Il Sole 24 ORE

Il responsabile dei dati? Meglio un esterno

–di **Antonio Montanaro*** - 20 novembre 2018

(Reuters)

L'approvazione da parte dell'Unione europea della nuova Normativa sulla Privacy 2016/679, più comunemente definita GDPR, ha generato non poca confusione. Questo perché il nuovo testo non sostituisce completamente il vecchio codice sulla privacy, ma piuttosto introduce numerose modifiche e nuove regole per le organizzazioni che detengono e trattano dati di persone fisiche residenti nei Paesi dell'Unione. Motivo per cui da maggio 2018 le caselle di posta elettronica dei cittadini comunitari sono state invase da messaggi informativi sull'aggiornamento della normativa.

La confusione che si è creata ha riguardato soprattutto la figura del Responsabile della protezione dei dati, ovvero il DPO (Data protection officer). Il DPO è una figura prevista

dall'art. 37 del Regolamento (UE) 2016/679. Si tratta del soggetto designato dal titolare o dal responsabile del trattamento dati che ha il compito di assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento stesso. Il DPO coopera con l'Autorità e per questo il suo nominativo va comunicato al Garante e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento).
Il DPO deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il Titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve agire in piena indipendenza e autonomia e riferire direttamente ai vertici.
Alla designazione del DPO sono tenuti il Titolare e il Responsabile del trattamento nei casi che rientrano nella previsione di cui all'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679: si tratta di soggetti le cui principali attività consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati. A titolo esemplificativo e non esaustivo sono state individuate la categorie di soggetti certamente tenuti alla nomina del DPO: istituti di credito, società finanziarie, di informazione creditizia e commerciale, società di recupero crediti, partiti politici, sindacati, società del campo delle utilities (distribuzione energia elettrica, gas, telecomunicazioni), della somministrazione del lavoro e della ricerca del personale, società che forniscono servizi informatici, che operano nel settore della cura della salute, etc.
Per alcune categorie la designazione di un DPO non è obbligatoria: sono esclusi a titolo esemplificativo i liberi professionisti operanti in forma individuale, le imprese individuali o familiari, e le piccole e medie imprese con riferimento ai trattamenti dei dati di fornitori e dipendenti. Nonostante questo, è comunque utile procedere alla designazione su base volontaria, come precisato anche dal Garante.

Il DPO dovrà operare in base a un contratto di servizi e tendenzialmente si tratta di una figura professionale esterna alla struttura del Titolare, tuttavia il ruolo può essere ricoperto

anche da un dipendente del titolare o del responsabile (non in conflitto di interessi), mediante specifico atto di designazione, anche se quest'ultima pare essere soluzione incapace di soddisfare completamente i criteri di autonomia ed indipendenza.

(*responsabile "privacy" Studio Martinez & Novebaci)