UNA FORMAZIONE DI QUALITÀ PER LE NUOVE SFIDE DELLA PRIVACY

Convegno in occasione della presentazione del
Master universitario di II livello
del Dipartimento di Giurisprudenza
Responsabile della protezione dei dati personali: Data Protection Officer e Privacy Expert

Università Roma Tre – Roma 24 novembre 2015

Avv. Fabio Di Resta – LL.M. – Lead Auditor ISO 27001
Studio legale Di Resta – www.studiolegalediresta.it
Presidente del Centro europeo per la Privacy (EPCE)
www.europeanprivacycentre.eu

Data Protection Officer (DPO)

Responsabile della protezione dei dati personali

Il ruolo di Supervisore Indipendente

Interno

(rapporto di lavoro subordinato – “assunto” o “membro del personale”)

Esterno

(contratto di servizi)

Articolo 35 (Ris. Parlamento europeo 12 marzo 2014)
Designazione del responsabile della protezione dei dati

Il responsabile del trattamento e l'incaricato del trattamento designano sistematicamente un responsabile della protezione dei dati quando:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, oppure
- il trattamento è effettuato da una persona giuridica e riguarda più di 5000 interessati in qualsiasi periodo di 12 mesi consecutivi; oppure
- le attività principali del responsabile del trattamento o dell'incaricato del trattamento consistono in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il controllo regolare e sistematico degli interessati; oppure […]

Tuttavia, si deve trovare un testo condiviso con il Consiglio dell'UE: (Fonte documento DAPIX group del 19 dicembre 2014 e confermato anche nel doc. del 11 giugno 205):

Designazione facoltativa del responsabile della protezione dei dati.

Focus sui principali compiti del DPO
Supervisore indipendente (art. 37)

Sorvegliare l'attuazione e l'applicazione del regolamento e delle altre disposizioni in materia, nonché le politiche del responsabile in materia di protezione dati personali, la sensibilizzazione e la formazione del personale.

Controllare la DPIA (Data Protection Impact Analysis – l'effettuazione delle Valutazione di impatto sulla protezione dei dati), ma deve anche partecipare alla redazione della procedura di valutazione d'impatto (PE) – «Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dati e sorvegliare lo svolgimento» (Consiglio dell'EU versione 11 giugno 2015).

Controllare che le violazioni dei dati personali (c.d. Data Breach Notification) siano documentate, notificate e comunicate.

Sorvegliare l'attuazione e l'applicazione del principio di data protection by design e di quello data protection by default, nonché della sicurezza dei dati.

Elementi caratterizzanti l'indipendenza del DPO (art. 35)

Requisito negativo

- Non incompatibilità con altre funzioni e assenza di un conflitto di interessi

- Non ingerenza nell'esercizio delle sue funzioni da parte del responsabile o incaricato: nessuna «istruzione per quanto riguarda il loro esercizio»

concetto di indipendenza effettiva, nota a livello giurisprudenziale, in particolare, in ambito organizzativo come i Modelli di Organizzazione (c.d. MOGC secondo d.lgs. 231/2001) e i relativi Organismi di Vigilanza

Elementi per la designazione del DPO (art. 35)

- qualità professionali

- conoscenza specialistica della normativa in materia di protezione dei dati personali sulla base di trattamenti dei dati personali effettuati dal Titolare del trattamento

- «pratiche» (*rectius* esperienza) e capacità di svolgere le mansioni assegnate

Elementi di valutazione in base alle best pratice in ambito DPO, nell'ottica di un'effettività di indipendenza:

DPO interno: parti time/full time;
contratto a tempo determinato/contratto a tempo indeterminato;
figura senior/figura junior
«non deve essere penalizzato nell'esecuzione dei propri compiti» (art. 36 co. 3 versione Consiglio EU 11 giugno 2015);

Elementi caratterizzanti l'indipendenza e autonomia del DPO (art. 35)

Requisito positivo (Proposta di Regolamento Generale sulla protezione dei dati)

- Deve avere "tutti i mezzi, inclusi il personale, i locali, le attrezzature e ogni altra risorsa necessaria per adempiere le proprie funzioni e compiti di cui all'art. 37 e per mantenere la propria conoscenza professionale" (vers. PE), «Risorse necessarie per adempiere i propri compiti» (Consiglio UE – 11 giugno 2015)

- Riferisce direttamente ai «superiori gerachici esecutivi» (PE), «massimi superiori gerarchici» (Consiglio UE – 11 giugno 2015)

Elementi di valutazione in base alle best pratice in ambito DPO:

Piena autonomia finanziaria per eseguire i propri compiti o richiesta ad altre funzioni interne o direttamente al Titolare del trattamento

Durata e cessazione dell'incarico

- "Periodo di almeno quattro anni in caso di un contraente di servizi esterno" (PE);
- "il mandato è rinnovabile" (PE);
- "Può essere destituito solo se non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni" (PE);
- "oltre che per gravi motivi i quali, a norma del diritto dello Stato membro interessato, giustifichino la destituzione di un dipendente o di un funzionario pubblico" (versione del Consiglio UE, 11 giugno 2015).

Sanzioni previste

Commissione europea 2012: fino **1 Ml** di Euro o **2 %** di fatturato mondiale annuo

Parlamento europeo 21/11/2013: fino **100 Ml** di Euro o **5 %** di fatturato mondiale annuo

Consiglio dei Ministri UE 11/06/15 (Dapix woking group): fino **1 Ml** di Euro o **2 %** f.m.a.

Riepilogo conclusivo

Il ruolo del responsabile del protezione dei dati personali (DPO) è una forte novità nell'ordinamento italiano

Il DPO rappresenta un'opportunità nel contesto del nuovo regolamento europeo al fine di garantire una maggiore conformità normativa ed effettività di tutela rispetto agli obblighi previsti nel nuovo regolamento europeo

Per soddisfare i requisiti richiesti per il ruolo del DPO è necessario aver effettuato percorsi formativi specialistici e qualificanti oltre ad aver maturato esperienza in materia

Avv. Fabio Di Resta – LL.M. – Lead Auditor ISO 27001
Studio legale Di Resta – [www.studiolegalediresta.it](http://www.studiolegaledresta.it)
Presidente del Centro europeo per la Privacy (EPCE)
www.europeanprivacycentre.eu