# 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 azzeccagarbugli: ne va della credibilità della sua stessa professione.