DIRITTO D'IMPRESA, Privacy

Data protection officer interno o esterno? Il DPO sarà una figura strategica per ogni tipo di organizzazione, non affidiamola al caso

di **Andrea Lisi**

https://www.anorc.eu/

Si discute moltissimo in questi giorni della figura del Data Protection Officer o Responsabile della protezione dei dati personali (in seguito DPO o RPD). Una figura che, come sappiamo, è stata introdotta nel sistema normativo europeo dal GDPR (General Data Protection Regulation - Regolamento UE 2016/679), la cui nomina è stata resa obbligatoria per alcuni Titolari e Responsabili del trattamento[1] ed è, comunque, caldamente consigliata, in termini di buone prassi, in tutti i casi in cui, nell'esercizio delle attività di trattamento, siano ravvisabili concreti rischi per i diritti e le libertà delle persone fisiche (in attuazione del fondamentale principio dell'accountability).

A questa delicata figura e ai compiti alla stessa attribuiti sono già stati dedicati alcuni approfondimenti[2]. Eviterò, quindi, di dilungarmi su ciò che è stato ampiamente trattato (spesso in modo compilativo) sia da altri autori, sia (in modo dettagliato) nelle Linee Guida sui Responsabili della protezione dei dati del Gruppo di lavoro art. 29 in materia di protezione dei dati personali (in seguito citate come Linee Guida RPD).

Ciò che mi interessa, in questa sede, è invece riflettere con attenzione su quanto sia effettivamente diverso il DPO/Responsabile della protezione dei dati personali dal Responsabile del trattamento, così come disciplinato dal nostro Codice per la protezione dei dati personali e, soprattutto, così come è stato recepito nell'esperienza di molte realtà aziendali.

L'obiettivo di questa analisi è quindi quello di valutare, con adeguata ponderazione, in che misura lo stesso Responsabile del trattamento previsto, oggi, dall'art. 28 del GDPR, vada a collimare con l'omologa figura definita e interpretata, fino a questo momento, nel nostro diritto vivente.

In realtà, come già sappiamo, la figura del RPD non costituisce in ambito europeo un'assoluta novità. La direttiva 95/46/CE, nella sua genericità di fonte a efficacia indiretta, prevedeva espressamente le sole figure giuridiche dei Titolari e degli Incaricati, lasciando agli Stati membri ampio margine di manovra, alla luce delle criticità specifiche e del livello di complessità riscontrabile in materia di trattamento dei dati personali nei rispettivi ordinamenti, tenendo anche conto delle prassi di enti pubblici e privati.

Nonostante l'assenza di specifici obblighi posti dalla direttiva 95/46, alcuni Stati europei hanno deciso già da tempo di prevedere espressamente la figura del DPO a presidio delle tipologie più delicate di trattamento dei dati personali. L'Italia, d'altro canto, con il suo Codice per la protezione dei dati personali (contenuto – come sappiamo – nel D. Lgs. 196/2003) ha scelto di affiancare al Titolare del trattamento una figura di Responsabile (interno o esterno) che, per certi versi, sembra discostarsi da quanto è oggi definito (nell'art. 4, par. 1, n. 8)[3] e disciplinato (nell'art. 28)[4] nel GDPR e che racchiude invece molte peculiarità attribuite, dallo stesso Regolamento, al DPO.

Nello specifico il nostro Codice definisce (art. 4, comma 1, lett. g) il Responsabile del trattamento come: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali. Tale definizione non coincide del tutto con quella di Responsabile del trattamento attualmente contenuta nel GDPR, che invece lo considera la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento: definizione che, peraltro, coincide sostanzialmente con quella di semplice "Incaricato" presente nella direttiva 95/46/CE[5].

