Working Party 29 - Linee-guida sui responsabili della protezione dei dati (RPD) - Versione emendata e adottata il 5 aprile 2017
Sono state pubblicate sul sito del Gruppo di Lavoro Art. 29 le linee-guida aggiornate sul Responsabile della protezione dei dati, alla luce della consultazione pubblica terminata il 15 febbraio 2017. Il Garante per la protezione dei dati personali ha pubblicato in questa pagina la traduzione italiana del testo e in tempi brevi metterà a disposizione una versione aggiornata della scheda informativa.

di Michele Iaselli

LE LINEE-GUIDA SULLA FIGURA DEL RESPONSABILE DELLA PROTEZIONE DEI DATI: ANALISI E CONSIDERAZIONI CRITICHE

Michele IASELLI, avvocato, vicedirigente del Ministero della Difesa, docente a contratto di logica ed informatica giuridica presso l'Università degli Studi di Napoli Federico II, d'informatica giuridica alla LUISS, Pres. dell'Associazione Nazionale per la Difesa della Privacy (ANDIP).

1. Introduzione

Tra le maggiori novità del Regolamento Europeo sulla protezione dei dati personali n. 2016/679 rientra sicuramente la previsione del Data Protection Officer (DPO) o responsabile della protezione dei dati (RPD, acronimo equivalente a DPO), figura di indubbio rilievo le cui competenze, per la verità, non sono state ancora chiarite nel modo migliore dagli organi comunitari. In effetti il DPO rimane una figura controversa che è stata molto discussa in seno alla Commissione Europea. È sicuramente un'importante figura professionale fortemente voluta i cui compiti e responsabilità, però, non sono particolarmente chiari, specialmente avuto riferimento ai rapporti con il titolare del trattamento.
Proprio per questi motivi il WP 29, istituito dalla Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, ha adottato il 16 dicembre 2016 delle linee guida sui responsabili della protezione dei dati, emendate poi il 5 aprile 2017, al fine di chiarire quali debbano essere i requisiti ed i compiti di un DPO e quale dovrà essere in concreto il suo apporto nel campo della protezione dei dati personali di un'unità organizzativa. **Innanzitutto le linee guida chiariscono che alcuni titolari e responsabili del trattamento sono tenuti a nominare un DPO in via obbligatoria**. Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali (dati sensibili).
La figura del DPO non costituisce una novità assoluta. La direttiva 95/46/CE non prevedeva alcun obbligo di nomina di un DPO, ma in molti Stati membri questa è divenuta una prassi nel corso degli anni (v. ad esempio la Germania). Il WP29 ha sempre sostenuto che questa figura rappresenti un elemento fondante ai fini della responsabilizzazione, e che la nomina del DPO possa facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese. Oltre a favorire l'osservanza attraverso strumenti di *accountability (per esempio, supportando o svolgendo valutazioni di impatto e audit in materia di protezione dei dati), i DPO fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente.*

2. Competenze e capacità del DPO

Riguardo poi le competenze e capacità del DPO le linee guida forniscono molti chiarimenti. In base all'articolo 37 del Regolamento, paragrafo 5, il DPO "*è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39*". Nel considerando 97

si prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento. Il livello di conoscenza specialistica richiesto non trova una definizione tassativa; piuttosto, deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il DPO avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche distinguere in base all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea.

L'articolo 37, paragrafo 5, non specifica le qualità professionali da prendere in considerazione nella nomina di un DPO; tuttavia, sono pertinenti al riguardo la conoscenza da parte del DPO della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del Regolamento. Proficua anche la promozione di una formazione adeguata e continua rivolta ai DPO da parte delle Autorità di controllo. È utile la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare; inoltre, il DPO dovrebbe avere sufficiente familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare. Nel caso di un'autorità pubblica o di un organismo pubblico, il DPO dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili. Quando, poi, il Regolamento nell'individuare i requisiti del DPO parla di capacità di assolvere i propri compiti si deve intendere sia quanto è legato alle qualità personali e alle conoscenze del DPO, sia quanto dipende dalla posizione dello stesso all'interno dell'azienda o dell'organismo. Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici; il DPO dovrebbe perseguire in via primaria l'osservanza delle disposizioni del Regolamento.

