European Journal of Privacy Law & Technologies



2019/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2019/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it



The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published Online by G. Giappichelli in June 2019
www.ejplt.tatodpr.eu

IL DATA PROTECTION OFFICER: LE CARATTERISTICHE E I CONNESSI PROFILI DI RESPONSABILITÀ

Maria Roberta Perugini e Deborah Caputo

Abstract:

Premesso un breve inquadramento del concreto ruolo e dell'effettiva funzione del Data Protection Officer (DPO), l'articolo analizza i diversi profili di responsabilità (privacy e civilistici) di tale figura in relazione ai trattamenti dell'ente designante (senza però tralasciare alcune riflessioni sui trattamenti che il DPO attua "autonomamente" nel contesto dell'esercizio delle proprie funzioni). In particolare, l'analisi viene condotta prendendo in considerazione due possibili situazioni "patologiche" (e precisamente, inadempimento e conflitto di interessi), evidenziando al contempo le peculiarità ravvisabili a seconda che il DPO sia interno (in quanto dipendente dell'ente designante) o esterno (in quanto consulente incaricato in forza di un contratto di servizi).

Key-words: DPO, Responsabilità

Summary: Introduzione. – 1. Ruolo e funzione del DPO. – 2. Le caratteristiche essenziali del DPO. – 3. Assenza di responsabilità "esterna" del DPO per i trattamenti dell'ente designante e per i trattamenti attuati nell'esercizio delle proprie funzioni. – 4. Responsabilità del DPO per inadempimento: inquadramento del tema – (*Segue*). Responsabilità del DPO per inadempimento: principi applicabili. – 5. Obbligo dell'ente designante di "sostenere" il DPO e conseguenze in tema di allocazione di responsabilità tra designante e DPO. – 6. Profili di responsabilità in caso di DPO in conflitto di interessi: inquadramento. – 7. DPO interno in conflitto di interessi: azioni di prevenzione. – 8. Responsabilità dell'ente per il conflitto di interessi del DPO interno. – 9. DPO esterno in conflitto di interessi: azioni di prevenzione. – 10. Conseguenze del conflitto di interessi in termini di allocazione della responsabilità tra designante e DPO. – 11. Effetti del conflitto di interessi sul contratto di servizi tra privati. – 12. Responsabilità del DPO in conflitto di interesse nominato attraverso gara pubblica.

Introduzione

L'introduzione con il Reg. UE 679/2016 (GDPR) del *Data Protection Officer* (DPO) ha sinora portato in Italia all'adozione di soluzioni perlopiù di

compromesso, poco rispondenti alla normativa o addirittura manifestamente inadempienti sotto diversi profili: conflitti di interesse, incompetenza, assegnazione di mezzi e tempi insufficienti conducono allo svuotamento sostanziale di questo strumento, riducendo l'atto di nomina a mero adempimento formale e dunque al fallimento – sotto questo profilo – del percorso di conformità alle norme del titolare o responsabile del trattamento che si dota del DPO.

Per comprendere l'effettiva portata e le conseguenze di tale mancata conformità è necessario inquadrare la funzione assolta dal DPO nel contesto delle attività di trattamento dell'ente designante e del relativo percorso di *accountability* e, al contempo, individuare le caratteristiche essenziali di questa figura.

In quest'ottica, è utile ricordare che il sistema complessivo introdotto dal GDPR fa perno sulla prevenzione del rischio di violazione di dati personali e dei (connessi) diritti e libertà fondamentali della persona. Affinché tale prevenzione sia adeguata ed efficace, il GDPR ha attribuito ai soggetti attivi del trattamento compiti e obiettivi generali (quali la progettazione, l'attuazione e il controllo del trattamento) e, al contempo, la capacità (e l'onere) di dimostrare che il trattamento attuato è conforme alle norme (art. 5, co. 2 e 25 GDPR): in tale modo è stato procedimentalizzato, in capo a detti soggetti, un principio generale di responsabilità (art. 24 GDPR: l'"*accountability*").

Un siffatto sistema induce l'ente ad adottare misure concrete per "*attuare i principi di protezione dei dati*" (art. 25 – Privacy by design e by default) e "*garantire un livello di sicurezza adeguato al rischio*" (art. 32 – Sicurezza del trattamento), in modo da offrire nella pratica una protezione che sia reale ed effettiva.

Naturalmente, affinché le misure adottate risultino efficaci è necessario che vengano individuate dall'ente autonomamente, in rapporto alle peculiarità del caso specifico, ponendo particolare attenzione al rischio inerente al trattamento e alla natura dei dati da proteggere.

Nel contesto dell'elaborazione, da parte del titolare del trattamento, di un sistema di gestione *privacy* idoneo a minimizzare il rischio, assume pertanto grande rilevanza la nomina (anche volontaria) del DPO, il quale viene a rappresentare un vero e proprio strumento dell'*accountability*, adottabile (obbligatoriamente o volontariamente, a seconda dei casi) dall'ente nel contesto delle azioni volte ad attenuare il rischio di violazione dei dati personali e dei diritti delle persone fisiche.

1. Ruolo e funzione del DPO

Il DPO si configura quale terzo rispetto al titolare o responsabile del trattamento che lo designa: è lo specifico organismo istituito dal GDPR cui è attribui-

to il compito di assistere il titolare/responsabile del trattamento «*nel controllo del rispetto del (...) regolamento*» [1] e che per legge deve svolgere la propria funzione (mista di consulenza, vigilanza e controllo) in assoluta autonomia e indipendenza [2].

È inoltre compito del DPO fungere da interlocutore dell'Autorità Garante e degli interessati per l'ente designante [3] (e «*sorvegliare l'osservanza*» di tutte le norme nonché delle politiche del designante in ordine al trattamento 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*» [4]).

Il DPO è dunque chiamato ad assumere un ruolo chiave nella definizione del percorso di conformità al GDPR dell'ente designante. Ciò malgrado, esso è estraneo al trattamento dell'ente sotto il profilo decisionale e della responsabilità che ne deriva (profili rimessi dalla legge esclusivamente al titolare e al responsabile del trattamento, come si preciserà tra breve).

Si tratta, infatti, di una figura di natura eterogenea rispetto al titolare e al responsabile – in rapporto ai quali si colloca non in posizione alternativa o cumulativa, ma *a latere* –, non rivestendo alcun diretto ruolo attivo nei relativi trattamenti, pur assumendo in rapporto ad essi un fondamentale valore strategico.

