La nuova figura del Data Protection Officer

di Gianluca Satta (*)

L'articolo si propone di illustrare brevemente la nuova figura del Data Protection Officer, introdotta dal Reg. UE 2016/679, che sarà obbligatoria a partire dal prossimo 25 maggio 2018. L'analisi affronta tutte le questioni più delicate riguardanti il DPO, dai requisiti per la designazione, alla definizione dei compiti fino agli aspetti contrattuali più rilevanti.

Inquadramento giuridico del Data Protection Officer

Il quadro di riferimento in termini di *compliance* per la protezione dei dati nell'Unione Europea, tracciato dal Reg. UE 2016/679 ("Regolamento Generale in materia di Protezione dei Dati", di seguito anche "RGPD"), ruota attorno al principio di responsabilizzazione (*accountability*). In forza di questo principio, che costituisce l'aspetto più rilevante tra le novità introdotte in tema di *privacy* rispetto all'assetto prima delineato dalla Direttiva UE 95/46/CE, al Titolare del trattamento è affidato il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento (1).

Il Responsabile della Protezione dei Dati - RPD (o *Data Protection Officer* - per brevità, di seguito anche "DPO") è una figura che si colloca al centro di questo nuovo quadro giuridico fondato sul principio di responsabilizzazione, con il ruolo principale di agevolare e accompagnare tutti i soggetti coinvolti nel trattamento dei dati personali verso una corretta osservanza delle norme del Regolamento. Tale complessa funzione si articola in due principali linee direttrici: da una parte, al DPO sono assegnati compiti di controllo e sorveglianza, oltre che di consulenza, nell'ambito dell'organizzazione del Titolare e del Responsabile del trattamento; dall'altra, invece, il DPO deve fungere da interfaccia e da punto di collegamento tra tutti i soggetti coinvolti (dalla base ai vertici dell'organizzazione, fino agli interessati ed alle autorità di controllo).

Nel panorama europeo, la figura del DPO non rappresenta una novità assoluta. Infatti, sebbene non prevista dalla precedente disciplina di cui alla Direttiva 95/46/CE, in numerosi Stati membri la nomina di figure analoghe è divenuta una prassi assai consolidata (2).

Le norme principali sul Responsabile della Protezione dei Dati sono contenute nella Sezione 4, Capo IV del Reg. UE 2016/679; in particolare, l'art. 37 RGPD prevede le condizioni per la designazione obbligatoria del DPO e ne descrive i profili di natura organizzativa, l'art. 38 RGPD, invece, inquadra e definisce la posizione e lo *status* del Responsabile della Protezione dei Dati e, infine, l'art. 39 RGPD delinea i principali compiti assegnati al DPO. Oltre alle citate disposizioni, all'interno di numerose altre norme del Regolamento si rinvengono ulteriori richiami a tale figura, che contribuiscono a tracciarne i profili di collegamento con gli altri adempimenti posti a carico

Note:

(*) Avvocato in Cagliari, cultore in materia di Diritto dell'Informatica presso l'Università degli Studi di Cagliari

(1) In virtù di questa nuova impostazione, oltre a dover adempiere agli obblighi in materia, il Titolare dovrà adoperarsi per documentare e motivare adeguatamente ogni attività e adempimento, in modo tale da essere sempre in grado di dimostrare che tali scelte siano coerenti, corrette e pertinenti.

(2) All'interno degli ordinamenti dei Paesi europei si rinvengono figure dai contorni molto simili quali, ad esempio, il *Responsable de seguridad* in Spagna e il *Correspondant Informatique et Libertés* (CIL) in Francia; con l'applicazione del nuovo Regolamento, secondo alcune indicazioni delle stesse autorità di controllo competenti, queste figure andranno ad essere assorbite da quella nuova del DPO.

dei Titolari e dei Responsabili del trattamento (3).

Nel panorama europeo, la figura del DPO non rappresenta una novità assoluta: in numerosi Stati membri la nomina di figure analoghe è una prassi assai consolidata.

