Privacy

Privacy in azienda: ripensare il modello organizzativo per minimizzare i costi e creare valore aggiunto

di **Ludovica De Benedetti**

Il Regolamento Generale sulla Protezione dei Dati (GDPR) è pienamente in vigore in tutta Europa da diversi mesi. Per garantire la conformità alla nuova normativa, le organizzazioni hanno dovuto affrontare costi anche molto elevati. Questi costi potrebbero essere ridotti e potrebbero essere massimizzati i benefici derivanti dal trattamento di dati personali, attraverso un'adeguata divisione dei compiti.

Partiamo da un presupposto: nominare un DPO e delegargli l'attività di adeguamento alla nuova normativa è un approccio che si pone in contrasto con il dettato del GDPR per due ragioni. La prima è di natura pratica: se il DPO si deve occupare di tutte le attività di adeguamento alla normativa – spesso con scarse risorse - non può riuscire a svolgere le attività proprie della sua funzione quali la gestione delle richieste degli interessati o la sorveglianza sulla corretta gestione dei dati. La seconda è di natura giuridica: al DPO che, in base a quanto stabilito dal GDPR, è una figura (anche) di controllo, deve essere garantita l'indipendenza rispetto all'ente controllato. Se gli fossero demandate tutte le attività legate all'adeguamento e mantenimento degli obblighi previsti dal Regolamento, controllore e controllato finirebbero per coincidere.

Un DPO, da solo, soprattutto nelle realtà più ampie e complesse, non potrebbe gestire in modo efficiente tutti gli obblighi previsti dal GDPR. È allora particolarmente importante pensare ad un diverso modello organizzativo che possa venire incontro alla triplice esigenza di garantire l'indipendenza e l'effettività del ruolo del DPO, garantire l'efficienza nell'utilizzo dei dati e abbattere, quanto più possibile, i costi di adeguamento alla nuova normativa.

Al fine di raggiungere tali finalità risulta fondamentale procedere in due direzioni: da un lato prevedere una suddivisione ragionata dei compiti e delle responsabilità, dall'altro creare meccanismi che permettano una visione d'insieme dei trattamenti effettuati ed un continuo dialogo fra tutti i soggetti che trattano dati all'interno di un'organizzazione.

Quattro sono le azioni che, se integrate fra loro, possono aiutare un'organizzazione a raggiungere i massimi risultati per quanto riguarda l'adempimento degli obblighi privacy e un utilizzo efficiente dei dati:

1. la creazione di un ufficio che affianchi il DPO;
2. la riorganizzazione aziendale;

3. la creazione di un comitato privacy;
4. il coinvolgimento del DPO in tutte le attività afferenti al trattamento di dati personali.

La prima azione, la creazione di un ufficio dedicato (che, per semplicità, chiameremo Ufficio) che affianchi il DPO nello svolgimento dei suoi compiti, serve a garantire a quest'ultimo un supporto effettivo per lo svolgimento dei suoi compiti. A tale fine è fondamentale un'approfondita conoscenza della realtà aziendale in cui si opera ed è necessario creare una sinergia fra anima giuridica e tecnica per analizzare i possibili rischi sottesi ad un trattamento di dati personali. All'interno dell'ufficio devono, allora, coesistere più professionalità: giuristi, informatici, ingegneri, professionisti in ambito risk management; inoltre una parte dei membri dell'Ufficio dovrebbe essere scelta fra i dipendenti interni all'azienda (Ufficio Legale, IT Security).

La creazione di un Ufficio Data Protection non risolve, però, il problema dell'indipendenza del DPO (controllore e controllato continuerebbero a coincidere). Inoltre delegare tutti gli adempimenti privacy al DPO e al suo Ufficio non è una soluzione efficiente: ogni ente è suddiviso in aree funzionali (Ufficio Legale, Marketing, Credito). Ognuna di tali aree effettua determinati trattamenti di dati che possono, dunque, essere conosciuti in modo approfondito solo da chi lavora quotidianamente all'interno dell'area stessa. Solo questi ultimi soggetti, hanno la possibilità di tenere costantemente sotto controllo le particolarità ed inefficienze dei trattamenti operati e, di conseguenza, posso proporre soluzioni pratiche per garantire performance migliori per l'azienda.