---

[1] V. considerando 97 GDPR: «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».

[2] V. spec. art. 38, par. 3 e 6, GDPR.

[3] V. artt. 38, par., e art. 39 GDPR.

[4] V. art. 39, par.1 lett. b, GDPR.

2. Le caratteristiche essenziali del DPO

In ragione della complessità del ruolo e delle funzioni attribuitegli, il DPO dovrebbe: *i)* essere un professionista esperto, dotato di competenze specifiche e specialistiche in materia di protezione dei dati personali, con particolare riferimento alla conoscenza della normativa e delle prassi inerenti [5]; *ii)* possedere essenziali requisiti di indipendenza [6]; *iii)* essere collocato, nel contesto aziendale dell'ente designante, in una posizione tale da riferire al più alto livello gerarchico [7] e da non dare adito a un conflitto di interessi [8].

Le peculiarità che caratterizzano la figura in esame inducono ad alcune riflessioni sui profili di responsabilità che ne scaturiscono.

3. Assenza di responsabilità "esterna" del DPO per i trattamenti dell'ente designante e per i trattamenti attuati nell'esercizio delle proprie funzioni

È innanzitutto necessario chiedersi, da un lato, perché all'autonomia ed indipendenza del DPO nello svolgimento della propria funzione non conseguano responsabilità autonome "esterne" per sanzioni o a titolo di risarcimento dei danni agli interessati, a fronte di una eventuale non conformità alla legge dei trattamenti dell'ente designante; dall'altro lato, se possano individuarsi a carico del DPO – e in che termini e con quali conseguenze – profili di responsabilità "interna", dunque nei confronti dell'ente designante.

Partendo dal primo interrogativo, è un dato di fatto che le conseguenze del

---

[5] V. art. 37, par. 5, GDPR.

[6] V. 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".

[7] V. art. 38, paragrafo 3, GDPR: «Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento». A tale proposito, si ricorda che il "vertice gerarchico" è stato identificato in linea generale dal WP29, nelle proprie "Linee-guida sui responsabili della protezione dei dati (RPD)", [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048] nel CdA: «Al riguardo, l'art. 38, paragrafo 3, prevede che il RPD "riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento". Tale rapporto diretto garantisce che **il vertice amministrativo (per esempio, il consiglio di amministrazione) sia a conoscenza delle indicazioni** e delle raccomandazioni fornite dal RPD nel quadro delle sue funzioni di informazione e consulenza a favore del titolare o del responsabile.» (cfr. par. 3.3. «Istruzioni e [significato di] "adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente»)

[8] V. art. 38, par.6, GDPR.

fallimento dell'ente designante nel relativo percorso di conformità al GDPR ricadono esclusivamente su di esso: infatti, l'art. 83 GDPR prevede sanzioni solo a carico del «*titolare*» e del «*responsabile*» del trattamento mentre non se ne rinvengono rivolte al DPO; parimenti, l'art. 82 GDPR riconduce espressamente la responsabilità per il risarcimento del danno causato da una violazione del GDPR ai soli «*titolare*» e «*responsabile*» del trattamento.

È importante indagare la *ratio* di tale scelta legislativa.

Va considerato che l'ente designante persegue proprie finalità generali di gestione aziendale/istituzionale che comprendono – presupponendolo – il rispetto delle norme applicabili, tra cui l'adempimento dell'obbligo di *conformità* al GDPR: proprio in osservanza di tale obbligo è dovere dell'ente esplicitare in un apposito incarico i compiti assegnati al DPO [9] e fornirgli «*le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*» [10].

Tuttavia in questo contesto, seppure nei limiti fissati dai compiti predefiniti nell'incarico, il DPO determina ed effettua in «*autonomia e indipendenza*», obbligatoriamente in assenza di qualsivoglia «*istruzione*» [11], i trattamenti di dati personali strettamente connessi all'esercizio delle sue funzioni, e dunque per specifiche finalità di assistenza dell'ente e controllo della relativa conformità al GDPR.

Ciò detto, sembrerebbe naturale desumere in capo al DPO una titolarità di tali trattamenti [12], seppure caratterizzata da una evidente correlazione con i trattamenti direttamente imputabili all'ente e finalizzati alla conformità normativa della propria azione, in generale e con specifico riferimento al GDPR.

Va però sottolineato che la stretta correlazione funzionale esistente tra la finalità particolare dei trattamenti effettuati dal DPO e quella generale di conformità alla legge perseguita dell'ente designante è istituita dalla stessa normativa [13], con la conseguenza che la prima appare essere (non altro che) una subfinalità della seconda.

---

[9] V. art. 39 GDPR.

[10] V. art. 38, par. 2, GDPR.

[11] V. art. 38, par. 3 GDPR.

[12] Non vi è difficoltà ad individuare la titolarità del trattamento in capo ad un organo interno di un ente: l'art. 4, n.1 GDPR definisce infatti il «Titolare» quale «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali». Dunque, il presupposto qualificante della titolarità è solo il potere decisionale esercitato nella determinazione dei trattamenti.

[13] Tale correlazione è ben riassunta dal dettato del già citato Considerando 97: «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».

Insomma, la finalità dei trattamenti del DPO è una specificazione di quella generale propria dell'ente stesso (vale a dire, l'adempimento da parte di quest'ultimo dell'obbligo legale di *conformità* al GDPR), che è il solo che ha il potere decisionale sui mezzi per raggiungerla: innanzitutto – nei casi di istituzione volontaria – la stessa decisione di dotarsi del DPO (e se questo debba essere "interno" o "esterno"), poi la definizione dell'ampiezza del relativo incarico, delle iniziative per garantirne indipendenza e autonomia nello svolgimento delle relative funzioni, delle risorse da stanziare, nonché l'istituzione e la regolamentazione dei flussi informativi tra DPO e altri organi / funzioni aziendali, l'adozione di misure di sicurezza tecniche ed organizzative, etc.

Ne discende che il DPO non è soggetto attivo autonomo neppure dei trattamenti da esso attuati nello svolgimento del proprio ruolo; tali trattamenti, infatti, sono imputabili direttamente all'*accountability* dell'ente di riferimento, cui in ultima analisi sono rimesse le decisioni in ordine alle relative finalità e modalità.