Le regole per la designazione del DPO

Il Regolamento ha previsto tre distinti casi in cui la nomina del DPO è obbligatoria, secondo tre differenti criteri: nel primo rileva la qualificazione giuridica soggettiva del Titolare del trattamento, mentre nei restanti due casi le condizioni per la nomina obbligatoria sono determinate da specifiche caratteristiche del trattamento effettuato.
In primo luogo, il DPO deve essere nominato quando "il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, ad eccezione delle autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali" (4). Le nozioni di "autorità pubblica" e di "organismo pubblico" non sono definite nel Regolamento, pertanto, per una corretta interpretazione è necessario far ricorso ai principi generali dell'ordinamento; in linea di massima, l'obbligo di nominare il DPO si estende a tutti soggetti pubblici e le Pubbliche amministrazioni (5). L'obbligo di nomina non si estende nel caso di esercizio di funzioni pubbliche da parte di soggetti privati, come nel caso dei concessionari di servizi pubblici; tuttavia, per tali soggetti è fortemente raccomandato procedere alla nomina del DPO, quantomeno con riferimento a tutti i trattamenti di dati personali aventi finalità connesse all'espletamento delle funzioni pubbliche (6).
Proseguendo nell'ordine dettato dall'art. 37 RGPD, la nomina del DPO è altresì obbligatoria quando "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" (7). Per meglio comprendere la portata di tale disposizione normativa, è opportuno definire meglio le nozioni di "attività principali", di "monitoraggio regolare e sistematico" e, infine, di "larga scala". Con la prima locuzione, si intendono tutte le operazioni essenziali, necessarie al raggiungimento degli obiettivi perseguiti dal Titolare o dal Responsabile del trattamento (8), mentre restano escluse tutte le attività accessorie quali, ad esempio, i trattamenti di dati personali finalizzati al pagamento delle retribuzioni al personale o alla predisposizione di una struttura *standard* di supporto informatico alle attività principali. Il concetto di "monitoraggio regolare e sistematico", invece, si riferisce principalmente a tutte le forme di tracciamento e profilazione su *Internet*, anche per finalità di pubblicità comportamentale (9). Secondo i criteri definiti dai Garanti Europei (WP29) (10) il monitoraggio si considera "regolare" quando avviene in modo continuativo, ovvero a intervalli definiti, quando è ricorrente o ripetuto a intervalli

Note:
(3) A tal proposito, è opportuno fare chiarezza su alcuni termini che potrebbero generare un potenziale rischio di sovrapposizione e confusione nel lettore; in particolare, il riferimento è al termine "Responsabile del trattamento", soggetto delegato dal Titolare del Trattamento allo svolgimento di attività a lui spettanti, disciplinata dall'art. 28 RGPD, infelicemente somigliante al termine "Responsabile della Protezione dei Dati (RPD)" che, invece, corrisponde alla traduzione italiana del termine *Data Protection Officer*. Per meglio comprendere le differenze tra le due figure, si richiama quanto illustrato, a proposito del Responsabile del trattamento, nell'articolo di cui al precedente numero della presente rivista. Cfr. G. Satta, "Regolamento Privacy: novità e punti fermi della nuova disciplina", in questa *Rivista*, n. 2/2018.
(4) Art. 37, par. 1, lett. a), RGPD.
(5) Si considerano tali: le Amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti, e così via. Un valido riferimento normativo per una corretta individuazione degli enti rientranti nella categoria delle Pubbliche amministrazioni, è dato dall'art. 1, comma 2, del D.Lgs. 30 marzo 2001, n. 165.
(6) Cfr. FAQ n. 1 in "Nuove FAQ sul Responsabile della protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29 in Allegato alle Linee guida sul RPD)" pubblicata sul sito *web* del Garante per la protezione dei dati personali (www.garanteprivacy.it).
(7) Art. 37, par. 1, lett. b), RGPD.
(8) Tale interpretazione discende dal considerando n. 97 del RGPD, in cui si afferma che "le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria".
(9) In proposito, è doveroso precisare che l'attività di monitoraggio richiesta dalla norma, non deve necessariamente svolgersi in ambienti *on line*, ma può anche riguardare attività *offline*.
(10) Gruppo di lavoro art. 29 in materia di protezione dei dati personali, "Linee-guida sui responsabili della protezione dei dati (RPD)" adottate il 13 dicembre 2016 - Versione emendata e adottata in data 5 aprile 2017. Traduzione a cura del Garante per la protezione dei dati personali - Unità Documentazione Internazionale e Revisione UE.

