Il Data Protection Officer: in quali casi è obbligatorio nominarlo.

Il nuovo Regolamento Europeo in materia di protezione dei dati personali, tra le numerose novità introdotte al fine di rafforzare i presidi posti a tutela della riservatezza degli individui, ha tracciato la nuova figura del Responsabile della Protezione dei dati (Data Protection Officer).

A partire dal 25 maggio 2018, un numero elevatissimo di enti pubblici (tutta la Pubblica Amministrazione), enti e società private nonché gli studi professionali, saranno obbligati a individuare e nominare il Data Protection Officer (di seguito D.P.O.), all'interno del proprio organico ovvero all'esterno tramite contratti di outsourcing.

Purtuttavia e nonostante il breve periodo di tempo che ci separa dal termine ultimo entro cui bisogna nominare tale figura, un ristrettissimo numero di istituzioni pubbliche e private si sta occupando o preoccupando di formare il Data Protection Officer, allo stato non paragonabile ad altra figura consulenziale o aziendale già esistente ed operativa. In altri termini, sul mercato italiano delle professioni, ad oggi, non si è in grado, a meno di "forzature" dannose e controproducenti, di riscontrare un profilo professionale dotato delle abilità e competenze richieste dal Regolamento Comunitario.

Secondo la nuova normativa europea, il Data Protection Officer è un professionista aziendale "poliedrico", con competenze giuridiche, informatiche e aziendalistiche¸ tra le quali il profilo legale deve necessariamente prevalere sulle altre figure professionali (l'informatico e l'aziendale).

In buona sostanza, il Data Protection Officer si può definire come il professionista al servizio di vari soggetti istituzionali (azienda, ente, Pubblica Amministrazione, studi professionali ecc. ecc.), la cui mission è **assicurare la protezione del patrimonio informativo aziendale e dei dati personali trattati dagli stessi**. Il DPO avrà una necessaria vocazione giuridica, ma dovrà essere dotato di conoscenze adeguate di natura informatica e aziendale, che saranno supportate dalle figure che opereranno a suo sostegno (i Privacy Officer); egli **costituirà il fulcro di tutti i processi aziendali e degli Uffici incardinati nelle Pubbliche Amministrazioni, in modo trasversale e con concretezza decisionale, a fianco del Top Management, consigliando e sorvegliando sulla corretta applicazione del Nuovo Regolamento Comunitario.**

In pratica, la figura professionale del DPO come sopra delineata ad oggi non è ancora ben inquadrata nel nostro ordinamento giuridico e, allo stato attuale, appare di difficilissima reperibilità, eccezion fatta per rarissimi casi di professionisti che, vuoi per vocazione vuoi per esperienza personale, hanno operato in contesti aziendali connotati dalla trasversalità organizzativa.

Uno degli interrogativi principali che connotano attualmente la discussione in materia riguarda l'individuazione dei casi in cui sia obbligatorio designare il D.P.O., in quanto il Regolamento Comunitario introduce tale obbligo in presenza di ***attività dei titolari del trattamento che richiedono il monitoraggio regolare e sistematico di dati su larga scala.*** Considerata la genericità delle indicazioni fornite dal Regolamento stesso circa l'obbligatorietà o meno di tale designazione per le aziende, e stante invece l'obbligatorietà della designazione per tutte le pubbliche amministrazioni, il Working Party dei Garanti privacy europei ha emanato le linee guida per fornire i chiarimenti in merito.

Quando si configura un monitoraggio regolare e sistematico di dati su larga scala?

I Garanti europei riuniti nel Working Party si sono occupati in via principale di individuare i soggetti destinatari dell'obbligo di designazione attraverso la definizione del concetto di larga scala e di monitoraggio regolare e sistematico.

I fattori connotanti un **trattamento su larga scala** individuati dai garanti europei sono alternativamente:

- il **numero di soggetti interessati dal trattamento**, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- **il volume dei dati** e/o le **diverse tipologie di dati** oggetto di trattamento;
- **la durata**, ovvero **la persistenza**, dell'attività di trattamento;
- **la portata geografica** dell'attività di trattamento.