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

3. Aspetti organizzativi relativi alla funzione del DPO

La funzione di DPO può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna all'organismo o all'azienda titolare/responsabile del trattamento. In tal caso, è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante quale DPO soddisfi tutti i requisiti applicabili come fissati nella Sezione 4 del Regolamento; per esempio, è indispensabile che nessuno di tali soggetti versi in situazioni di conflitto di interessi. Le linee guida suggeriscono, al fine di favorire una corretta e trasparente organizzazione interna, di procedere a una chiara ripartizione dei compiti all'interno del gruppo di lavoro DPO e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi.

Inoltre si ricorda che l'articolo 37, settimo paragrafo, del Regolamento impone al titolare o al responsabile del trattamento

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

Queste sono disposizioni che mirano a garantire che tanto gli interessati (all'interno o all'esterno dell'ente/organismo titolare o responsabile) quanto le autorità di controllo possano contattare il DPO in modo facile e diretto senza doversi rivolgere a un'altra struttura operante presso il titolare/responsabile. D'altro canto, ai sensi dell'articolo 38 del Regolamento, il titolare e il responsabile assicurano che il DPO sia "*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*".
È, difatti, essenziale che il DPO, per far valere le proprie capacità, debba essere coinvolto quanto prima possibile in ogni questione attinente la protezione dei dati. Per quanto concerne le valutazioni di impatto sulla protezione dei dati, il Regolamento prevede espressamente che il DPO vi sia coinvolto fin dalle fasi iniziali e specifica che il titolare ha l'obbligo di consultarlo nell'effettuazione di tali valutazioni.
Altro aspetto fondamentale connesso alla funzione del DPO è rappresentato dalle risorse disponibili. In merito l'articolo 38, secondo paragrafo, del Regolamento obbliga il titolare o il responsabile del trattamento a sostenere il DPO "*fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*".
È quindi necessario: un supporto attivo delle funzioni del DPO da parte del *senior management (per esempio, a livello del consiglio di amministrazione);* l'individuazione del tempo sufficiente per l'espletamento dei compiti affidati al DPO; un Supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale; la Comunicazione ufficiale della nomina del DPO a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'azienda/dell'organismo; l'accesso garantito ad altri servizi (risorse umane, ufficio giuridico, IT, sicurezza, ecc.) così da fornire al DPO supporto, informazioni e input essenziali; la formazione permanente.

4. Compiti del DPO

Le linee guida analizzano anche i compiti del DPO fornendo alcuni utili suggerimenti.

4.1. Vigilare sull'osservanza del Regolamento

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

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità, e
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Il controllo del rispetto del Regolamento non significa che il DPO sia personalmente responsabile in caso di inosservanza.
Il Regolamento chiarisce che spetta al titolare, e non al DPO, "*mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*" (art. 24, paragrafo 1).

Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento, non del DPO.

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

L'art. 35 del Regolamento parla di valutazione d'impatto sulla protezione dei dati che deve essere effettuata dal titolare del trattamento quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
In base all'art. 35, paragrafo 1, spetta al titolare del trattamento, e non al DPO, condurre, ove necessario, una valutazione di impatto sulla protezione dei dati (DPIA, nell'acronimo inglese). Tuttavia, il DPO svolge un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di tale DPIA. In ossequio al principio di "protezione dei dati fin dalla fase di progettazione" (o *data protection by design*), l'art. 35, secondo paragrafo, prevede in modo specifico che il titolare *"si consulta"* con il DPO quando svolge una DPIA. A sua volta, l'art. 39, primo paragrafo, lettera c) affida al DPO il compito di "*fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento*".

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

In base all'art. 39, paragrafo 1, lettere d) ed e) del Regolamento, il DPO deve "cooperare con l'autorità di controllo" e "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione".
Le linee guida chiariscono che questi compiti attengono al ruolo di "facilitatore" attribuito al DPO nel senso che lo stesso funge da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti ispettivi o connessi all'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'art. 58 del Regolamento.