Quello che si può dunque constatare è che nella fluidità adattiva della direttiva 46, ogni Stato ha potuto agire in base alla propria sensibilità interpretativa e secondo modelli più in linea con il proprio ordinamento giuridico; ciò ha favorito inevitabilmente un approccio piuttosto differente da Stato a Stato su alcuni istituti del "diritto alla privacy" e ha inevitabilmente portato il legislatore europeo ad accettare, con il GDPR, un compromesso necessario a favorire una maggiore uniformità normativa e un miglior coordinamento a livello interpretativo.

Proprio in base alla chiave di lettura appena proposta, il Responsabile del trattamento come, in definitiva, disciplinato nelle sue funzioni e responsabilità dall'art. 28 del GDPR, non coincide esattamente con il nostro "Responsabile del trattamento", definito nell'art. 4 e poi regolato nell'art. 29 del Codice della protezione dei dati personali[6]. Oltretutto, l'astrattezza funzionale degli articoli del Codice ha favorito lo sviluppo di prassi diverse nelle nomine a Responsabili del trattamento, sia orientate verso l'esterno (fornitori di servizi informatici, consulenti, studi professionali etc.) sia verso l'interno (dipendenti con funzioni apicali, dirigenti, etc.) e, benché il Codice precisasse che i compiti affidati al Responsabile dovessero essere analiticamente specificati per iscritto dal Titolare (facendo intendere ad alcuni interpreti che ci fosse sempre la necessità per il Responsabile di dover seguire una sorta di "lista della spesa" dettagliatamente sviluppata e messa in atto dal Titolare), allo stesso modo la sua designazione come figura "preposta" al trattamento dal Titolare ha orientato scelte aziendali più oculate e proattive, tendenti al conferimento di posizioni spesso autonome, consulenziali o anche di auditor in capo a questa importante figura prevista nella nostra normativa.

Nel Codice della protezione dei dati personali, infatti, il Responsabile non agisce solo per conto del titolare, ma è da questi preposto al trattamento, acquisendo quindi la facoltà di sostituirlo nelle scelte, sia all'interno e sia all'esterno dell'organizzazione di riferimento. Del

resto, lo stesso Codice precisa che tale figura debba essere individuata tra soggetti che per: esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Allo stesso modo sancisce che possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

Al Titolare, quindi, è concessa massima autonomia organizzativa nell'affidamento (facoltativo e in forma scritta) dell'incarico in capo a figure di Responsabili adeguate alle specifiche esigenze poste dalle attività di trattamento. Come già ricordato, l'astrattezza della fattispecie del Responsabile del trattamento contenuta nel Codice ha permesso di considerare Responsabili (esterni) del trattamento anche persone giuridiche e, ormai da tempo, la prassi del Garante aveva consentito, entro precisi limiti, anche la subdelega delle relative responsabilità[7].

L'art. 28 del GDPR, a ben vedere, ha ripreso queste figure di Responsabili esterni, mutuando molti concetti dall'esperienza italiana, e dettagliandone (forse in maniera anche troppo particolareggiata), finalità, compiti, responsabilità e modalità di nomina.

Nella attuale figura del DPO, come delineata negli articoli 37-39 del GDPR, non possiamo non riconoscere molti concetti espressi dalle prassi italiane proprio in quei modelli organizzativi che prevedevano (all'interno o all'esterno di organizzazioni complesse) figure di confine, nominate spesso "Responsabili del trattamento", che assumevano con una certa autonomia, di volta in volta, compiti di assistenza, consulenza, auditing e così via.

Sostanzialmente - come previsto nel nostro Codice per il Responsabile del trattamento - il DPO contenuto nel GDPR deve, secondo l'art. 37 par. 5, essere 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[8].

Considerati i numerosi compiti di questo "super consulente privacy" e anche la posizione a esso conferita dall'art. 38 del GDPR[9], è ovvio che debba esser garantita a questa figura una conoscenza specialistica della materia attraverso percorsi di formazione dedicati e vanno, pertanto, verificate con attenzione quelle proposte di formazione collegate (in modo più o meno indiretto) a processi "certificativi" (più o meno farlocchi), spuntati come funghi nel "mercato della privacy" in quest'ultimo periodo, con inevitabile annessione di mirabolanti promesse di posti di lavoro assicurati come DPO (o figure similari)[10].