È allora consigliabile ripensare i vecchi modelli organizzativi aziendali e prevedere una ripartizione dei compiti di data protection a livello delle singole aree funzionali richiedendo al responsabile di ogni area di coordinare le attività di data protection e di individuare i soggetti (uno o più anche in base alla complessità dell'area), fra coloro che lavorano con lui, che, in base alla conoscenza dei trattamenti ed al tempo a disposizione, possano operare quali punti di riferimento privacy. I referenti scelti dovrebbero adempiere operativamente a quanto previsto dal GDPR e interfacciarsi sia con il DPO, sia con il proprio responsabile di area, riferendo a entrambi la propria attività. In tal modo, è garantito un controllo costante e diffuso sull'adempimento degli obblighi privacy e si una divisione dei ruoli fra controllore (DPO) e controllato (Titolare del trattamento) in quanto le attività operative di data protection non verrebbero effettuate dall'Ufficio del DPO, ma da soggetti interni al titolare stesso.

Abbiamo, inizialmente, detto che oltre a un'efficiente divisione dei compiti è necessario muoversi anche in una seconda direzione: garantire un dialogo fra tutti i soggetti che trattano dati personale nello stesso ente. La ragione sta nel fatto che raramente i trattamenti di dati personali si esauriscono in un singolo dipartimento e per tale ragione, può non essere sufficiente che ogni area tratti i dati nel modo più corretto perché il trattamento finale garantisca i risultati migliori all'azienda.

Attraverso la condivisione delle "best practices" e la partecipazione del DPO si possono garantire modalità di utilizzo dei dati più efficienti e conformi a quanto richiesto dalla

normativa. Per garantire questo dialogo e migliorare le performance aziendali sarebbe utile prevedere una struttura di raccordo collettiva che possa valutare le problematiche connesse ai diversi trattamenti, individuare collegialmente le migliori modalità per affrontarle e prendere decisioni sulle questioni più impattanti per l'organizzazione, come la notifica agli interessati di un data breach o la decisione di procedere ad una consultazione preventiva all'Autorità.

Infine bisogna tener presente che il DPO rimane una figura di importanza fondamentale e non solo perché in alcuni casi la sua nomina è obbligatoria, ma soprattutto per la possibilità che ha di ad evitare inefficienze comunicative, aiutando le funzioni di business ad estrarre valore dai dati raccolti e trattati. A tal fine il DPO deve sempre mantenere una visione ampia e globale delle attività di trattamento di dati personali che si svolgono nella realtà in cui opera attraverso un dialogo costante con i responsabili e i referenti di ogni area che devono tenerlo aggiornato sull'attività che svolgono riguardante i trattamenti di dati e devono richiedere la sua consulenza in tutti i casi in cui ritengano necessario il suo supporto (formazione specifica, risposte agli interessati, valutazioni di impatto, violazioni dei dati, uso di nuove tecnologie...).

In conclusione, è importante comprendere come il GDPR non debba essere visto solo come un costo per le organizzazioni, ma anche come un'opportunità. La nuova normativa richiede una maggiore conoscenza e consapevolezza riguardo alle modalità con cui si trattano dati personali. E proprio questa consapevolezza si può rivelare un'inestimabile risorsa, permettendo un utilizzo più efficiente dei dati e performance, anche economiche, migliori. Perché ciò sia possibile, però, come visto, sono necessari due fattori: una ragionata condivisione e suddivisione di compiti e responsabilità che permetta un controllo, aggiornamento e verifica costante e diffusa dei trattamenti e delle loro possibili inefficienze e un dialogo fra tutte le parti che trattano dati che garantisca una condivisione delle migliori soluzioni e pratiche e una risoluzione più efficiente delle problematiche legate ai trattamenti.