costanti oppure quando è costante a intervalli periodici; mentre si considera "sistematico" quando avviene con metodi predeterminati, organizzati, strategici, ovvero nell'ambito di un progetto complessivo di raccolta di dati (11). Infine, con il termine "larga scala" il legislatore ha inteso estendere l'obbligo del DPO solo nei casi in cui le attività principali di monitoraggio sistematico e regolare abbiano ad oggetto "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" (12). L'assenza di un riferimento normativo preciso, rende impossibile definire *a priori* la quantità di dati oggetto di trattamento o il numero di interessati ricompresi nel concetto di "larga scala"; per queste ragioni, l'ampia zona grigia dovuta all'assenza di parametri valutativi precisi, comporta la necessità per il Titolare del trattamento di ricorrere ad un'attenta valutazione d'impatto nella quale documentare le ragioni per le quali ritiene o meno di procedere alla nomina del DPO (13).

L'ultimo caso di nomina obbligatoria del DPO, si ha quando "le attività principali del titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10" (14). Ferme le argomentazioni già svolte in merito ai criteri di interpretazione di "attività principale" e di "larga scala", la nomina obbligatoria è richiesta anche quando il trattamento ha ad oggetto determinate categorie di dati. Nello specifico, si tratta dei dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (15), nonché dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza (16).

Definito l'ambito applicativo dell'obbligo di designazione del *Data Protection Officer*, occorre preliminarmente chiarire che tale vincolo grava sia sul Titolare del trattamento che sul Responsabile del trattamento. La presenza di entrambe le figure, quali destinatarie del precetto, è volutamente prevista al fine di ricomprendere anche tutti quei casi in cui, sebbene l'attività principale del Titolare non rientri nelle casistiche previste dall'art. 37 RGPD, una parte dei servizi e dei relativi trattamenti sono delegati ad un Responsabile del trattamento esterno il quale, invece, svolgendo tali attività per professione, potrebbe ricadere nell'obbligo di designazione del DPO (17).

In presenza di situazioni complesse, come nel caso delle forme imprenditoriali articolate su gruppi di imprese, per agevolarne l'organizzazione il legislatore ha previsto la possibilità di designare un unico Responsabile della Protezione dei Dati, a condizione che il soggetto nominato sia facilmente raggiungibile da ciascuno stabilimento (18). Analogamente, per

Note:

(11) A mero titolo esemplificativo, si possono considerare ricadenti in questa casistica, tutti i trattamenti finalizzati al *marketing* basato sull'analisi dei dati raccolti, alla profilazione e *scoring* per finalità di valutazione del rischio (per esempio, valutazione del rischio creditizio, definizione dei premi assicurativi), al tracciamento dell'ubicazione (per esempio, da parte di *app* su dispositivi mobili), trattamenti finalizzati alla realizzazione di programmi di fidelizzazione o di pubblicità comportamentale oppure trattamenti mediante telecamere a circuito chiuso. Si badi bene, però, che la nomina del DPO è richiesta quando tutte queste operazioni costituiscono "attività principale" del Titolare o del Responsabile del trattamento.

(12) Cfr. considerando n. 91 RGPD.

(13) Considerando il numero di interessati, il volume dei dati, la durata dell'attività di trattamento e la portata geografica dell'attività, ancora una volta a titolo esemplificativo, si possono considerare su larga scala: i trattamenti eseguiti dalle strutture ospedaliere sui dati dei pazienti nell'ambito delle ordinarie attività; i trattamenti relativi agli spostamenti di utenti di un servizio di trasporto pubblico (per esempio, attraverso il tracciamento mediante i titoli di viaggio); infine, i trattamenti di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale.

(14) Art. 37, par. 1, lett. c), RGPD.

(15) Cfr. art. 9 RGPD.

(16) Cfr. art. 10 RGPD.

(17) È il caso, ad esempio, di una piccola azienda operante nel settore vendite che si serve di un'agenzia pubblicitaria, Responsabile del trattamento esterno, che fornisce loro 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 dell'agenzia non generano trattamenti di dati "su larga scala", in considerazione del ridotto numero di clienti e della gamma relativamente limitata delle attività; tuttavia, il Responsabile del trattamento, operando per conto di numerosi clienti, svolge, nel suo complesso, trattamenti su larga scala e pertanto soggetto all'obbligo di nomina del DPO.