L'articolazione dell'incarico da parte del titolare/responsabile diventa così il punto di snodo per il coordinamento tra l'autonomia e indipendenza della funzione di vigilanza rispetto al soggetto vigilato e la necessaria riconducibilità delle attività di trattamento svolte dal DPO nell'alveo di quelle proprie dell'ente designante.

Pertanto, il DPO non assume alcuna diretta responsabilità né per sanzioni né per risarcimenti nei confronti degli interessati per la non conformità dell'ente di riferimento alle norme (neppure se gli inadempimenti sono dipesi da colpa o dolo del DPO).

Parimenti, ricade integralmente sull'ente designante l'obbligo di informare tutti i potenziali interessati della nomina del DPO e dei trattamenti ad esso attribuiti, indubbiamente connessi alle funzioni previste dalla legge [14], in aggiunta alla obbligatoria pubblicazione dei dati del DPO.

4. Responsabilità del DPO per inadempimento: inquadramento del tema

Se il DPO va esente da responsabilità in termini di sanzioni applicabili nel caso di irregolarità o inadempienze agli obblighi in materia di protezione dei dati personali, sotto il profilo della responsabilità "interna" la prospettiva invece appare differente, considerato che: *(i)* tra ente designante e DPO sussiste un rapporto contrattuale; *(ii)* come precisato, per previsione di legge il DPO deve essere un soggetto dotato di competenze specifiche e *conoscenze specialistiche* della materia.

[14] Spec. art. 39 par. 1 lett. b) e c) GDPR.

Occorre pertanto indagare cosa accade nell'ipotesi in cui il DPO svolga i propri compiti senza diligenza, ad esempio fornendo al titolare informazioni e consigli non corretti in merito all'adempimento delle prescrizioni a suo carico o pareri erronei sulla valutazione d'impatto.

La questione va affrontata tenendo in debita considerazione il dovere del designante di "sostenere" il DPO «*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*» [15].

La normativa non effettua distinzioni tra DPO interno o esterno in merito alle modalità e al tenore del sostegno che il designante è tenuto ad offrire. Tuttavia, per esplorare compiutamente le possibili responsabilità del DPO in caso di sua negligenza o imperizia è necessario distinguere il caso del DPO dipendente da quello del DPO esterno, e ciò sia in relazione al livello di diligenza richiesto sia al contenuto dell'obbligo di sostegno gravante a carico del designante.

(*Segue*). Responsabilità del DPO per inadempimento: princìpi applicabili

Con riferimento al DPO "esterno" si ricorda che, in via generale, i parametri di diligenza sanciti dalla legge per valutare la condotta del debitore di una prestazione sono previsti dall'art. 1176 c.c. («*Diligenza nell'adempimento*»), che introduce due parametri: uno generico al primo comma («*Nell'adempiere l'obbligazione il debitore deve usare la diligenza del buon padre di famiglia*») e l'altro specifico/qualificato al secondo comma («*Nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata*»).

In base alla norma citata la condotta del professionista, in ragione delle sue competenze specialistiche, deve essere valutata assumendo come criterio di confronto la preparazione, il possesso di nozioni tecniche e l'attenzione (vale a dire l'accuratezza, la prudenza e la precisione) media che quella determinata professione richiede [16].

---

[15] V. art. 38 par. 2 GDPR.

[16] Sul punto, v. C.M. Bianca, in *Diritto civile*, IV, *L'obbligazione*, Milano, 91. L'Autore definisce la «la diligenza adeguata alla natura dell'attività esercitata» che il debitore deve usare nell'adempimento delle obbligazioni professionali in luogo della diligenza del buon padre di famiglia richiesta per le prestazioni comuni, come «quello sforzo di energie e mezzi mediamente e normalmente richiesto alla categoria professionale a cui il debitore appartiene, che «esprime (...) una misura oggettiva dello sforzo volitivo e tecnico richiesto al debitore». Inoltre, secondo l'Au-

Nel caso del DPO troverà pertanto applicazione il parametro della diligenza professionale di cui al secondo comma dell'art. 1176 c.c., la cui mancata integrazione determina in capo al professionista una responsabilità anche per colpa lieve [17].

---

tore, «la diligenza professionale opera come criterio fondamentale di responsabilità e come criterio di determinazione della prestazione dovuta indicando nel primo caso, lo sforzo che il debitore deve impiegare per evitare l'inadempimento o l'inesattezza dell'inadempimento e, nel secondo caso, il modello di precisione e di abilita tecnica cui il comportamento dovuto deve conformarsi». Si veda anche A. Perullo, *Il lavoro autonomo*, in *Trattato di diritto civile e commerciale diretto da Cicu e Messineo*, XXVII, t. 1, Milano 1996, p. 580 ss., che ritiene che il dovere di attenzione si rapporti sempre con quello «medio» di una determinata categoria professionale di appartenenza, dovendosi intendere tale diligenza come buona, sebbene non eccezionale, ossia come diligenza qualificata. In giurisprudenza si afferma che, «il prestatore d'opera intellettuale viola il proprio dovere di diligenza, e perciò è inadempiente alle obbligazioni nascenti dal contratto d'opera professionale, quando risulti che agli abbia agito con negligenza, imperizia, imprudenza tali da violare le regole di comportamento alle quali si sarebbe attenuto un ipotetico professionista medio in relazione al caso concreto ed al risultato che le parti si ripromettevano». In giurisprudenza, per la giurisprudenza di merito v. Tribunale Bergamo, 12 marzo 2019, in Pluris, che (pronunciandosi sulla diligenza del professionista avvocato) ha avuto modo di precisare, in termini generali, che il professionista incaricato «nell'espletare la sua attività, deve impiegare la diligenza del professionista di media attenzione e preparazione ex *art. 1176 c.c.*»; Trib. Oristano, 29 novembre 2016, in Pluris che ha precisato che «l'inadempimento del professionista (che nella fattispecie era un avvocato) non può essere desunto senz'altro dal mancato raggiungimento del risultato utile avuto di mira dal cliente, ma deve essere valutato alla stregua della violazione dei doveri inerenti allo svolgimento dell'attività professionale e, in particolare, al dovere di diligenza. Quest'ultimo – trovando applicazione in subiecta materia il parametro della diligenza professionale fissato *dall'art. 1176, secondo comma, c.c.*, in luogo del criterio generale della diligenza del buon padre di famiglia – deve essere commisurato alla natura dell'attività esercitata, sicché **la diligenza che il professionista deve impiegare, nello svolgimento dell'attività professionale in favore del cliente, è quella media, cioè la diligenza posta nell'esercizio della propria attività dal professionista di preparazione professionale e di attenzione media**». Per la giurisprudenza di legittimità v, tra le altre, Cass, 20 novembre 2018, n. 29846, in *Pluris*. La Suprema Corte ha precisato che «le obbligazioni inerenti all'esercizio dell'attività professionale sono, di regola, obbligazioni di mezzi e non di risultato, in quanto il professionista, assumendo l'incarico, si impegna a prestare la propria opera per raggiungere il risultato desiderato, ma non a conseguirlo. Pertanto, ai fini del giudizio di responsabilità nei confronti del professionista, rilevano le modalità di svolgimento della sua attività in relazione al parametro della diligenza fissato *dall'art. 1176 c.c.*, comma 2, che è quello della diligenza del professionista di media attenzione e preparazione in relazione alla prestazione resa".

