DANDRIA - Studio Legale

PRIVACY & DATA PROTECTION BRIEFING

n. 9 del 13 febbraio 2017

DATA PROTECTION OFFICER: LE NUOVE LINEE GUIDA

---

di Francesco Alongi

Il regolamento europeo n. 2016/679 sulla protezione dei dati ("regolamento generale sulla protezione dei dati"), che diventerà direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018, ha introdotto, per determinati soggetti, l'obbligo di nominare un responsabile della protezione dei dati ("Data Protection Officer" o "DPO").

Si tratta di una figura professionale già prevista dalla legislazione di alcuni Paesi europei, i cui compiti includono:

- assistere e consigliare il titolare e il responsabile del trattamento, nonché i dipendenti che effettuano il trattamento dei dati;
- sorvegliare l'osservanza del regolamento e della normativa europea e nazionale applicabile;
- fungere da punto di contatto per le autorità di controllo in relazione a tutte le questioni connesse al trattamento.

Al fine di chiarire in quali casi è obbligatorio designare un DPO, quali sono i suoi compiti e la sua posizione, il 13 dicembre 2016 il Gruppo di lavoro ex articolo 29 ha adottato delle Linee guida sulla figura del responsabile della protezione dei dati[1].

[1] Accessibili all'URL: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf. Il Gruppo di lavoro è un organismo istituito ai sensi dell'art. 29 della Direttiva 95/46/CE, a "carattere consultivo e indipendente", composto da rappresentanti delle autorità di controllo degli Stati Membri, del Garante europeo della protezione dei dati e della Commissione europea.

(I) DESIGNAZIONE DEL DATA PROTECTION OFFICER

Ai sensi dell'art. 37 del regolamento generale sulla protezione dei dati, il titolare o il responsabile del trattamento dovranno obbligatoriamente designare un Data Protection Officer:

1) quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, fatta eccezione per le autorità giudiziarie quando esercitano le loro funzioni giurisdizionali;

2) quando le attività principali del titolare o del responsabile del trattamento consistono in trattamenti che, per la loro natura, ambito di applicazione o finalità richiedono un monitoraggio regolare e sistematico degli interessati su larga scala; oppure

3) quando le attività principali del titolare o del responsabile consistono nel trattamento, su larga scala, di categorie particolari di dati personali (di cui all'art. 9 del regolamento stesso[2]) o di dati relativi a condanne penali e a reati commessi (ai sensi dell'art. 10 del regolamento).

L'art. 37.2 prevede inoltre la possibilità per i gruppi imprenditoriali di nominare un unico responsabile della protezione dei dati, a condizione che il DPO sia agevolmente raggiungibile da ciascuno stabilimento.

Con le sue Linee guida, il Gruppo di lavoro è intervenuto per chiarire alcuni dei termini utilizzati dal legislatore europeo e per formulare alcune raccomandazioni.

In prima battuta, il Gruppo di lavoro ha rilevato che la nozione di "autorità o organismi pubblici" deve essere interpretata sulla base della legge

[2] L'art. 9 del regolamento (Ue) n. 2016/679 fa riferimento ai "*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché* [i] *dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*".

nazionale, raccomandando tuttavia la designazione di un DPO anche da parte delle società o organizzazioni private che svolgono attività o incarichi di rilievo pubblicistico o nel pubblico interesse.

Con riferimento invece alla nozione di trattamento di dati personali su "larga scala" (che comporterebbe l'obbligo di designazione di un DPO), il Gruppo di lavoro ha individuato alcuni fattori che dovrebbero essere presi in considerazione dagli operatori:

- il numero degli interessati coinvolti dal trattamento (quale numero assoluto o quale proporzione della popolazione);
- il volume o la gamma dei dati trattati;
- la durata delle attività di trattamento;
- l'ambito geografico del trattamento.

Con riferimento alla nozione di "monitoraggio regolare e sistematico" degli interessati, le Linee guida rinviano al considerando 24 del regolamento, che fa espresso riferimento al monitoraggio delle persone fisiche su internet e alla profilazione degli interessati "*in particolare per* […] *analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali*". Il Gruppo di lavoro ha inoltre chiarito che il monitoraggio deve considerarsi "regolare" se è costante o se avviene periodicamente o ad intervalli regolari.

Il monitoraggio deve invece considerarsi "sistematico" se effettuato sulla base di un sistema prestabilito, organizzato e metodico, se rientra in un piano generale di raccolta dei dati o se effettuato sulla base di una strategia. Ad esempio, secondo il Gruppo di lavoro rientrano nella nozione di monitoraggio regolare e sistematico i trattamenti effettuati per la gestione di reti di telecomunicazione, le strategie di "email targeting" e di profilazione a fini di valutazione del rischio di insolvenza, la geolocalizzazione attraverso APP telefoniche, le strategie di behavioural

advertising, il monitoraggio delle condizioni di salute degli utenti e la telesorveglianza.

Anche qualora non dovesse sussistere l'obbligo di designare un DPO, il Gruppo di lavoro raccomanda al titolare e al responsabile di trattamento di documentare le valutazioni e le analisi effettuate per determinare se tale obbligo sussiste. Ad ogni modo, se – pur in assenza di un obbligo in tal senso – un'organizzazione decide di nominare un DPO, le sue attività e il suo ruolo saranno disciplinati dalle disposizioni del regolamento generale sulla protezione dei dati.

