fieldfisher

Il nuovo regolamento europeo sulla privacy - GDPR (Reg. UE 2016/679)

Il DPO, una nuova figura?

Avv. Francesca Gravili

Milano, 11 ottobre 2017

Studio Associato Servizi Professionali Integrati

Panoramica della riforma

Regolamento 679/16
In vigore dal 25 maggio 2016 – si applica dal 25 maggio 2018

- rafforza i diritti dei singoli
- crea meccanismi di tracciabilità che imporranno alle aziende di allocare al loro interno le responsabilità nel trattamento dei dati personali.
- impone sanzioni pesanti commisurate al fatturato delle aziende

Studio Associato Servizi Professionali Integrati

Panoramica della riforma - Principi generali e novità

- Privacy by design e Privacy by default
- Il principio dell'Accountability
- Data breach
- Rafforzamento della tutela delle persone fisiche
- Le sanzioni

Il Data Protection Officer - DPO

Responsabile della protezione dei dati personali - spesso indicato con l'acronimo inglese **DPO (Data Protection Officer)**

Riferimenti

1. GDPR
2. Linee guida sui responsabili della protezione dei dati (Gruppo di lavoro art. 29 in materia di protezione dei dati) adottate il 13 dicembre 2016 ed emendate il 5 aprile 2017
3. Scheda informativa del Garante Privacy

Studio Associato Servizi Professionali Integrati

La centralità del Responsabile della protezione dei dati personali

Chi è obbligato a nominare il DPO?

a) **enti pubblici**, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) titolari del trattamento le cui attività principali consistono in trattamenti che per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico** degli interessati su larga scala; o
c) titolari del trattamento le cui attività principali consistono nel trattamento, su larga scala, di **categorie particolari** di dati personali (art. 9) o di dati relativi a condanne penali e reati di cui all'articolo 10 GDPR.

Studio Associato Servizi Professionali Integrati

La centralità del Responsabile della protezione dei dati personali

Esempi di trattamenti su larga scala (dalle Linee Guida WP 29)

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala (dalle Linee Guida WP 29)

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Studio Associato Servizi Professionali Integrati

La centralità del Responsabile della protezione dei dati personali

1. La nomina del DPO riguarda enti pubblici ed aziende private; titolari e responsabili del trattamento dei dati
2. La nomina è obbligatoria nei casi previsti dal GDPR ma gli Stati membri possono ampliare queste ipotesi con proprie norme
3. La determinazione circa l'obbligatorietà della nomina presuppone un'adeguata valutazione preliminare, da tracciare
4. Anche se non obbligatoria, la nomina del DPO è consigliata per i benefici in termini di accountability, effettività e vigilanza
5. Nei gruppi aziendali, la scelta tra un unico DPO o molteplici dipende dalla valutazione di effettività del ruolo e mansioni
6. La designazione è bene che avvenga con delibera del CdA, in analogia all'OdV 231

Studio Associato Servizi Professionali Integrati

La centralità del Responsabile della protezione dei dati personali

Designazione del DPO

- Il DPO è designato dal Titolare e dal Responsabile del trattamento
- Il DPO è **designato per iscritto** con analitica elencazione dei compiti e responsabilità, cioè tutti quelli previsti dal GDPR più eventualmente quelli oggetto di specifica delega di funzioni (proprie) da parte del Titolare (o del Responsabile)

Studio Associato Servizi Professionali Integrati

La centralità del Responsabile della protezione dei dati personali

FAQ

DPO INTERNO O ESTERNO?
Vantaggi

DPO INTERNO
- ✓ conoscenza del contesto e del modello organizzativo
- ✓ maggiore familiarità e partecipazione ai flussi informativi interni
- ✓ costante presenza in azienda

DPO ESTERNO
- ✓ maggior indipendenza
- ✓ specializzazione autonoma
- ✓ ottimizzazione

Dalla FAQ n. 10 del WP 29 - Linee-guida sui responsabili della protezione dei dati (DPO)
A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione con 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. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un DPO esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati.

Studio Associato Servizi Professionali Integrati

La centralità del Responsabile della protezione dei dati personali

Principali compiti del DPO

- informare e consigliare il titolare, il responsabile e i dipendenti in merito agli obblighi derivanti dal GDPR;
- verificare che la normativa vigente e le *policy* interne del titolare siano correttamente attuate e applicate. In particolare, sorvegliare l'osservanza del GDPR, 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;
- cooperare con le autorità di controllo e fungere da punto di contatto per le autorità stesse.