[17] Sul punto v. App. Milano, 5 aprile 2017, in Boll. Trib., 2017, 23, 1760, che ha precisato che «la diligenza che il professionista deve impiegare nello svolgimento della sua attività è quella media relativa al collega di preparazione professionale e di attenzione medie. La conseguente responsabilità può, quindi, trovare fondamento in una gamma di atteggiamenti subiettivi, che vanno dalla semplice **colpa lieve**, al dolo»; Trib. Monza, 18 settembre 2014, in Pluris, che ha espressamente affermato che «il professionista è tenuto ad eseguire la prestazione con la diligenza e la perizia adeguate alla materia tecnica di competenza (*art. 1176, comma 2, c.c.*) e risponde, in mancanza, anche per colpa lieve.». Per la giurisprudenza di legittimità v. Cass., 24 novembre 2003, n. 17871, in *Mass. Giur. It.*, 2003: la Suprema Corte ha confermato il principio per cui «in materia

Al contempo è importante segnalare, accanto alla norma generale (e in un certo senso ad "integrazione" [18] della stessa), l'art. 2236 c.c., che delimita la responsabilità professionale alle sole ipotesi di dolo o colpa grave quando la prestazione comporta la risoluzione di problemi tecnici di particolare complessità (vale a dire di problemi che trascendono la preparazione media) o novità [19].

La limitazione di responsabilità di cui all'art. 2236 c.c. è però circoscritta solo ai casi di imperizia giustificata dalla particolare difficoltà dei problemi tecnici affrontati, mentre non trova applicazione nei casi di negligenza e imprudenza, nei quali il professionista – essendo sempre operante il livello "alto" di diligenza richiestogli – risponde anche per colpa lieve [20].

Considerata la novità della figura del DPO e la complessità della normativa

---

di esercizio di attività professionale, il professionista è responsabile anche per colpa lieve (*art. 1176, secondo comma, c.c.*), salvo che la prestazione dedotta in contratto implichi la soluzione di problemi tecnici di speciale difficoltà…».

[18] Come precisato dalla giurisprudenza. Si veda, per tutte, Cass., 15 gennaio 2001, n. 499, in *Mass. Giur. It.*, 200.

[19] In tale senso, tra le tante, v. per la giurisprudenza di legittimità Cass., 22 aprile 2005, n. 8546, in *CD* Cedam 2005. La Suprema Corte ha affermato il condiviso principio per cui qualora la prestazione professionale implichi la soluzione di problemi tecnici di particolare difficoltà trova applicazione l'art. 2236 c.c. che prevede una attenuazione della normale responsabilità, nel senso che il professionista è tenuto al risarcimento del danno unicamente per dolo o colpa grave; per la giurisprudenza di merito, cfr. App. Milano, 5 aprile 2017, cit., che ha confermato il principio per cui «qualora la prestazione professionale da eseguire in concreto involga la soluzione di problemi tecnici di particolare difficoltà, la responsabilità deve ritenersi attenuata, configurandosi, secondo l'espresso disposto *dell'art. 2236 c.c.*, solo nel caso di dolo o colpa grave».

[20] In tale senso, si vedano: Cass., 27 ottobre 2011, n. 22398, in *Resp. civ.*, 2011, 12, 860, che ha precisato che, qualora l'inosservanza (che nella fattispecie consisteva nell'inosservanza da parte di un notaio dell'obbligo di espletare la visura dei registri immobiliari in occasione di una compravendita immobiliare) non sia riconducibile a un'ipotesi di imperizia ma a negligenza o imprudenza, «cioè alla violazione del dovere della normale diligenza professionale media esigibile ai sensi del secondo comma dell'art. 1176 c.c.», rileva anche la colpa lieve, non trovando applicazione «la limitazione di responsabilità prevista per il professionista dall'art. 2236 c.c. con riferimento al caso di prestazione implicante la soluzione di problemi tecnici di speciale difficoltà»; Cass., 13 marzo 2007, n. 5846 in *Ragiusan*, 2007, 281-282, 289, che ha affermato in termini generali che «*l'art. 2236 c.c.* (che nei casi di prestazione che implichino la soluzione di problemi tecnici particolarmente difficili, limita la responsabilità del professionista ai soli casi di dolo o colpa grave) non trova applicazione per i danni ricollegabili a negligenza o imprudenza, dei quali il professionista risponde anche solo per colpa lieve. Infatti l'applicazione *dell'art. 2236 c.c.* è circoscritto ai casi di imperizia ricollegabili alla particolare difficoltà di problemi tecnici che l'attività professionale in concreto renda necessario affrontare»; Cass., 19 aprile 2006, n. 9085 in *Mass. Giur. It.*, 2006, che ha osservato che la «limitazione di responsabilità professionale (…) ai soli casi di dolo o colpa grave, ai sensi *dell'art. 2236 c.c.*, attiene esclusivamente alla perizia, per la soluzione di problemi tecnici di particolare difficoltà, con esclusione dell'imprudenza e della negligenza. Infatti anche nei casi di speciale difficoltà, tale limitazione non sussiste con riferimento ai danni causati per negligenza o imprudenza, dei quali [il professionista] risponde in ogni caso».

in materia di protezione dei dati personali, è tutt'altro che da escludere l'applicabilità di tale disposizione per valutare un'eventuale responsabilità del DPO per imperizia.