Ai sensi dell'art. 37.5 del regolamento, il DPO è designato in funzione delle sue qualità professionali (e in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati), e della capacità di assolvere i compiti previsti dal regolamento stesso.

Nelle Linee guida, il Gruppo di lavoro ex art. 29 chiarisce che l'esperienza e le competenze del DPO devono essere commisurate alla delicatezza e alla complessità del trattamento effettuato e al volume dei dati gestiti dall'organizzazione. In ogni caso, il DPO dovrebbe possedere una conoscenza approfondita della normativa nazionale ed europea in materia di protezione dei dati e delle attività economiche svolte dal titolare e dal responsabile del trattamento.

Le qualità personali del DPO devono inoltre includere una spiccata integrità e un'elevata etica professionale, dato che uno dei suoi compiti principali è quello di promuovere lo sviluppo di una cultura rispettosa della normativa sulla protezione dei dati all'interno dell'organizzazione nella quale si trova ad operare.

Ai sensi dell'art. 37 del regolamento, il DPO può essere un dipendente del titolare o del responsabile del trattamento o può assolvere i suoi compiti in base a un contratto di servizi. Sul punto, le Linee guida sono

intervenute per chiarire che se il ruolo di DPO è svolto da un'organizzazione esterna, ciascun membro di tale organizzazione deve rispettare tutti i requisiti previsti dalla Sezione IV del regolamento. Inoltre, tutti i membri dell'organizzazione che svolge le funzioni del DPO devono godere delle tutele previste dal regolamento.

Infine, anche se l'art. 37 del regolamento non prevede alcun obbligo in tal senso, il Gruppo di lavoro raccomanda di comunicare sia all'autorità competente che ai dipendenti della società oltre ai dati di contatti anche il nome del DPO.

(II) IL RUOLO DEL DATA PROTECTION OFFICER

L'art. 38 del regolamento dispone che il DPO deve essere tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati.

Il Gruppo di lavoro ha dunque ribadito l'importanza del coinvolgimento del DPO sin dalle fasi iniziali delle attività che richiedono il trattamento dati. È in particolare necessario fornire tempestivamente al DPO tutte le informazioni necessarie per svolgere le sue mansioni e assicurare la sua partecipazione alle riunioni del management.

Il DPO dovrà essere inoltre prontamente consultato in caso di incidenti o perdite di dati e qualsiasi decisione del management che si discosti dalle indicazioni del DPO dovrebbe essere adeguatamente motivata.

Il Data Protection Officer deve disporre delle risorse necessarie (finanziarie ed organizzative) e del tempo sufficiente per assolvere i suoi compiti e l'intera organizzazione dovrebbe essere messa al corrente del suo ruolo e delle sue funzioni. In ogni caso, le risorse messe a disposizione del DPO dovranno essere commisurate alla complessità delle operazioni di trattamento svolte dall'organizzazione (che potrebbe in alcuni casi rendere necessaria la designazione di un "DPO team").

L'art. 38 del regolamento dispone che "*il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione* [dei suoi] *compiti*". Nelle Linee guida, il Gruppo di lavoro ha chiarito che il DPO non può ricevere istruzioni dai propri superiori sui risultati da raggiungere o sulla necessità di svolgere indagini o di informare le autorità competenti.

Il regolamento dispone inoltre che il DPO non può essere rimosso o penalizzato dal titolare o dal responsabile del trattamento per l'adempimento dei propri compiti. Il Gruppo di lavoro ha chiarito che il divieto previsto dal regolamento si applica anche alle sanzioni indirette, quali ad esempio la mancata o ritardata promozione e l'esclusione dai benefit dei quali godono gli altri dipendenti.

Infine, il regolamento dispone che il titolare o il responsabile del trattamento devono assicurarsi che i compiti e le funzioni del DPO non diano adito a conflitti di interessi. Le Linee guida suggeriscono l'adozione di procedure e regolamenti interni atti a prevenire l'insorgere di tali conflitti.

(III) I COMPITI DEL DATA PROTECTION OFFICER

Ai sensi dell'art. 39 del regolamento, il DPO deve sorvegliare l'osservanza della normativa europea e nazionale relativa alla protezione dei dati. Le Linee guida chiariscono tuttavia che è obbligo del titolare del trattamento (e non del DPO) mettere in atto tutte le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati è effettuato conformemente alla normativa applicabile.

Il Gruppo di lavoro raccomanda inoltre ai titolari del trattamento di consultare il DPO in merito all'opportunità di effettuare una valutazione

d'impatto sulla protezione dei dati o di adottare misure tecniche o organizzative per tutelare i diritti degli interessati. In caso di disaccordo fra titolare del trattamento e DPO, sarebbe inoltre opportuno motivare adeguatamente qualsiasi decisione che si discosti dalle indicazioni di quest'ultimo.

Le Linee guida raccomandano inoltre al DPO di adottare un approccio pragmatico, basato sull'individuazione dei rischi prioritari, e di prestare particolare attenzione alla regolare tenuta del registro delle attività di trattamento dei dati.

***

Il presente briefing non costituisce un parere legale. Per ulteriori informazioni sul tema si invita a contattare l'Avv. Francesco Alongi (falongi@dandria.com).