Mentre per ciò che attiene gli ulteriori due requisiti, ovvero **monitoraggio regolare e sistematico**, essi sono stati così definiti:

- l'aggettivo **regolare** per i garanti indica un trattamento di dati che avviene in modo continuo ovvero ricorrente o ad intervalli periodici;
- l'aggettivo **sistematico** è stato fatto corrispondere ad un trattamento di dati:
  - **che avviene per sistema**;
  - **predeterminato, organizzato o metodico;**
  - **che ha luogo nell'ambito di un progetto complessivo di raccolta dati;**
  - **svolto nell'ambito di una strategia.**

Mediante una lettura sovrapposta del Regolamento e delle citate linee guida, si può credibilmente concludere che siano soggetti all'obbligo di nomina del Responsabile tutte quelle **aziende e quei professionisti che operano su banche dati (clienti, dipendenti e fornitori, consulenti), effettuano attività di marketing attraverso la profilazione online dei clienti, trattano dati sensibili e/o giudiziari, utilizzano apparecchiature tecnologiche di GEOLOCALIZZAZIONE E GEOREFERENZIAZIONE, VIDEOSORVEGLIANZA, CONTROLLO ACCESSI, SISTEMI BIOMETRICI,**

In altri termini, anche alla luce degli esempi riportati nelle citate linee guida dei Garanti Europei, è possibile evidenziare:

- **l'OBBLIGO** generalizzato di nominare i Data Protection Officer **per tutta la PUBBLICA AMMINISTRAZIONE** (vale a dire, tutte le Amministrazioni dello Stato, gli Istituti e Scuole di ogni ordine e grado, le Istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300);

- **<u>l'OBBLIGO</u> di nominare i Data Protection Officer <u>per i seguenti enti privati</u>:**
- Istituzioni finanziarie e istituti di credito;
- Società di recupero crediti;
- Istituzioni e compagnie assicurative;
- Aziende sanitarie private – cliniche, poliambulatori, laboratori analisi cliniche e diagnostiche e altri istituti sanitari;
- Società di servizi / consulenza;
- Centri elaborazione dati e Internet provider;
- Società di somministrazione di pubblica utilità (energia elettrica, acqua, gas, telecomunicazioni);
- Società di trasporti, agenzie di viaggio, strutture alberghiere e ricettive in genere;
- Società commerciali e industriali allorquando trattino una mole di dati personali dei propri dipendenti, clienti, fornitori, consulenti esterni, tale da far ritenere soddisfatto uno dei fattori che connota il trattamento su larga scala[1] (dunque, per un'ulteriore esemplificazione: Società di produzione e/o trasformazione di prodotti ortofrutticoli con 40 dipendenti, 4 unità locali dislocate sul territorio nazionale e dotate di sistemi di videosorveglianza/controlli accessi);
- Studi professionali associati, società di revisione, società tra professionisti.

Considerata la **<u>vastità degli operatori che saranno interessati da tale obbligo</u>** (che ho cercato di delineare a mero titolo di esempio nell'elencazione di cui sopra) nonché della **<u>complessità nel gestire tali adempimenti</u>**, si rende necessario per le aziende nominare – in aggiunta al Data Protection Officer, profilo che sarà probabilmente individuato all'esterno in outsourcing anche per motivi di opportunità – **una ulteriore figura che si occupi dall'interno della società stessa di tali materie, ovvero il Privacy Officer.**

La differenza tra tali due figure sta nel **maggior grado di responsabilità** gravante sul Data Protection Officer, nel suo dover rispondere ai puntuali requisiti tratteggiati dal Regolamento UE, nonché nella **conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati personali**; conoscenze che saranno dimostrate anche mediante il conseguimento o il possesso di specifiche certificazioni. **Il Privacy Officer** dal suo canto, come espressamente chiarito dall'art. 38 del Regolamento[2], **è la risorsa ausiliaria necessaria al Responsabile della Protezione dei dati personali** per assolvere i suoi compiti ed accedere ai dati personali ed ai trattamenti e per mantenere la propria conoscenza specialistica.

[1] Si considerano, in particolare, il numero di potenziali clienti soprattutto se trattasi di persone fisiche e/o se vengono poste in essere attività di marketing/profilazione della clientela, se i dati sono gestiti da un sistema automatizzato in clouding o con server proprietari, oltre che al numero di fornitori e altri soggetti che operano con la società obbligata al DPO. Altro elemento da considerare è poi la portata geografica del trattamento intesa anche quale possibile trasferimento dei dati in Paesi extra-UE, in particolar modo, verso Paesi dove non vigono regole adeguate del rispetto della Privacy come in UE.

[2] <u>Art. 38, co 2, Reg. UE n. 2016/679</u>: Il titolare del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Quali gli scenari futuri?

E' assolutamente necessario formare la nuova figura del Data Protection Officer, non solo perché' costituisce un **obbligo imperativo** del Regolamento Comunitario (la cui mancata ottemperanza determinerebbe l'**irrogazione di pesantissime sanzioni**), ma anche per **scongiurare il possibile impiego di figure provenienti da altri Stati membri dell'UE**, dove la figura del Data Protection Officer già esiste da anni e risultano già ben consolidati i processi operativi che ad essa fanno capo.

Documento a cura di:

Avv. Domenico Vozza

Avvocato stabilito del foro di Roma – Privacy & Compliance Expert

Vice Presidente Ass.Pri.Com.

Blog: www.tuttosullaprivacy.it