4.4. Approccio basato sul rischio

In base all'art. 39, secondo paragrafo, il DPO deve "*considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo*". Si tratta di una disposizione di portata generale e ispirata a criteri di buon senso, verosimilmente applicabile sotto molti riguardi all'attività quotidiana del DPO. In sostanza, si chiede al DPO di definire un ordine di priorità nell'attività svolta e di concentrarsi sulle questioni che presentino maggiori rischi in termini di protezione dei dati. Seppure ciò non significhi che il DPO debba trascurare di sorvegliare il grado di conformità di altri trattamenti associati a un livello di rischio comparativamente inferiore, di fatto la disposizione segnala l'opportunità di dedicare attenzione prioritaria agli ambiti che presentino rischi più elevati.

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

Come noto l'art. 30 del Regolamento prevede che ogni titolare del trattamento e il suo eventuale rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità e lo stesso discorso vale anche per il responsabile del trattamento. Di conseguenza la stessa disposizione, primo e secondo paragrafo, prevede che sia il titolare o il responsabile del trattamento, e non il DPO, a "*tenere un registro delle attività di trattamento svolte sotto la propria responsabilità*" ovvero "*un registro di tutte le categorie di trattamento svolte per conto di un titolare del trattamento*".
Nella realtà, sono spesso i DPO a realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali. In effetti l'art. 39, primo paragrafo, contiene un elenco non esaustivo dei compiti affidati al DPO. Pertanto, niente vieta al titolare o al responsabile del trattamento di affidare al DPO il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare stesso.

5. Conclusioni

Da quanto è stato esposto in precedenza si evince che il ruolo del DPO è davvero molto delicato poiché funge da punto di raccordo fra il titolare ed il responsabile da un lato e l'Autorità Garante dall'altro. In considerazione, poi, della grande rilevanza che il regolamento comunitario attribuisce alle certificazioni di qualità, **in questo periodo stiamo assistendo a numerosi percorsi di formazione professionale che si concludono con l'acquisizione di specifiche certificazioni sebbene private e proprio per questo motivo il Garante privacy insieme ad Accredia con un comunicato del 18 luglio 2017 ha chiarito che** per quanto tali percorsi formativi possano essere di indubbio interesse al momento le certificazioni di persone, nonché quelle emesse in materia di privacy o data protection eventualmente rilasciate in Italia, **non possono definirsi "conformi agli artt. 42 e 43 del regolamento 2016/679",** poiché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione.
In realtà in ambito nazionale la figura del DPO necessiterà di ulteriori chiarimenti poiché a seguito dei lavori congiunti UNI – UNINFO per la redazione dello standard sui Profili professionali relativi al trattamento e alla protezione dei dati personali è stato redatto un progetto ormai definitivo e di imminente pubblicazione di norma UNI che sicuramente avrà riflessi importanti per il DPO ed in generale in tutto il settore privacy. Il progetto prevede, infatti, diverse figure professionali competenti nel campo della protezione dei dati personali: il manager privacy, lo specialista privacy ed il valutatore privacy, oltre al DPO.

A parere di chi scrive la norma UNI così come è stata predisposta è fuorviante rispetto alla normativa europea e poco aderente alla realtà organizzativa degli enti ed aziende. Innanzitutto come precisato dal legislatore comunitario nel Regolamento UE 2016/679 il DPO è una sola figura professionale con precisi compiti di carattere consultivo e manageriale. Può essere persona fisica o giuridica, ma è individuata come unica figura professionale. **Appare, quindi, inopportuna l'individuazione di tante figure che ruotano intorno al mondo della protezione dei dati personali** che generano una grande confusione in una materia tra l'altro molto delicata. Non bisogna dimenticare, difatti, che esistono anche un titolare del trattamento ed un responsabile del trattamento chiamati direttamente a rispondere in caso di inosservanza del Regolamento. Inoltre, tale norma sarebbe del tutto inapplicabile in realtà aziendali ed anche pubbliche che avranno difficoltà già a prevedere un DPO seppur obbligatorio per ovvie motivazioni di carattere economico ed organizzativo.
Del resto bisogna riconoscere che in un settore così delicato ciò che conta è la specifica preparazione ed esperienza del professionista a prescindere da certificazioni che non sempre possono fornire un'indubbia garanzia di competenza. ©