Passando al caso del DPO "interno", ossia dipendente del designante, per la definizione della sua responsabilità per inadempimento rilevano, oltre ai criteri generali di diligenza già esaminati (art. 1176 c.c.), anche le norme specificamente dettate per i lavoratori subordinati e precisamente l'art. 2104 c.c. («*Diligenza del prestatore di lavoro*»), in forza del quale: «*Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale*».

Sul piano generale, il parametro della diligenza (insieme al criterio dell'osservanza) specifica il contenuto della prestazione di lavoro subordinato e costituisce indice di misura dell'adempimento della prestazione [21], concorrendo a individuare i doveri del lavoratore [22].

Quanto all'intensità della diligenza richiesta, è pacifico in giurisprudenza che l'obbligo di diligenza del lavoratore subordinato debba essere letto con maggiore intensità in ragione della sua qualifica professionale e che quindi varî a seconda della delicatezza e complessità delle mansioni affidate [23].

Da ciò discende che anche l'attività del DPO dipendente deve essere valutata ai sensi del secondo comma dell'art. 1176 c.c., e dunque in forza del criterio di diligenza qualificata.

Ciò ben si concilia con la prospettazione che il GDPR offre di questa nuova figura, quale soggetto dotato di competenze specifiche e qualificate, e con il tenore dell'art. 2104 c.c., che costituisce una specificazione del principio generale stabilito dall'art. 1176 c.c.

Da queste considerazioni emerge che in linea di principio, in caso di prestazione non conforme agli standard professionali di riferimento, il DPO inadempiente all'obbligo di diligenza (nascente dal contratto di lavoro o di servizi) si espone a responsabilità contrattuale *ex* art. 1218 c.c.: il DPO potrà quindi essere chiamato a risarcire il designante dei danni da quest'ultimo subìti per colpa della sua condotta negligente (si pensi, ad esempio, all'inflizione di una sanzione

---

[21] In tale senso v. Galantino, in *Diritto del lavoro*, Torino, 1998, 452.

[22] In tale senso v. F. Carinci, R. De Luca Tamajo, P. Tosi, T. Treu, in *Diritto del lavoro*, II, *Il rapporto di lavoro subordinato*, Torino, 1998, 236.

[23] Sul punto, v., per la giurisprudenza di legittimità, Cass., Sez. Lavoro, 9 ottobre 2013, n. 22965, in *Danno e Resp.*, 2014, 2, 216; Cass., 15 marzo 1977, n. 1037, in *Pluris*; per la giurisprudenza di merito, Trib. Milano, 6 luglio 1996, in *Lavoro nella Giur.*, 1996, 1032. In dottrina, v. F. Santoni, in *Rapporti speciali di lavoro, Il licenziamento discriminatorio del dirigente*, Torino, 1993, 122, secondo il quale la delicatezza delle funzioni dirigenziali esige una diligenza più intensa, da apprezzarsi in relazione allo specifico contenuto del rapporto ed alle mansioni contrattualmente dovute dal prestatore il quale rivesta la qualifica di dirigente.

da parte del Garante, a un eventuale risarcimento corrisposto dal designante all'interessato per errori imputabili al DPO, nonché al danno reputazionale conseguente a certi tipi di *data breach*).

Assume inoltre rilievo nel (solo) caso del DPO "interno" anche una eventuale responsabilità disciplinare [24].

Secondo l'orientamento prevalente della giurisprudenza di legittimità [25], in caso di danni procurati dal lavoratore al datore di lavoro, quest'ultimo in linea generale può chiedere il risarcimento dei danni, avviare il procedimento disciplinare o procedere con entrambi contemporaneamente (sempre che il contratto collettivo di lavoro applicabile alla fattispecie concreta non stabilisca condizioni più restrittive per il datore, ad esempio prevedendo che esso possa chiedere l'indennizzo solo dopo avere adottato il provvedimento disciplinare nei confronti del dipendente negligente).

5. Obbligo dell'ente designante di "sostenere" il DPO e conseguenze in tema di allocazione di responsabilità tra designante e DPO

Appurato che il DPO inadempiente al contratto si espone nei confronti del designante a una responsabilità risarcitoria, è utile svolgere qualche considerazione di carattere pratico in merito al più volte citato "sostegno" del designante, il cui contenuto può influenzare in modo decisivo l'allocazione della responsabilità eventualmente contestata al DPO.

Nella generalità della lettera dell'art. 38 par. 2 GDPR, l'interpretazione del concreto contenuto di questo dovere risulta strumentale per delineare i confini dell'eventuale inadempienza del DPO: è chiaro infatti che la responsabilità di quest'ultimo scema laddove non sia stato messo nella condizione di svolgere il proprio lavoro.

Se pensiamo al DPO esterno, perché questi possa diligentemente adempiere ai propri compiti è certamente necessario che il titolare gli offra un supporto concreto. Per esempio: organizzando i flussi di informazioni e dati necessari per l'espletamento delle sue funzioni, da parte delle funzioni aziendali coinvolte e da e per gli altri organismi di controllo, facendolo assistere alle riunioni ove

[24] V. art. 7 Stat. Lav. Si ricorda che per la corretta corrispondenza tra gravità della infrazione realizzata dal DPO e la sanzione applicabile si deve fare riferimento al contratto collettivo di riferimento.

[25] Sul punto v: Cass., Sez. lavoro, 26 giugno 2000, n. 8702 in *Mass. Giur. It.*, 2000; Cass., Sez. lavoro, 3 febbraio 1999, n. 950, in *Notiz. Giur. Lav.*, 1999; Cass., Sez. lavoro, 7 gennaio 1995, n. 208, in *Giur. It.*, 1996, I, 1, 687; Cass, Sez. lavoro, 5 aprile 1990, n. 2822, in *Mass. Giur. It.*, 1990; Cass., Sez. Lavoro, 29 novembre 1989, n. 5250, in *Mass. Giur. It.*, 1989.

vengono prese le decisioni rilevanti in materia di trattamento di dati personali e coinvolgendolo anche nei tavoli operativi in caso di nuovi progetti nonché garantendogli la possibilità di definire e attuare in autonomia programmi di verifica e controllo delle attività di trattamento dell'ente.

Il costante aggiornamento e il mantenimento di «*conoscenze specialistiche*» non pare invece che possa costituire un obbligo del titolare (o comunque solo del titolare) quando il DPO è esterno. Trattandosi di un professionista, è infatti ragionevole ritenere che l'onere di per sé ricada sullo stesso DPO, restando a carico del designante piuttosto un impegno formale a incentivare il DPO ad aggiornarsi e, quindi, al contempo a consentire ed agevolare la partecipazione del DPO a seminari, corsi e altre occasioni di formazione (ad esempio, indicando al DPO le tematiche in relazione alle quali è necessario un approfondimento poiché di particolare interesse per l'ente).

