Il DPO: logiche e costo

1. **Il DPO non è un consulente: FALSO.** Il DPO svolge principalmente un ruolo di *informazione e sorveglianza* che è sostanzialmente affine alle attività tipiche della consulenza specialistica.
2. **Il DPO effettua le Valutazioni d'Impatto sulla Protezione dei Dati / PIA / DPIA (ex art. 35): FALSO.** Il suo compito è quello di *informare il Titolare della necessità* di farle - o farle fare dal *Privacy Officer* - e poi eventualmente di controllarle, su richiesta, al fine di *verificare* che siano state fatte nel modo opportuno (il *parere* di cui al *comma c* di cui sopra).
3. **Il DPO compila il Registro dei Trattamenti (ex art. 30): FALSO.** Vedi quanto detto sopra per le *Valutazioni d'Impatto* (punto 2).
4. **Il DPO è il principale punto di riferimento normativo dell'azienda in tema di Privacy. FALSO.** Quel ruolo spetta in prima battuta al *Privacy Officer*, ovvero all'ufficio *privacy e/o compliance* aziendale. Il compito del DPO è semmai quello di fornire consulenza in merito ai punti non già adeguatamente coperti dalle procedure esistenti, con l'obiettivo di rendere queste ultime sempre più adeguate alle tipologie di dati trattati (e relativi oneri). **Il DPO non è un tappabuchi:** il suo compito è *spingere l'azienda a imparare a tapparli da sola*.
5. **Il DPO deve occuparsi di formazione dei dipendenti o del personale: FALSO.** Vale lo stesso discorso fatto per il punto 4: al DPO non spettano le attività di formazione, il suo compito è assicurarsi che *l'azienda provveda a organizzare i percorsi di formazione* adeguati alle tipologie di dati trattati (e relativi oneri).
6. **Il DPO ha la responsabilità di come l'azienda opera e agisce in ambito Privacy: FALSO.** La responsabilità ricade sempre e comunque in carico al Titolare del trattamento e, limitatamente al loro incarico, ai Responsabili da lui nominati; il DPO non ha responsabilità ulteriori a quelle direttamente connesse alle sue mansioni - come ad es. la comunicazione obbligatoria al garante in caso di *Data Breach* rilevante, anch'essa peraltro su impulso dell'azienda.

ma cosa può chiedere un DPO?

Una ipotesi verosimile da cui partire potrebbe essere la seguente:

- **Attività svolte in azienda : 100 € + IVA / ora.** Audit, sopralluoghi, controlli e verifiche *on-site*, interviste, riunioni et al.
- **Attività svolte da remoto : 50 € + IVA / ora.** Revisione della documentazione, consulenza *off-site*, controlli delle informative, ricerche normative, comunicazioni al garante, conference-call et al.
- spese di trasferta al pari di quelle pagate per i revisori

E' superfluo sottolineare che il criterio di cui sopra è pensato per DPO esterni o per collaboratori assunti con partita IVA: del resto esiste un *general consensus* sul fatto che nominare un dipendente non sia una buona idea, stante l'oggettiva difficoltà di dimostrare i requisiti di indipendenza, autonomia e libertà previsti e richiesti dal GDPR.

Questo semplice metodo di calcolo non è ovviamente sufficiente per formulare un'offerta, ma può costituire una buona base di partenza se coadiuvato da un piano di *audit* adeguato e da una stima di un certo numero di *attività standard*, che è possibile pre-programmare e pre-calcolare: il tutto al netto di possibili attività ulteriori - rigorosamente da concordare e autorizzare nel corso dell'anno - che si renderanno eventualmente necessarie a seguito di eventi imprevedibili ovvero emergenziali, anche in conseguenza del possibile cambio delle normative o di nuovi provvedimenti attuativi emanati dal Garante: si pensi ad esempio al tanto atteso *decreto di armonizzazione*, previsto per agosto 2018, e alle novità che potrebbe introdurre - in positivo o in negativo - in merito agli oneri connessi alla figura del Titolare ovvero del DPO.

Volendo fare un esempio pratico, utilizzando i numeri di cui sopra sarebbe possibile ipotizzare un preventivo di questo tipo:

- **Analisi documentale** (16 ore *off-site*): 800 €
- **1 Audit annuali** (4 ore *on-site* ciascuno): 400 €
- **Consulenza remota** (8 ore *off-site*): 400 €

Per un totale di **1600 € / anno**, al netto di ulteriori esigenze o necessità da valutare in corso d'opera: si tratta senz'altro di un compenso adeguato all'*effort* sostenuto in termini di servizio reso.

In linea generale, chiunque lavori o abbia lavorato nel ramo della consulenza sa perfettamente che l'adozione di un criterio di determinazione del *pricing* basato sulle ore di impiego effettivo ha l'enorme vantaggio di tutelare sia il committente

(l'azienda) che il professionista (il DPO): il primo eviterà il rischio di pagare costi eccessivi rispetto ai servizi ricevuti, mentre il secondo non correrà mai il rischio di dover lavorare al di sotto del margine di guadagno previsto. Non serve una *risk analysis* per comprendere che si tratta di una riduzione considerevole del *rischio di impresa* per entrambe le parti, a tutto vantaggio della valorizzazione (e quindi, si spera, della qualità) del lavoro effettivamente svolto.

