Il ruolo del DPO nel settore pubblico

A domanda risponde Prof. Avv. Michele IASELLI

29 ottobre 2024 - dalle ore 11.30 alle 12.30

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione
degli Enti Locali
Email info@dpoinrete.it
Numero Verde 800.16.56.54
Web: www.dpoinrete.it
www.asmel.eu

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

La previsione normativa

L’art. 37 del Regolamento prevede che quando:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali, oppure
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9 (dati sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10
il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati (c.d. **data protection officer**).

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

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

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

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

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

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

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

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Molti chiarimenti sulla figura del DPO sono state fornite dalle Linee-guida sui responsabili della protezione dei dati (RPD) del WG 29 adottate il 16 dicembre 2016 ed emendate in data 5 aprile 2017 dalle linee guida dello stesso Garante Privacy nonché dalle FAQ del Garante relative sia al DPO nell'ambito pubblico che a quello nell'ambito privato.

Faq Garante su DPO in ambito pubblico

1. Quali sono i soggetti tenuti alla designazione del RPD, ai sensi dell'art. 37, par. 1, lett. a), del RGPD?
2. Nel caso in cui il RPD sia un dipendente dell'autorità pubblica o dell'organismo pubblico, quale qualifica deve avere?
3. Quali certificazioni risultano idonee a legittimare il RPD nell'esercizio delle sue funzioni, ai sensi degli artt. 42 e 43 del RGPD?
4. Con quale atto formale deve essere designato il RPD?
5. La designazione di un RPD interno all'autorità pubblica o all'organismo pubblico richiede necessariamente anche la costituzione di un apposito ufficio?
6. È ammissibile che uno stesso titolare/responsabile del trattamento abbia più di un RPD?
7. Quali sono gli ulteriori compiti e funzioni che possono essere assegnati a un RPD?

Attività DPO

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

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

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

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

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

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

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

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

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

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

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

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

Maggiori problematiche e suggerimenti

Il DPO deve creare un clima di consapevolezza circa gli aspetti inerenti la protezione dei dati personali nell'ambito della realtà organizzativa di riferimento. Non dimenticare mai di far presente al titolare del trattamento che la formazione del personale è fondamentale.

Il DPO deve contribuire a far crescere quel forte senso di responsabilizzazione nell'ambito dell'articolazione organizzativa del titolare del trattamento coinvolgendo i responsabili delle diverse unità organizzative e dialogando sempre con coloro che sono poi i referenti del titolare. Abbiamo visto che per il DPO interno questa non è un'attività facile, ma va evitato assolutamente qualsiasi contrasto che potrebbe far nascere grosse criticità.

Non dimenticare mai che il lavoro del DPO presenta aspetti di interdisciplinarietà fondamentali. Quindi è necessario curare gli aspetti organizzativi, gestionali, informatici, comunicativi senza dimenticare nulla. Anche piccoli accorgimenti possono aiutare il titolare a rispettare quel fondamentale principio di accountability.
In sede di ispezione il Garante terrà conto anche di queste attenzioni.
Un DPO esterno naturalmente è avvantaggiato sotto questo aspetto, poiché probabilmente è supportato da diversi collaboratori, ma anche il DPO interno, specialmente in realtà organizzative di notevoli dimensioni, deve convincere il titolare del trattamento circa la necessità di costituire un gruppo di diverse professionalità che possano dare una mano al DPO nello svolgimento di questa complessa funzione.

Il DPO deve evitare di limitare i rapporti con la titolarità solo attraverso contatti informali, ma documentare tutto ricorrendo a comunicazioni scritte, predisposizione di verbali di riunione, relazioni, garantendo quella tracciabilità che assume la dovuta rilevanza qualora dovessero sorgere dubbi, incomprensioni specialmente conseguenti a problematiche ispezioni.

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

Fare attenzione all’atto di nomina/designazione per il DPO interno oppure al contratto per il DPO esterno poiché spesso non ci si attiene ai classici compiti del DPO, ma si chiede anche qualcosa in più. Naturalmente se il compenso è commisurato all’incarico ricevuto che ben venga, ma è necessario che il DPO sappia bene quali sono le ulteriori attività che gli vengono chieste al fine di evitare problemi successivi di incomprensione.

Nel caso di DPO esterno evitare di accettare incarichi con compensi irrisori o comunque non adeguati che sviliscono la professionalità e rischiano di banalizzare un lavoro che invece è molto complesso.
Per lo stesso motivo nel caso di DPO interno rifiutare categoricamente l'incarico quando lo stesso non ha carattere di esclusività ma viene condiviso con altre incombenze, in caso contrario, il rischio è che le attività cui il DPO è chiamato finiscano per essere trascurate a causa di conflitti con altre priorità.

Aiutare il titolare ad inquadrare correttamente quei rapporti di contitolarità, responsabilità ex art. 28 del GDPR o comunque anche quei casi di titolarità autonoma che spesso vengono poco considerati. La giusta impostazione delle posizioni soggettive consente poi di evitare errori e facilitare la definizione dei diversi rapporti. In questa attività potranno essere molto utili le recenti linee guida del Comitato europeo sulla protezione dei dati personali.

Best practices

- Accessibilità del DPO
- Indipendenza operativa e gestione dei conflitti
- Allocazione di risorse adeguate
- Formazione continua
- Integrazione strategica nelle decisioni
- DPIA
- Comunicazione trasparente