È naturalmente opportuno che il contratto di incarico del DPO contenga una declinazione pratica, per quanto esemplificativa, dell'obbligo in esame.

Inoltre, pare ragionevole che tra le pratiche utili a fornire al DPO il sostegno richiesto dalla legge debba essere annoverato anche il riconoscimento di un corrispettivo adeguato: un corrispettivo irrisorio, o comunque incoerente con la specialità della competenza e l'impegno richiesti, è sintomo di scarsa considerazione dell'importanza dell'attività del DPO per la propria organizzazione e dunque di un approccio puramente formale al tema.

Quanto al DPO interno, la questione presenta alcune peculiarità (soprattutto in relazione a quelle situazioni di soggetti già dipendenti della società che vengono poi destinati anche a tale incarico).

Non va dimenticato che ricade sul datore di lavoro quello che la dottrina definisce il *dovere di cooperazione* del datore all'adempimento del lavoratore, in applicazione del fondamentale principio di buona fede e correttezza contrattuale (art. 1175 c.c.), che comporta l'obbligo del datore di porre il dipendente nelle condizioni di potere assolvere correttamente al proprio incarico: ad esempio fornendogli gli strumenti idonei, carichi di lavoro proporzionali alle ore, etc.).

In relazione al DPO interno, rilevano quindi contestualmente a carico dell'ente: *(i)* in quanto datore di lavoro, gli obblighi "giuslavoristici" (di formare il proprio personale e di porre lo stesso nelle condizioni – anche organizzative – idonee a esercitare la propria mansione); *(ii)* in quanto designante del DPO, gli obblighi *ex* art. 38 GDPR (di fornire supporto adeguato al dipendente indicando espressamente i compiti attribuiti, le eventuali risorse assegnate per il loro svolgimento, nonché ogni informazione utile in rapporto al contesto di riferimento).

In altri termini, nel caso del DPO dipendente alcuni obblighi (come ad esempio quello formativo) a carico dell'ente/datore di lavoro presentano una duplice base legale, scaturendo in parallelo dal rapporto di lavoro subordinato e

dallo specifico ruolo di DPO che il dipendente ha assunto nell'organizzazione aziendale.

Nel caso poi del DPO interno già dipendente, e dunque già stabilmente inserito nell'organigramma aziendale, il datore di lavoro/designante dovrà prestare particolare attenzione nel rispettare il corretto inquadramento del lavoratore in relazione al contratto collettivo.

È possibile infatti che le ulteriori funzioni assegnate, gli aspetti di autonomia per legge attribuiti al DPO, le competenze professionali altamente specialistiche richieste assumano rilievo in relazione al livello di inquadramento del dipendente scelto, rendendo ad esempio necessario un "avanzamento" per adeguare le mansioni, le responsabilità, l'autonomia decisionale al livello spettante. Naturalmente, tali valutazioni rilevano anche nella individuazione della giusta retribuzione, dovendo il grado responsabilità affidata a un lavoratore costituire uno dei parametri rilevanti. Purtroppo, le prassi attualmente in voga si muovono nel senso opposto, con la conseguenza di attribuire importi irrisori rispetto alla funzione effettiva (potenzialmente non corretti a livello contrattuale) a un soggetto che, *ex lege* e nella sostanza, ricopre invece un ruolo di estrema rilevanza con riferimento alla regolarità dei trattamenti di dati personali aziendali.

6. Profili di responsabilità in caso di DPO in conflitto di interessi: inquadramento

L'altra circostanza in cui la nomina di un DPO può rivelarsi in contrasto con le prescrizioni normative, e dunque foriera di responsabilità, è quella del DPO in conflitto di interessi.

Si tratta di un tema di particolare attualità: la diffusa mancanza di consapevolezza e sensibilità in merito all'effettivo ruolo del DPO conduce nella pratica attuazione della normativa a frequenti fraintendimenti sul posizionamento del DPO nell'ambito dell'organizzazione aziendale dell'ente designante, sulle effettive funzioni di tale soggetto e sul ruolo dallo stesso assunto rispetto ai trattamenti di dati personali effettuati dell'ente e al relativo processo di adeguamento continuativo al GDPR.

Come visto, l'art. 38, par. 6, GDPR dispone che gli enti che lo designano devono «*assicurarsi*» che il DPO non agisca in conflitto di interessi, cioè non svolga funzioni/mansioni tali da dare adito a incompatibilità, trovandosi a controllare situazioni di gestione di dati personali da lui stesso determinate per posizione gerarchica o cui contribuisce o ha contribuito nella sua funzione aziendale o incarico professionale: quelle situazioni in cui, cioè, si trovi ad essere allo stesso tempo controllore e controllato.

Ciò posto, occorre domandarsi cosa succede se il DPO versa in conflitto di

interessi. In particolare, considerato che legge pone su chi nomina il DPO la responsabilità di assicurarsi che il conflitto non vi sia, il DPO in conflitto va esente da responsabilità?

Anche in questo caso le situazioni prospettabili cambiano a seconda che il DPO sia interno o esterno.

7. DPO interno in conflitto di interessi: azioni di prevenzione

Il DPO interno, nella maggior parte dei casi pratici, è un soggetto già dipendente dell'ente che continua a svolgere altre funzioni contestualmente a quella di DPO.

Come evitare in questo caso il conflitto?

Il GDPR omette di dettare specifiche misure per fare fronte al problema, che è coerentemente rimesso all'*accountability* del designante: è evidente che la chiave è una corretta gestione dell'assetto organizzativo aziendale, attività che spetta naturalmente al datore di lavoro (anche titolare o responsabile del trattamento).

Occorrerà quindi che il datore di lavoro, se sceglie il DPO tra soggetti già dipendenti dell'ente, svolga una rigorosa valutazione dell'organigramma della società evitando tra i candidati alla funzione di DPO – oltre a tutte le persone che non abbiano sufficiente esperienza e competenza – coloro che nell'esecuzione delle proprie mansioni lavorative abbiano, o abbiano avuto, influenza sulle decisioni relative al trattamento dei dati personali.