(18) Con il termine "raggiungibile" si intende che il DPO deve rappresentare un punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente e che devono essere garantite forme di

(segue)

venire incontro alle difficoltà organizzative e anche di carattere economico delle Pubbliche amministrazioni, tenuto conto della loro struttura organizzativa e dimensione, è consentita la nomina di un unico DPO per più autorità pubbliche o organismi pubblici (19).
Quando il Titolare del trattamento ritiene di non ricadere in uno dei tre casi, sin qui esaminati, non dovrà procedere alla designazione del DPO; tuttavia, è bene evidenziare che, in virtù del principio di *accountability* stabilito nel Regolamento, anche in caso di mancata nomina del DPO al Titolare del trattamento è consigliabile documentare il proprio processo valutativo, così da poter dimostrare che l'analisi effettuata abbia preso in esame in modo corretto tutti i fattori pertinenti (20).
Infine, il Titolare del trattamento che, pur non essendo tenuto alla nomina obbligatoria, opta per la nomina facoltativa del DPO, sarà comunque soggetto a tutte le regole previste dal Regolamento per la sua nomina, ivi compresi i profili legati alla selezione, alla designazione, all'inquadramento del Responsabile della protezione dei dati, che saranno oggetto di approfondimento nei successivi paragrafi.

Ruolo e compiti particolari

I compiti affidati al DPO, oltre ad essere elencati analiticamente dall'art. 39 del Regolamento, sono determinati anche dal Titolare del trattamento il quale, nell'esercizio della propria autonomia organizzativa, può decidere di affidare al DPO delle funzioni diverse, integrative di quelle già previste dalla legge, purché non in contrasto con lo spirito e il ruolo stesso del DPO.
In particolare, procedendo nell'ordine, il DPO ha il dovere di informare e fornire consulenza al Titolare o al Responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi in materia di protezione dei dati, previste dal Regolamento e da altre disposizioni normative (21).
L'altro compito, di particolare interesse per il rapporto con il principio di responsabilizzazione alla base del nuovo impianto normativo, è quello di sorvegliare sull'osservanza del Regolamento e delle altre norme in materia di protezione dei dati personali, ivi compresi i profili di attribuzione delle responsabilità, nonché la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo (22). Per poter espletare queste funzioni, quindi, il Titolare del trattamento dovrà considerare l'opportunità di garantire al DPO designato, quantomeno, l'accesso a tutte le informazioni riguardanti i trattamenti e gli adempimenti eseguiti.
Il DPO, inoltre, è tenuto anche a cooperare con l'autorità di controllo (in Italia, l'Autorità Garante per la protezione dei dati personali) oltre che a fungere da punto di contatto con quest'ultima per questioni connesse al trattamento, come nel caso della consultazione preventiva (art. 36 RGPD) o in altri casi quali, ad esempio, in occasione di ispezioni o controlli (23). Per queste ragioni, al fine di consentire lo svolgimento di tale funzione, è previsto l'obbligo da parte del Titolare di pubblicare e comunicare all'autorità di controllo i dati di contatto del soggetto designato quale DPO.
Il *Data Protection Officer* svolge un ruolo determinante, non solo nella sorveglianza e nella consulenza, ma anche nell'esecuzione di alcuni adempimenti interni spettanti al Titolare del trattamento. Nello specifico, l'art. 39 del Regolamento assegna al DPO il compito di fornire, su richiesta, un parere in merito alla valutazione d'impatto sulla protezione dei dati (DPIA) e di sorvegliarne lo svolgimento (24). Tuttavia, pur non essendo previsto dalla normativa, considerata la centralità della funzione del Registro delle attività di trattamento (art. 30 RGPD) nell'ambito del quadro generale degli adempimenti interni, è consigliabile affidare al DPO anche il compito di cooperare, in termini di affiancamento o di monitoraggio, nelle attività di redazione, tenuta e aggiornamento del registro stesso.
Infine, il DPO assume anche un ruolo importante nel rapporto verso l'esterno, in quanto può essere incaricato anche di riscontrare le richieste e le

Note:
(continua nota 18)
comunicazioni agevoli per gli interessati, ivi compreso il profilo della lingua utilizzata, in caso di trattamenti effettuati in contesti internazionali.
(19) Cfr. art. 37, par. 2 e 3, RGPD.
(20) In particolare, tale principio discende dall'obbligo previsto dall'art. 24 RGPD, secondo cui il Titolare "mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento".
(21) Art. 39, par. 1, lett. a), RGPD.
(22) Art. 39, par. 1, lett. b), RGPD.
(23) Art. 39, par. 1, lett. d) e e), RGPD.
(24) Art. 39, par. 1, lett. c), RGPD.

istanze degli interessati per tutte le questioni relative al trattamento dei propri dati personali e all'esercizio dei diritti loro riconosciuti dal Regolamento (25).