Una professionalità così delicata non si può improvvisare, né si possono mercificare le sue competenze.

Il DPO va, infatti, considerato come un manager del cambiamento digitale (che è il presupposto su cui è fondato l'intero GDPR) che deve acquisire conoscenze multidisciplinari per poter garantire in piena autonomia l'assistenza necessaria ai Titolari e/o Responsabili del

trattamento nella costruzione di adeguati modelli organizzativi che siano, a loro volta, animati dai principi fondamentali della privacy by default e della privacy by design, nell'ambito dell'accountability che permea tutta l'attuale normativa europea.

Per poter assicurare tutto questo è d'obbligo possedere solidissime basi di conoscenza ed esperienza e su questo occorre che ci sia massimo rigore da parte di tutti, nell'interesse del Sistema Paese. Del resto le stesse Linee Guida sul DPO si soffermano molto (pagg. 11-12) nell'illustrare i dettagli delle conoscenze specialistiche, delle qualità professionali e della capacità di assolvere i propri compiti, indicate come presupposti necessari nel già citato art. 37 par. 5 e nel considerando 97 del GDPR[11].

Proviamo a soffermarci infine su un punto molto delicato della nomina del DPO: il requisito dell'autonomia e indipendenza nell'esercizio delle sue funzioni. L'art. 37 par. 6 del GDPR precisa che il Responsabile della protezione dei dati può essere sia un dipendente del Titolare del trattamento (o del Responsabile del trattamento) e sia assolvere i suoi compiti in base a un contratto di servizi. Quindi, come precisato nel considerando 97, tali Responsabili della protezione dei dati, dipendenti o meno del Titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente. In particolare, il par. 3 dell'art. 38 del GDPR stabilisce 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[12]. Il Responsabile della protezione dei dati inoltre non può essere rimosso o penalizzato dal Titolare del trattamento o dal Responsabile del trattamento per l'adempimento dei propri compiti. Il Responsabile della protezione dei dati infine deve riferire direttamente al vertice gerarchico del Titolare del trattamento o del Responsabile del trattamento.

Assicurare piena autonomia nell'esercizio di compiti complessi, all'interno di un modello organizzativo che in parte sembra ricalcare quanto previsto in Italia dal D. Lgs. 231/2002[13] (dedicato – lo ricordiamo - alla responsabilità amministrativa degli enti) e che avvicina il DPO per molti aspetti all'ODV[14], non appare affatto ovvio nell'ambito di un rapporto di lavoro dipendente[15]. Non si può non riflettere su questo.

Appare quanto meno più naturale attendersi, soprattutto in organizzazioni più complesse, lo sviluppo di modelli più strutturati a presidio della privacy e che prevedano dei Team, magari indirizzati e governati da figure parificabili ai "vecchi" Responsabili del trattamento (interni) come previsti dal Codice (e che si spera siano preservati in quell'opera di rivisitazione che il Codice subirà inevitabilmente[16]), i quali potranno/dovranno periodicamente confrontarsi e saranno guidati da DPO esterni competenti e attenti (spesso strutturati a loro volta in team multidisciplinari)[17].

[1] Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, ad eccezione delle autorità giurisdizionali nell'esercizio delle proprie funzioni, 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): così le Linee-Guida sui responsabili della protezione dei dati (RPD) adottate dal Gruppo di lavoro articolo 29 in materia di protezione dei dati personali in data 13 dicembre 2016 (e emendate in data 5 aprile 2017). Inoltre, secondo l'art. 37, quarto paragrafo, il diritto dell'Unione o degli Stati membri può prevedere casi ulteriori di nomina obbligatoria di un RPD.

[2] Utilissimi due Vademecum, uno generale sul GDPR e uno dedicato alle Linee Guida dei Garanti in materia di DPO, scaricabili gratuitamente da qui: https://www.studiolegalelisi.it/dl-department/attivita/item/privacy-3.