Chiaramente, il datore di lavoro dovrà anche avere cura di non affidare al dipendente DPO, successivamente alla nomina, altri incarichi che implichino la possibilità di assumere decisioni aziendali in materia di trattamento.

Al fine di evitare il concretizzarsi di tali situazioni, il gruppo di lavoro Articolo 29 Working Party (WP29, oggi European Data Protection Board – EDPB) (nelle Linee Guida WP243) e il Garante italiano (nelle FAQ) hanno stilato un elenco delle situazioni tipo in presenza delle quali è elevato il rischio di conflitto di interessi. Per quanto riguarda il settore pubblico si suggerisce ad esempio di evitare di nominare quale DPO, oltre a chi già è investito di ruoli manageriali di vertice, le figure apicali dell'amministrazione con capacità decisionali in ordine alle finalità e ai mezzi del trattamento, ivi compreso il responsabile IT (chiamato ad individuare le misure di sicurezza necessarie) e il responsabile dell'Ufficio di statistica; nel settore privato, si ritiene preferibile evitare di assegnare il ruolo di DPO a soggetti con incarichi di alta direzione (amministratore delegato, membro del consiglio di amministrazione, direttore generale*, etc*.) ovvero funzioni aziendali aventi potere decisionale in ordine alle finalità e alle modalità/ai mezzi del trattamento (direzione risorse umane, direzione marketing, responsabile IT, etc.).

Anche l'European Data Protection Supervisor (EDPS), nel *Position Paper del 30.9.2018* ha esemplificato situazioni di incompatibilità rispetto all'assunzione del ruolo di DPO all'interno di un'organizzazione, sottolineando come l'esistenza del conflitto non si configuri necessariamente in rapporto a una situazione apicale [26].

Va inoltre considerato che il conflitto potrebbe instaurarsi sotto profili anche diversi dalla gestione dei dati personali: per esempio, nel caso di dipendente DPO "polifunzionale" può crearsi un conflitto legato al tempo assorbito dalle diverse funzioni assunte, che rischia di rendere inefficace l'azione del DPO [27]. In tale caso, possono e devono essere adottate prassi e azioni utili a perseguire un assetto organizzativo aziendale idoneo ad evitare l'instaurarsi del conflitto: per esempio, il datore di lavoro potrà indicare preventivamente il tempo destinato all'attività di DPO (compresa la formazione e l'aggiornamento) e quello da dedicare alle altre mansioni affidate.

8. Responsabilità dell'ente per il conflitto di interessi del DPO interno

Quanto alle conseguenze in capo all'ente designante, anche in caso di conflitto d'interessi del DPO esso è l'unico destinatario dell'obbligo di legale di *conformità* al GDPR dei trattamenti di dati personali ad esso riferibili, nel cui contesto si colloca il già richiamato obbligo di "assicurarsi" che il DPO non operi in conflitto di interessi.

Poiché tale risultato, nel caso del DPO interno, è strettamente connesso alle scelte organizzative del datore di lavoro, la responsabilità di un eventuale conflitto non può che essere imputabile esclusivamente al designante, il quale di conseguenza resta soggetto a una sanzione fino a € 10.000.000 o al 2% del fatturato annuo mondiale (ove superiore) [28]. Da un punto di vista pratico, spetterà dunque al datore di lavoro trovare la soluzione organizzativa idonea a prevenire

[26] https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf. V. par. 4.5: «Functions that would in principle be incompatible with the DPO function include high level positions within management, human resources, IT services, medical services, security services, internal audit, etc.» (…) «A conflict of interests may typically also arise (even for lower level positions), (…) when a DPO who is also part of the compliance team must assess compliance checks and related data processing that they have designed».

[27] V. in tale senso EDPS, Position Paper 30.9.2018, par. 4.3: «Experience has shown that part-time DPOs have found themselves in a permanent conflict between allocating time and efforts to their regular tasks as opposed to investing in their DPO duties».

[28] V. art. 83 par. 4 lett. a) GDPR.

o a fare cessare la situazione di incompatibilità (valutando eventualmente la revoca dell'incarico di DPO, ferme restando tutte le cautele di tipo giuslavoristico).

9. DPO esterno in conflitto di interessi: azioni di prevenzione

Passando al DPO esterno, incaricato tramite un contratto di servizi, innanzitutto si deve ricordare che le Linee Guida WP243 hanno precisato la possibilità di affidare tale incarico a un soggetto non persona fisica.

Come prevenire il rischio di conflitto di interessi, in questo caso?

Il WP29 ha indicato da un lato che i compiti del DPO «*potranno essere assolti efficacemente da un* team *operante* [però] *sotto l'autorità di un* [solo] *contatto principale designato*», quindi di una sola persona fisica che funga da «*"responsabile" per il singolo cliente*», per gli interessati e per il Garante; dall'altro lato, che «*è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale* DPO *soddisfi tutti i requisiti applicabili come fissati nel RGPD*» [29].

In ogni caso di nomina di un DPO è comunque consigliabile che il contratto di servizi sia sufficientemente preciso e dettagliato sul punto; ad esempio, è opportuno indicare le garanzie adottate per evitare che il DPO si trovi o venga successivamente a trovarsi in conflitto di interessi e inserire una dichiarazione espressa del DPO in merito all'assenza di incompatibilità (anche in relazione alla disponibilità di tempo o risorse da dedicare, pur in pendenza di altri incarichi per altri titolari), accompagnata dalla relativa garanzia e manleva.

È inoltre raccomandabile – in termini di documentazione di *accountability* e a fini di tutela del designante nei confronti del DPO stesso (*cfr. infra*) – attuare e documentare opportune verifiche.

Quanto al caso di DPO esterno di un ente pubblico, quindi nominato all'esito di un bando di gara, il tema è ancora più rilevante in quanto l'interesse dell'ente a selezionare soggetti dotati di specifici requisiti di affidabilità risponde a un interesse di portata generale.

---

[29] Nello stesso senso l'EDPS, cit., par. 4.4, con riferimento agli "assistant DPOS": «In practice, assistant DPOs not only assist the DPO, but also ensure the continuity of the function in the event of absence of the DPO. Despite the fact that the Regulation does not address the issue of the status of assistant DPOs, the EDPS believes that assistant DPOs should be offered the same guarantees as those provided for in the Regulation as concerns DPOs themselves. The same rules apply also to acting DPOs. The latter shall ensure in an independent manner the internal application of the Regulation, they may not receive any instructions in the performance of their duties, and their selection as acting DPO shall not be liable to result in a conflict of interests between his/her duty as acting DPO and any other official duties».

