazioni possono assumere molte forme e avere natura diretta o indiretta. Per esempio, potrebbero consistere nella mancata o ritardata promozione, nel blocco delle progressioni di carriera, nella mancata concessione di incentivi rispetto ad altri dipendenti. Non è necessario che si arrivi all'effettiva applicazione di una penalizzazione, essendo sufficiente anche la sola minaccia nella misura in cui sia rivolta al DPO in rapporto alle attività da questi svolte.

Viceversa, e conformemente alle normali regole di gestione applicabili a ogni altro dipendente o fornitore soggetto alla disciplina del rispettivo contratto nazionale ovvero alle norme di diritto penale e del lavoro, sarebbe legittimamente possibile interrompere il rapporto con il DPO per motivazioni diverse dallo svolgimento dei compiti che gli sono propri: per esempio, in caso di furto, molestie sessuali o di altro genere, o altre analoghe e gravi violazioni deontologiche.

Conflitto di interessi

In base all'art. 38, paragrafo 6, del Regolamento al DPO è consentito di "*svolgere altri compiti e funzioni",* ma a condizione che il titolare o il responsabile del trattamento si assicuri che *"tali compiti e funzioni non diano adito a un conflitto di interessi".*

Ciò significa, in modo particolare, che un DPO non può rivestire, all'interno dell'organizzazione del titolare o del responsabile, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali.
Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare o responsabile.

A seconda delle attività, delle dimensioni e della struttura organizzativa del titolare o del responsabile, si possono indicare le seguenti buone prassi:
- individuare le qualifiche e funzioni che sarebbero incompatibili con quella di DPO;
- redigere regole interne a tale scopo onde evitare conflitti di interessi;
- prevedere un'illustrazione più articolata dei casi di conflitto di interessi;
- dichiarare che il DPO non versa in alcuna situazione di conflitto di interessi con riguardo alle funzioni di DPO, al fine di sensibilizzare rispetto al requisito in questione;
- prevedere specifiche garanzie nelle regole interne e fare in modo che nel segnalare la disponibilità di una posizione lavorativa quale DPO ovvero nel redigere il contratto di servizi si utilizzino formulazioni sufficientemente precise e dettagliate così da prevenire conflitti di interessi. Al riguardo, si deve ricordare, inoltre, che un conflitto di interessi può assumere varie configurazioni a seconda che il DPO sia designato fra soggetti interni o esterni all'organizzazione.

M2.13 Compiti generali

Vigilare sull'osservanza del Regolamento

L'art. 39, paragrafo 1, lettera b), affida al DPO, fra gli altri, il compito di sorvegliare l'osservanza del Regolamento.
Nel considerando 97 si specifica che il titolare o il responsabile del trattamento dovrebbe essere "*assistito [dal DPO] nel controllo del rispetto a livello interno del presente 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.

Il controllo del rispetto del Regolamento non significa che il DPO sia personalmente responsabile in caso di inosservanza.
Il Regolamento chiarisce che spetta al titolare, e non al DPO, "*mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento"* (art. 24, paragrafo 1).
Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento, non del DPO.

Il ruolo del DPO nella valutazione d'impatto sulla protezione dei dati

In base all'art. 35, paragrafo 1, spetta al titolare del trattamento, e non al DPO, condurre, ove necessario, una valutazione di impatto sulla protezione dei dati (DPIA, nell'acronimo inglese). Tuttavia, il DPO svolge un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di tale DPIA.

In ossequio al principio di "protezione dei dati fin dalla fase di progettazione" (o *data protection by design),* l'art. 35, secondo paragrafo, prevede in modo specifico che il titolare *"si consulta"* con il DPO quando svolge una DPIA.

A sua volta, l'art. 39, primo paragrafo, 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*".

Il WP29 raccomanda che il titolare si consulti con il DPO, fra l'altro, sulle seguenti tematiche:
- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al Regolamento.

Cooperazione con l'autorità di controllo e funzione di punto di contatto

In base all'art. 39, paragrafo 1, lettere d) ed e) del Regolamento, il DPO deve "cooperare con l'autorità di controllo" e "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 ogni altra questione".

Le linee guida chiariscono che questi compiti attengono al ruolo di "facilitatore" attribuito al DPO nel senso che lo stesso funge 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 ispettivi o connessi all'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'art. 58 del Regolamento.

