

Il DPO è per sempre?

Recentemente il Garante per la protezione dei dati personali ha ordinato al Mise il pagamento di una sanzione di 75mila euro per non avere nominato il Responsabile della protezione dati (Rpd), o – come forse è più conosciuto – il DPO (Data Protection Officer), entro il 28 maggio 2018 (data di piena applicazione del GDPR), e per avere diffuso sul sito web istituzionale informazioni personali di oltre 5mila manager.

Questa notizia, accanto alle ormai quotidiane notizie di data breach sempre più spesso determinate da scarsa consapevolezza sulla protezione dei dati personali, mi hanno portato a sviluppare una serie di riflessioni sul ruolo del DPO che provo a sintetizzare qui di seguito.

Il vero DPO

Prima di tutto **il ruolo del DPO è fondamentale per garantire consapevolezza diffusa sulle politiche di trattamento dei dati personali negli enti pubblici e privati**. È fondamentale garantire informazione e formazione capillare su questi argomenti, perché non c'è misura di sicurezza informatica che tenga di fronte all'approssimazione e al semplicismo dei comportamenti umani!

Abbiamo avuto la prova “certificata” di questa necessità per enti pubblici e privati attraverso un servizio del Tg3 sulla Protezione Civile nel contenimento del virus, dove incredibilmente sono state esposte le password di un presidio sanitario.

Così come è emblematica in tal senso l'esperienza delle tre strutture sanitarie coinvolte in recenti provvedimenti sanzionatori del Garante.

In realtà, **non è importante solo avere il DPO quando è obbligatorio (o è comunque consigliabile dotarsi di questa figura in azienda), ma è essenziale sceglierlo bene**, tra professionisti (o propri dipendenti) che siano preparati, indipendenti e abbiano esperienza adeguata in quel settore di riferimento in cui dovranno operare.

Avere invece – come troppo spesso accade – un “DPO fantoccio”, sottopagato, acquisito per dovere formale all'ultimo minuto – scegliendo così professionisti che replicano quel delicato incarico su più enti senza ritegno e cognizione di causa – è peggio che non averlo!

Credo che sia indispensabile riferire con forza oggi questi concetti e spero pertanto che la nostra Autorità Garante per la protezione dei dati personali possa avviare verifiche approfondite sia su enti pubblici privi ancora oggi di DPO, sia verso DPO totalmente inadeguati e incompetenti che moltiplicano alla rinfusa incarichi sottopagati, contribuendo così ad alimentare una cultura della protezione del dato burocratica, formale e ovviamente non compliant rispetto a ciò che il GDPR pretenderebbe.

Non solo il singolo

Mi occupo di diritto applicato all'informatica, digitalizzazione dei processi (aziendali e amministrativi) e protezione dei dati personali da circa 20 anni. Lo faccio con grande entusiasmo e con quell'attenzione alla qualità che la delicatezza di tali argomenti meritano. Credo fermamente che queste materie vadano affrontate, anche quando si rivestono incarichi di DPO, non in modo solitario ed elitario, **ma favorendo lo sviluppo di team aperti al confronto**, quindi in modo interdisciplinare tra professionalità diverse, determinando così la specifica comprensione delle singole e complesse sfaccettature che la “digitalità” porta con sé.



Amo ripetere che **non ci può essere processo di innovazione digitale senza attenzione alla protezione del dato personale** e mai come in questo periodo stiamo avvertendo sia le innegabili opportunità, sia purtroppo i pesanti rischi che sta comportando l'ingresso del digitale in ogni granello della nostra esistenza.

Infatti, il GDPR non sarebbe entrato così prepotentemente nel nostro ordinamento giuridico se non fossimo stati investiti da una profonda trasformazione sociale, culturale, economica e, quindi, giuridica, frutto dell'epocale passaggio verso l'era dei big data.

Per mia scelta consapevole rivesto il ruolo di Responsabile per la protezione dei dati personali in favore di pochissimi Clienti. Del resto, credo convintamente che il ruolo di DPO sia delicato e complesso e, secondo il principio dell'**accountability**, si possa portare avanti solo pienamente e con attenzione meticolosa verso i singoli processi di trattamento di ogni titolare o responsabile del trattamento in favore del quale si sviluppa tale ruolo. Per poterlo fare si deve essere in grado di rivestire contemporaneamente il ruolo di abile consulente, di motivatore di team, di ottimo docente e auditor capace.

Un esempio concreto

Come responsabile della protezione dei dati personali motivo, insegno, verifico, assisto un team a me affidato al fine di rendere sempre più libere, capaci e autosufficienti nella gestione dei loro dati e del loro patrimonio informativo pubbliche amministrazioni, ma anche imprese, che mi scelgono come loro autonomo e indipendente interlocutore (questo il DPO deve obbligatoriamente essere).

Questo, a mio avviso, è l'unico modo per poter rendere il servizio DPO davvero "di sostanza", utile e proattivo. Come il GDPR vorrebbe.

Così è stato, ad esempio con **ENEA**, in favore del quale ho prestato questa funzione per due intensi anni, e che oggi ha invece una valida Collega che mi ha sostituito internamente ed efficacemente nel delicato ruolo.

Successivamente la mia assistenza legale in favore di ENEA è anche continuata, ma in forma completamente diversa e meno pervasiva. Come è giusto che sia.

Conclusioni

Insomma, **affidarsi a un DPO dovrebbe significare oggi adottare una metodologia che garantisca a enti pubblici e privati comprensione piena delle tante, innumerevoli "problematiche privacy" in modo che in futuro si possa anche fare a meno di tale "ufficio in outsourcing"**.

Perché il modo migliore per proteggere un dato personale non è essere affiancati da esperti esterni e da tecnologie sicurissime, ma è essere direttamente competenti e responsabili dei processi sottoposti alla propria attenzione, acquisendo il metodo corretto per affrontare delle scelte consapevoli che impattano sul trattamento di dati personali.

Del resto, l'anello debole di qualsiasi catena della protezione di dati personali è sempre l'elemento umano e un bravo Responsabile per la protezione dei dati dovrebbe intervenire, quindi, sulle risorse umane e prima di tutto su se stesso.

Andrea Lisi

Avvocato, esperto in diritto dell'informatica e privacy, Titolare Studio Legale Lisi, Presidente di ANORC Professioni.

16 Marzo 2021

Articolo già pubblicato su <https://studiolegalelisi.it>