Requisiti e qualità professionali richiesti al DPO

L'attività sottesa alla scelta del soggetto che andrà a ricoprire l'incarico di *Data Protection Officer* non è scevra di vincoli normativi. Secondo il Regolamento, il DPO deve essere designato in funzione delle qualità professionali, delle conoscenze specialistiche della normativa e delle prassi in materia di protezione dei dati personali e, infine, della capacità di assolvere ai compiti a lui affidati (26).
Sebbene il livello di conoscenze specialistiche e le qualità professionali richieste al DPO non siano tassativamente definite, la loro valutazione dovrà necessariamente essere rapportata al grado di sensibilità, complessità e alla quantità dei dati e dei trattamenti sui quali il DPO dovrà operare, nonché in funzione delle capacità di ottemperare ai compiti previsti dal Regolamento.
Come si è avuto modo di apprezzare nel paragrafo che precede, il DPO rappresenta una figura chiave per la promozione della cultura della protezione dei dati all'interno dell'azienda o dell'ente, e contribuisce a dare attuazione a tutti i principi fondamentali e ai diritti degli interessati previsti dal Regolamento. Il DPO assume un ruolo importante anche nell'esecuzione di tutti gli adempimenti, compresa la protezione dei dati secondo il paradigma della "*data protection by design and by default*", i profili di sicurezza del trattamento e la gestione delle procedure di notifica delle violazioni dei dati personali (il c.d. *data breach*).
Alla luce di ciò, per una corretta valutazione delle conoscenze specialistiche, oltre alla normativa e alle prassi in materia di protezione dei dati personali, è opportuno considerare anche i percorsi formativi e le pregresse attività professionali svolte dal DPO, ivi comprese le conoscenze in merito ai settori del diritto coinvolti nell'ambito delle attività del Titolare del trattamento e complementari alla disciplina in materia di protezione dei dati personali.
Infine, a comprova della trasversalità nel ruolo del *Data Protection Officer*, nella valutazione della capacità di assolvere ai compiti previsti dal Regolamento, considerate le notevoli implicazioni di natura tecnico-informatica connesse al trattamento dei dati, non si può prescindere dal considerare con favore anche il possesso di competenze tecniche in materia di sicurezza e trattamenti in ambito informatico, specifiche per le esigenze e le caratteristiche dell'attività del Titolare del trattamento.

Gli aspetti contrattuali e la posizione del Responsabile della Protezione dei Dati

Il ruolo strategico riconosciuto al DPO, richiede una particolare cautela anche nella collocazione funzionale del soggetto nominato, in modo tale da garantire l'efficace assolvimento di tutti i compiti che la legge gli attribuisce. A tal fine, lo stesso Regolamento ha previsto alcune regole specifiche con l'obiettivo di garantire il coinvolgimento attivo del DPO nell'ambito dell'organizzazione e degli adempimenti *privacy*, in condizioni di autonomia e indipendenza, e in assenza di conflitti di interesse.
In primo luogo, per garantire l'effettiva partecipazione nelle scelte interne del Titolare del trattamento, il legislatore ha introdotto l'obbligo a carico di quest'ultimo di coinvolgere tempestivamente e adeguatamente il DPO in tutte le questioni riguardanti la protezione dei dati personali (27). In tal senso, una misura organizzativa adeguata è rappresentata dalla possibilità di prevedere che, per impostazione predefinita (ovverosia di *default*, mutuando il paradigma già citato), il Responsabile della Protezione dei Dati sia sempre invitato a prendere parte alle delibere del *management* di livello medio/alto o, quantomeno, ogni qual volta debbano essere assunte decisioni impattanti sulla protezione dei dati personali. Inoltre, per garantire un adeguato coinvolgimento e, allo stesso tempo, dimostrare il rispetto di tale obbligo, sarebbe opportuno prevedere delle procedure interne che stabiliscano le modalità e i casi di consultazione del DPO nonché la formulazione di adeguate motivazioni ogni qual volta si intenda