Approccio basato sul rischio

In base all'art. 39, secondo paragrafo, il DPO deve "*considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo*".

Si tratta di una disposizione di portata generale e ispirata a criteri di buon senso, verosimilmente applicabile sotto molti riguardi all'attività quotidiana del DPO.
In sostanza, si chiede al DPO di definire un ordine di priorità nell'attività svolta e di concentrarsi sulle questioni che presentino maggiori rischi in termini di protezione dei dati.
Seppure ciò non significhi che il DPO debba trascurare di sorvegliare il grado di conformità di altri trattamenti associati a un livello di rischio comparativamente inferiore, di fatto la disposizione segnala l'opportunità di dedicare attenzione prioritaria agli ambiti che presentino rischi più elevati.

Il ruolo del DPO nella tenuta del Registro delle attività di trattamento

L'art. 30, primo e secondo paragrafo, prevede che sia il titolare o il responsabile del trattamento, e non il DPO, a "*tenere un registro delle attività di trattamento svolte sotto la propria responsabilità*" *ovvero "un registro di tutte le categorie di trattamento svolte per conto di un titolare del trattamento".*

Nella realtà, sono spesso i DPO a realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali.
È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali nonché sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'Ue.

L'art. 39, primo paragrafo, contiene un elenco non esaustivo dei compiti affidati al DPO. Pertanto, niente vieta al titolare o al responsabile del trattamento di affidare al DPO il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare stesso.

Tale registro va considerato uno degli strumenti che consentono al DPO di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare o del responsabile.

Attività

Conoscere tutti gli aspetti organizzativi dell'azienda o ente: il DPO deve necessariamente analizzare ed approfondire il core business dell'azienda o comunque i compiti e le funzioni fondamentali dell'ente che assiste. Tale attività è fondamentale per consigliare nel modo migliore il titolare o responsabile del trattamento.

Mappare e classificare i trattamenti dati con un occhio particolare ai dati che vengono trasferiti all'estero ed a eventuali accordi di carattere contrattuale (binding corporate rules).
In genere questo tipo di attività viene svolto attraverso la diretta compilazione dei registri delle attività di trattamento che, come già si è avuto modo di vedere, per quanto considerate a livello di Regolamento attività proprie del titolare e del responsabile del trattamento, alla fine vengono svolte dallo stesso DPO, più che altro, per ragioni di opportunità.

Individuare un organigramma privacy e prevedere un coordinamento funzionale, ai fini privacy, tra i diversi uffici della realtà organizzativa. Si tratta di un aspetto delicato ma fondamentale che può consentire allo stesso DPO di individuare con immediatezza eventuali problematiche che dovessero insorgere nell'ambito dell'azienda o ente.

Prevedere specifiche policy del trattamento dei dati e fornire attività di consulenza in tale settore con un'attenzione particolare rivolta all'utilizzo delle nuove tecnologie (videosorveglianza, biometria, Rfid, big data, uso della rete per attività di marketing, profilazione, posta elettronica aziendale, sistemi automatici decisionali ed utilizzo dell'IA, tecnologie robotiche, cloud computing, IoT, ecc.).

Analizzare l'impatto delle predette nuove tecnologie in ambito protezione dei dati personali al fine di fornire specifica consulenza al titolare del trattamento per la predisposizione di un DPIA.

Aiutare il titolare del trattamento nel predisporre un'efficace politica di sicurezza informatica.
A tal fine sarà necessario dare utili suggerimenti in merito anche alla definizione di programmi di formazione ed aggiornamento per tutti gli operatori (autorizzati) e naturalmente per i referenti del titolare.

Curare, tramite il titolare del trattamento, i rapporti con gli interessati al fine di fornire risposta adeguata a determinate richieste di chiarimenti in materia o a reclami/ricorsi.

Supportare il titolare del trattamento nella predisposizione di specifici report di data breach e nelle relative comunicazioni agli interessati.

Aiutare il titolare del trattamento nella predisposizione e gestione di specifici audit privacy interni ed esterni.

Mantenersi aggiornati con riferimento alla normativa nazionale ed europea in materia di protezione dei dati personali confrontandosi nel caso anche con altri DPO.

Curare i rapporti con l'Autorità garante su tutte le tematiche che dovessero investire l'azienda o l'ente in materia di privacy.

Monitorare in generale tutte le attività di trattamento dati al fine di assicurare il rispetto della normativa nella specifica realtà organizzativa di riferimento.