Studio Associato Servizi Professionali Integrati

La centralità del Responsabile della protezione dei dati personali

focus

Principali compiti del DPO
Data Protection Impact Assessment (DPIA)

- Il titolare o il responsabile dovrebbero consultarsi con il DPO, fra l'altro, sulle seguenti tematiche:
- se condurre o meno un DPIA;
- quale metodologia adottare nel condurre un DPIA;
- se condurre il DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se il DPIA sia stato condotto correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi ai requisiti in materia di protezione dei dati.

Studio Associato Servizi Professionali Integrati

La centralità del Responsabile della protezione dei dati personali

focus

Principali compiti del DPO
Registro delle attività dei trattamenti

In merito al registro delle attività dei trattamenti, la sua tenuta è un obbligo che ricade sul titolare o sul responsabile, e non sul DPO.
Cionondimeno, **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 o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al DPO di adempiere agli obblighi di sorveglianza del rispetto del GDPR, informazione e consulenza nei riguardi del titolare o del responsabile.

Studio Associato Servizi Professionali Integrati

La centralità del Responsabile della protezione dei dati personali

focus

Principali compiti del DPO
Data breach

Il merito ai data breach, il DPO svolge un ruolo chiave nella notifica e comunicazione delle violazioni di dati personali.
Inoltre, si osservi che l'art. 33, paragrafo 3, lettera b) GDPR, ove sono indicate le informazioni da fornire all'autorità di controllo e agli interessati in caso di violazione dei dati personali, prevede che tali informazioni **comprendano anche il nominativo** (e non solo le informazioni di contatto) del DPO.

Studio Associato Servizi Professionali Integrati

La centralità del Responsabile della protezione dei dati personali

FAQ

Quale Curriculum deve avere un DPO?

Il Garante Privacy, nella newsletter del 15 settembre 2017 ha per la prima volta chiarito che i DPO dovranno possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Nella selezione sarà poi opportuno privilegiare soggetti che possano dimostrare qualità professionali adeguate alla complessità del compito da svolgere, magari documentando le esperienze fatte, la partecipazione a master e corsi di studio/professionali (in particolare se risulta documentato il livello raggiunto). Gli esperti individuati dalle aziende ospedaliere, ad esempio, in considerazione della delicatezza dei trattamenti di dati effettuati (come quelli sulla salute o quelli genetici) dovranno preferibilmente vantare una specifica esperienza al riguardo e assicurare un impegno pressoché esclusivo nella gestione di tali compiti.

Studio Associato Servizi Professionali Integrati

La centralità del Responsabile della protezione dei dati personali

Dubbi organizzativi…

Quali sono le risorse/supporti che il Titolare deve mettere a disposizione del DPO?

- supporto attivo della funzione di DPO da parte del senior management;
- tempo sufficiente per l'espletamento dei compiti affidati;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della designazione del DPO a tutto il personale;
- accesso garantito ad altri servizi all'interno della struttura del titolare/del responsabile in modo da ricevere tutto il supporto, le informazioni o gli input necessari;
- formazione permanente.

Studio Associato Servizi Professionali Integrati

La centralità del Responsabile della protezione dei dati personali

Responsabilità del DPO

Il DPO è personalmente responsabile in caso di inosservanza degli obblighi in materia di protezione dei dati?

No, il DPO non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dei dati. Spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento. La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sul titolare / sul responsabile del trattamento.

Studio Associato Servizi Professionali Integrati

Sedi e riferimenti

Milano
Via della Moscova, 3
20121 Milano
Tel. +39 02.80673.1
Fax +39 02.89010836

Bologna
Via della Barca, 19
40133 Bologna
Tel. +39 051.436359
Fax +39 051.6153548

Venezia
Viale Ancona, 26
30172 Mestre (VE)
Tel. +39 041.290571.1
Fax +39 041.2905770

Roma
Via Barberini, 47
00187 Roma
Tel. +39 06.697757.1
Fax +39 06.69775720

Torino
Corso Matteotti, 17
10121 Torino
Tel. +39 011.5119166
Fax +39 011.4407792

E-mail: **info.italy@fieldfisher.com**
Web: **www.fieldfisher.com**