Sul DPO si consiglia inoltra la lettura di questo interessante articolo di Michele Iaselli disponibile qui: https://www.anorc.eu/news/item/privacy-istruzioni-operative-sulle-attivita-del-data-protection-officer.

[3] Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

[4] Articolo 28 - Responsabile del trattamento

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il

responsabile del trattamento:

1. a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico
2. b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
3. c) adotti tutte le misure richieste ai sensi dell'articolo 32;
4. d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
5. e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
6. f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
7. g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
8. h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al

paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.
6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.
7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.
8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.
9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.
10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

[5] Infatti, secondo l'art. 2, lett. e) della direttiva, l'incaricato del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento.

[6] Art. 29. Responsabile del trattamento:

1. Il responsabile è designato dal titolare facoltativamente.
2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.
4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

[7] Pratica oggi legittimata definitivamente nei limiti e con i presupposti previsti dall'art. 28 par. 2 e par. 4 del GDPR.

[8] Art. 39 - Compiti del responsabile della protezione dei dati:

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
2. 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 presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

1. b) sorvegliare l'osservanza del presente 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;
2. 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;

1. d) cooperare con l'autorità di controllo; e
2. 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 qualunque altra questione.
3. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

[9] Articolo 38 - Posizione del responsabile della protezione dei dati:

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto

in tutte le questioni riguardanti la protezione dei dati personali.

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

3. 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.

4. 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 presente regolamento.

5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

6. 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.

[10] Esemplare sul punto l'importante e recentissima presa di posizione dell'Autorità Garante per la Protezione dei Dati su "Regolamento UE e Certificazione in materia di dati personali", acquisibile qui: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6621723. Inoltre, l'Autorità Garante spagnola ha pubblicato i primi di luglio un proprio schema di certificazione del DPO. Maggiori dettagli qui: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Certificacion/

ESQUEMA_AEPD_DPD_PUBLICO_1.0.pdf . Questo schema è un primo (un po' timido) tentativo di definire in modo chiaro i parametri di certificazione per una figura così delicata, ma a mio

avviso in Italia sarebbe utile proporre uno schema ben più rigido e legato alla nostra specifica esperienza in materia (che senz'altro può essere presa come punto di riferimento in Europa e guidare così scelte consapevoli da parte degli altri Stati membri).

[11] Considerando 97: per i trattamenti effettuati da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento. Nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria. Il livello necessario di conoscenza specialistica dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento. Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente.

[12] Questa è l'unica effettiva (pur se molto relativa) differenza tra il DPO e il Responsabile del trattamento dei dati come indicato nella sua genericità dall'art. 29 del Codice. Anche se – a leggere bene l'art. 29 – il legislatore italiano afferma nel comma 2 del citato articolo che "i compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare", ma non precisa che questi compiti debbano essere svolti seguendo precise istruzioni, anzi...

[13] Decreto Legislativo 8 giugno 2001, n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300" pubblicato nella Gazzetta Ufficiale n. 140 del 19 giugno 2001.

[14] Leggasi Organismo di Vigilanza.

[15] Le stesse Linee Guida DPO hanno precisato che occorre prestare massima attenzione a situazioni interne di conflitto di interesse, laddove a pag. 17 affermano che "a grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione del titolare o del responsabile riguardo a ruoli manageriali di vertice (amministratore delegato,responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento".

[16] In proposito rinviamo a questo contributo https://www.anorc.eu/news/item/deleghe-al-go

verno-per-il-recepimento-delle-direttive-europee-e-lattuazione-di-altri-atti-dellunione-europea-legge-di-delegazione-europea-2016

[17] Ovvio che si dovrà prestare massima attenzione nella definizione dei contratti di servizi anche al fine di evitare conflitti di interesse nell'affidamento di queste delicate funzioni e nelle Linee Guida sui DPO ci sono già alcune indicazioni in tal senso.