Note:
(25) Cfr. art. 38, par. 4, RGPD.
(26) Cfr. art. 37, par. 5, RGPD.
(27) Cfr. art. 38, par. 1, RGPD.

operare in modo difforme dalle raccomandazioni del DPO.
Secondo un altro requisito, è richiesto al Titolare e al Responsabile del trattamento di sostenere il DPO fornendo tutte le risorse necessarie per assolvere ai propri compiti, per accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica (28). Le modalità di assegnazione delle risorse, intese in senso generale, devono essere valutate anche in funzione dell'ulteriore obbligo di garantire l'effettiva autonomia e indipendenza (29), nonché l'assenza di conflitti di interessi (30) nella designazione della figura del DPO.
In termini più specifici, le risorse necessarie da destinare al DPO non sono solamente di natura finanziaria, ma anche di tipo logistico, infrastrutturale e organizzativo. Quanto alle risorse economiche, potrebbe essere utile destinare un *budget* di spesa concordato, purché sia sufficiente e tale da garantire una vera indipendenza dai vertici. Le risorse di natura logistica, infrastrutturale e organizzativa, invece, devono essere adeguate e tali da consentire al DPO di operare al meglio; in questo senso, ad esempio, sin dal momento della nomina, è opportuno valutare il tempo (in termini di ore di lavoro) che il DPO potrà destinare allo svolgimento dei compiti a lui assegnati, i livelli di priorità delle attività da compiere, la possibilità di affiancare del personale di supporto (anche attraverso la costituzione di un *team*) ed eventualmente l'organizzazione di un ufficio dotato di tutte le strumentazioni necessarie, il tutto tenuto conto della dimensione e della complessità della realtà in cui il DPO è chiamato ad operare.
Quanto agli aspetti contrattuali, sotto un profilo organizzativo va preliminarmente precisato che il *Data Protection Officer* può essere sia un dipendente del Titolare o del Responsabile del trattamento sia un soggetto esterno (31). Nel primo caso, sarà sufficiente un atto di nomina interno, mentre nel secondo caso dovrà essere stipulato un vero e proprio contratto di servizi con una persona fisica o giuridica esterna all'ente o all'azienda Titolare o Responsabile del trattamento.
Il contenuto dell'atto di designazione, in ogni caso, deve sempre prevedere e regolamentare ogni singolo aspetto della figura del DPO: dalla definizione analitica dei compiti assegnati, all'organizzazione, alla durata della nomina, nonché tutti i diritti e gli obblighi delle parti (32). Inoltre, come previsto dal Regolamento (33), si dovrà prevedere l'obbligo per il DPO nominato di mantenere assoluta segretezza e riservatezza in merito alle informazioni conosciute nell'adempimento dei propri compiti.
In conclusione, un breve accenno meritano gli aspetti legati alla responsabilità giuridica del *Data Protection Officer*, anche con riferimento alle altre figure *privacy*. Sebbene l'utilizzo del termine "responsabile" potrebbe far sembrare il contrario, il Responsabile della Protezione dei Dati non risponde personalmente in caso di inosservanza degli obblighi e degli adempimenti previsti dal Regolamento. L'onere di assicurare il rispetto della normativa in materia di protezione dei dati, infatti, ricade sul Titolare del trattamento (ed eventualmente anche sul Responsabile del trattamento) il quale è l'unico soggetto giuridicamente responsabile in caso di violazione degli obblighi previsti dal Regolamento. Il DPO, nell'ipotesi meno favorevole, potrà essere ritenuto giuridicamente responsabile nei soli limiti di quanto consentito dal contratto o dal rapporto con il Titolare o Responsabile del trattamento.

Note:

(28) Cfr. art. 38, par. 2, RGPD.
(29) L'art. 38, par. 3, RGPD dispone che: "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 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. Il Responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del Responsabile del trattamento".
(30) L'art. 38, par. 6, RGPD prevede che: "Il Responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il Responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi".
(31) Cfr. art. 37, par. 6, RGPD.
(32) In attuazione degli obblighi di indipendenza, previsti dall'art. 38, par. 3, RGPD, il contratto o la nomina non potranno prevedere la rimozione o la risoluzione ingiustificata del soggetto incaricato in rapporto alle attività svolte in quanto DPO. Cfr. nota 31.
(33) Cfr. art. 38, par. 5, RGPD.