L'assenza di un conflitto di interessi in capo al candidato alla carica di DPO è un requisito necessario per lo svolgimento dell'incarico e quindi costituirà una condizione necessaria per la partecipazione alla gara. Il concorrente sarà dunque presumibilmente chiamato a dimostrare tale requisito o, quantomeno, a fornire una opportuna dichiarazione sostitutiva di notorietà, ai sensi dell'art. 47 del D.P.R. n. 445/2000, attestante l'assenza di conflitto di interesse.

10. Conseguenze del conflitto di interessi in termini di allocazione della responsabilità tra designante e DPO

Ciò chiarito, bisogna chiedersi cosa potrebbe succede qualora il DPO dovesse omettere di dichiarare l'esistenza di una situazione di conflitto, magari difficilmente conoscibile da parte del Titolare.

Quanto all'allocazione della responsabilità per le conseguenze dannose causate in capo al designante dal conflitto di interessi, valgono i principi generali che disciplinano i rapporti contrattuali: l'art. 1375 c.c. (in forza del quale «*Il contratto deve essere eseguito secondo buona fede*») e più in generale l'art. 1175 c.c. (correttezza del comportamento delle parti in tutti i rapporti obbligatori); e l'art. 1218 c.c. (in forza del quale «*Il debitore che non esegue esattamente la prestazione dovuta è tenuto al risarcimento del danno*»).

In sostanza, la buona fede – che si traduce in una serie di doveri di collaborazione, tra cui l'obbligo di informare di ogni questione che sia rilevante per la controparte – impone al DPO di comunicare l'eventuale incompatibilità al designante, pena la sua responsabilità nei confronti di quest'ultimo. Tuttavia, sotto il profilo risarcitorio assume rilievo anche l'art. 1227 c.c., in forza del quale «*se il fatto colposo del creditore ha concorso a cagionare il danno, il risarcimento è diminuito secondo la gravità della colpa e l'entità delle conseguenze che ne sono derivate. Il risarcimento non è dovuto per i danni che il creditore avrebbe potuto evitare usando l'ordinaria diligenza*».

Traducendo questi principî nel contesto in esame, il designante concorre con il DPO reticente quando non attua idonee verifiche preventive sulla effettiva assenza di conflitto.

Quindi, il designante non può limitarsi a farsi rilasciare dichiarazioni in tale senso da parte del DPO, ma per quanto possibile deve attivarsi per verificarle: ciò è perfettamente coerente con la già ricordata previsione dell'art. 38, par. 6 GDPR, che attribuisce al designante l'onere di "assicurare" che non vi sia conflitto di interessi.

Pertanto, in caso di concorso di colpa il designante non potrà vedersi riconosciuto il danno causato dalla reticenza del DPO oppure otterrà un risarcimento ridotto rispetto al pregiudizio subito; in mancanza di concorso, si deve invece

ritenere che la sussistenza di un conflitto d'interessi "occulto" possa integrare un inadempimento del DPO al contratto che lo lega al designante, con il conseguente riconoscimento del risarcimento del danno procurato a quest'ultimo.

Ciò appare particolarmente rilevante anche in considerazione del fatto che – come detto – l'ente resta comunque soggetto al rischio di sanzione fino a € 10.000.000 (o al 2% del fatturato annuo mondiale ove superiore) [30] nel caso in cui non provveda a nominare il DPO secondo le prescrizioni della legge, e pertanto anche nel caso in cui il DPO non sia indipendente o si riveli in conflitto di interessi.

11. Effetti del conflitto di interessi sul contratto di servizi tra privati

Un ultimo aspetto che è opportuno analizzare riguarda la sorte del contratto di servizi stipulato con il DPO in conflitto di interessi.

In linea generale, un tale accordo potrebbe essere: (a) risolto a fronte di un inadempimento del DPO alle garanzie assunte; (b) annullato, su richiesta del designante, ai sensi dell'art. 1439 c.c. [31]; (c) dichiarato nullo per contrarietà a norme imperative *ex* art. 1418 c.c., mancando in tale caso un requisito inderogabilmente previsto dalla legge [32].

12. Responsabilità del DPO in conflitto di interesse nominato attarverso gara pubblica

Quanto al DPO di un ente pubblico, poiché l'assenza del conflitto di interessi rappresenta un requisito necessario per lo svolgimento dell'incarico, il concor-

[30] V. art. 83, par. 4, lett. a) GDPR.

[31] Ai sensi dell'art. 1439 comma 1 c.c. «il *dolo* è causa di *annullamento* del contratto quando i raggiri usati da uno dei contraenti sono stati tali che, senza di essi, l'altra parte non avrebbe contrattato».

[32] A tale proposito si ritiene condivisibile l'orientamento giurisprudenziale secondo cui «in tema di nullità del contratto per contrarietà a norme imperative, l'area delle norme inderogabili di cui all'art. 1418, comma 1, c.c., ricomprende, oltre le norme relative al contenuto dell'atto, anche quelle che, in assoluto, oppure in presenza o in difetto di determinate condizioni oggettive e soggettive, direttamente o indirettamente, vietano la stipula stessa del contratto ponendo la sua esistenza in contrasto con la norma imperativa». Cfr. sul punto Cass., Sez. Lavoro, 21 aprile 2016, n. 8066, in *CED Cassazione*, 2016 che in applicazione del suddetto principio ha confermato la decisione di merito che aveva ritenuto la nullità di un accordo transattivo relativo al conferimento dell'incarico di direttore generale della RAI illecito perché stipulato in violazione dell'incompatibilità di cui all'art. 2, comma 9, legge n. 481/1995.

rente sarà presumibilmente chiamato a dimostrare tale requisito o quantomeno a fornire una dichiarazione sostitutiva di notorietà attestante l'assenza di conflitto. In base ai principi generali, l'eventuale falsa dichiarazione da parte del DPO rileverà ragionevolmente come causa di annullamento del provvedimento di assegnazione dell'incarico nonché come circostanza di per sé idonea e sufficiente a ledere irrimediabilmente il rapporto fiduciario tra concorrente e appaltante, con la conseguente responsabilità (anche risarcitoria) del candidato DPO nei confronti dell'ente. Peraltro, non si può escludere che una simile circostanza possa comportare anche la segnalazione all'ANAC.