Al tempo stesso, non dubitiamo che ci saranno molti Titolari (e non pochi DPO) che non potranno fare a meno di storcere il naso di fronte a queste tariffe: i primi, perché si tratta di prendere seriamente in considerazione una “seccatura” che speravano di risolvere con una cifra modesta, nonché interamente stanziabile in sede di pre-consuntivo; i secondi, perché il pricing su base oraria e calcolato sulle attività effettivamente svolte è una doccia fredda per chi sogna compensi milionari a fronte di un lavoro che, per quanto specializzato e tutt'altro che semplice, non va sopravvalutato **né a livello di complessità né tanto meno a livello di assunzioni di responsabilità**, come abbiamo ampiamente dimostrato.

Ricordiamoci sempre che il compito principale del DPO è quello di *aumentare il livello di consapevolezza del Titolare e della sua azienda in materia di Privacy*, non certo quello di porsi come un misterioso, ineffabile e strapagato azzecagarbugli: ne va della credibilità della sua stessa professione.

il contratto del DPO

quando si sottoscrive un contratto con un DPO solitamente si ricevono immediatamente due servizi: la tutela presso il garante della funzione di DPO, che si esprime con la registrazione sul sito del garante della nomina stessa, e l'accesso ad una serie di documenti e prodotti (sito web dedicato, modelli, ecc.), che definiscono una prima erogazione di servizi in fase di sottoscrizione.

Per questi due servizi sarebbe opportuno che la pubblica amministrazione prevedesse un pagamento alla sottoscrizione del contratto a fronte dei servizi erogati, ed in ogni caso potrebbe sembrare che vincolare il pagamento di tutto il contratto alla fine del periodo di servizi configuri un'anomala posizione di

dipendenza del DPO dalla pubblica amministrazione, cosa fortemente sconsigliata dal garante stesso.

il contratto infatti ha uno svolgimento continuo che si estrinseca poi nella continua consulenza e nel continuo aggiornamento che il DPO deve effettuare, questo dovrebbe far sì che il pagamento avvenga in forma mensile ad erogazione di servizio.

calcolando l'esiguo valore dei contratti sarebbe quantomeno poco opportuno caricare l'amministrazione di fatture da 80 euro mese circa, quindi la soluzione migliore sembra proprio essere la formula del 50% subito e 50% fine contratto.

Responsabile del trattamento: interno od esterno?

OSSERVAZIONI RISPETTO A RESPONSABILE DEL TRATTAMENTO NOMINA INTERNA OD ESTERNA

In nessuno degli articoli e considerando PRESENTI NEL REGOLAMENTO viene definito il RTD come esterno all'azienda del titolare.

Il regolamento non prende posizione sulla scelta interna o esterna, ma definisce solo come ingaggiare l'rttd e cosa esso debba fare.

Ad oggi vi sono indicazioni che propendono per entrambe le scelte.

In considerazione della precedente indicazione legislativa in Italia il responsabile del trattamento era sempre identificato con interno, anche perché è necessaria la specifica conoscenza dei processi interni dell'ente pubblico e la loro gestione.

il Garante della Privacy, alla luce della disciplina aveva precisato che: *“è necessario precisare chi svolgerà l'eventuale ruolo di “responsabile del trattamento”. Conseguentemente, l'Amministrazione deve decidere se prevedere tale figura ed attribuirne la responsabilità o alla struttura esterna cui è affidata*

l'attività in concessione, oppure ad un dipendente di quest'ultima, o a un proprio ufficio o dipendente dell'Amministrazione stessa (quest'ultima opzione presuppone che l'ufficio o il funzionario pubblico abbiano poteri effettivi di ingerenza sulle attività e sull'organizzazione dell'impresa concessionaria: cosa, in realtà, poco frequente). In concreto, la nomina del responsabile, che deve essere effettuata in forma scritta, potrebbe essere inserita in un apposito articolo della convenzione, oppure essere oggetto di un distinto provvedimento amministrativo o atto di diritto privato".

Appare quindi evidente che la scelta di internalizzare o meno la figura è di pura pertinenza del titolare del trattamento.

Certamente per ora qualsiasi scelta appare conforme a quanto indicato dal garante, nel prosieguo si verificheranno ulteriori indicazioni.

Mentre per le aziende la scelta di nominare un responsabile esterno sembra prevalere, per le pubbliche amministrazioni la tendenza si inverte anche per ridurre i costi che altrimenti sarebbero da sostenere.

A parere di chi scrive in considerazione della giovinezza della materia e della consolidata esperienza precedente è opportuno provvedere a nomine che siano efficaci nell'immediato e non carichino di costi l'amministrazione in attesa di vedere le prossime linee guida del garante, PERTANTO è OPPORTUNO CHE LE SCUOLE IDENTIFICHINO UN RESPONSABILE INTERNO OVE POSSIBILE..