CONFINDUSTRIA

Position Paper

Data Protection Officer (DPO): alcuni dubbi del mondo imprenditoriale

Dicembre 2017

1) Nomina del DPO

1.1) In ambito privato, ai fini dell'individuazione dell'obbligo di designare il DPO, rilevano i concetti di: *a)* attività principale; *b)* trattamento di dati personali su larga scala; *c1)* trattamento di categorie particolari di dati ovvero di dati "giudiziari"; *c2)* monitoraggio regolare e sistematico degli interessati.

Considerato che ai fini della nomina obbligatoria i citati fattori devono sussistere congiuntamente, con riferimento al rapporto tra il concetto di attività principale e quello di monitoraggio regolare e sistematico, in che termini lo svolgimento di attività di profilazione o di *marketing basate sull'analisi dei dati raccolti* deve considerarsi *una componente inscindibile* del *core business* del titolare e, quindi, un elemento idoneo a determinare a carico di quest'ultimo l'obbligo di nominare il DPO?

In particolare, è tenuta a nominare il DPO l'impresa che:

- commercializza i propri prodotti e/o servizi ai consumatori con i canali tradizionali e tramite *e-commerce*, con esclusione dell'attività di profilazione dei consumatori ?
- commercializza i propri prodotti e/o servizi ai consumatori con i canali tradizionali e tramite *e-commerce* e previa profilazione del consumatore?
- provvede direttamente alla promozione e alla vendita dei propri prodotti attraverso *attività di marketing basate sull'analisi di dati raccolti*?

1.2) In merito alla designazione di un unico DPO per più organismi, considerato che in un gruppo di imprese è possibile nominare un solo DPO, se questo viene designato dalla società capogruppo, le società controllate e/o collegate che rientrano tra quelle tenute alla nomina del DPO o che intendono avvalersi del DPO devono comunque procedere a una designazione autonoma?

1.3) Quali sono i "fattori pertinenti" su cui il titolare o il responsabile devono fondare l'eventuale scelta di non ricorrere alla figura del DPO (es. tipologia di attività connessa al trattamento dei dati personali; organizzazione interna idonea a presidiare i rischi cui la figura del DPO è preposta)? È possibile predisporre un modello per la documentazione e la rendicontazione di tale decisione?

1.4) In caso di DPO sulla base di un contratto di servizi e della costituzione di un *team*, chi riveste il ruolo di DPO: il cd. contatto principale (v. Linee Guida par. 2.5, ultimo capoverso) o tutti i componenti del gruppo incaricati di svolgere le funzioni di DPO sotto la direzione di un responsabile (v. Linee Guida par. 3.2, penultimo capoverso)

2) Posizione del DPO

Con riferimento alla possibilità di nominare un DPO "interno", viste le incompatibilità individuate dal WP29 rispetto all'amministratore delegato, al responsabile operativo, al responsabile finanziario, al responsabile sanitario, al direttore *marketing*, al direttore risorse umane e al responsabile IT, è possibile attribuire il ruolo di DPO a chi svolge

funzioni di *staff* al *management*, come ad esempio, il legale interno o il responsabile della *compliance legale*?

Sempre in caso di DPO interno, la nomina può ricadere sul dipendente che:

- segue per l'impresa le vicende organizzative e operative per la protezione dei dati personali (es. gestione delle richieste di accesso ai dati, formazione del personale, redazione DPS);
- gestisce l'URP dell'impresa: raccoglie i reclami, i ringraziamenti e li comunica ai soggetti competenti.

Fermo il possesso delle richieste qualità professionali, è possibile affidare il ruolo di DPO all'*internal auditor*? Ai sensi del Codice di Autodisciplina, infatti, l'*internal auditor* garantisce indipendenza (con riporto al consiglio di amministrazione), legame funzionale all'amministratore delegato e assenza di conflitto di interessi.

3) Compiti del DPO

Il DPO può svolgere solo compiti di controllo e vigilanza del sistema privacy adottato dall'impresa oppure può svolgere anche ruoli operativi (es. redazione informative, lettere di nomina)?