

# Getmoon & Partners<sup>®</sup>

b u s i n e s s | p r | m a r k e t i n g

Spettabile

**ORDINE DEI PERITI INDUSTRIALI**

**E DEI PERITI INDUSTRIALI LAUREATI  
DI MILANO**

Via Jacopo Palma 26

20146 Milano (MI)

Trento 02.12.2020

Gentile Ordine,

con la presente e in riferimento all'incontro c/o la vs. sede, siamo a riproporre per l'anno 2021 i nostri servizi professionali per l'incarico di **DPO (Data Protection Officer) per l'Ordine dei Periti Industriali e dei Periti Industriali Laureati delle Province di Milano e Lodi.**

Il DPO - Responsabile della protezione dei dati, è un soggetto con un ruolo misto di consulenza e controllo che deve verificare l'applicazione del GDPR (General Data Protection Regulation), facilitarne l'osservanza e minimizzare il rischio di violazioni, informare e consigliare la P.A. e le imprese (contitolari e sub-responsabili) e fungere da interfaccia fra i diversi soggetti coinvolti (autorità di controllo, P.A., interessati, parti terze).

Il DPO opera in posizione di **autonomia** nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il DPO non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, **il DPO riferisce direttamente al Titolare ed al Responsabile del trattamento.**

Nel dettaglio i compiti del DPO consistono in :

- **informare e consigliare** le organizzazioni ed i loro dipendenti sui loro obblighi derivanti dal GDPR e dalla normativa nazionale;

- **sorvegliare l'osservanza del GDPR** e delle policies interne in materia di data protection, (compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale e i relativi audit);
- **sorvegliare le attribuzioni delle responsabilità agli incaricati/addetti e le attività di sensibilizzazione, formazione e controllo** poste in essere dal Titolare e dal Responsabile del trattamento, all'interno della struttura organizzativa cui fa capo;
- fornire, se richiesto, un **parere sulla valutazione d'impatto** del trattamento sulla protezione dei dati e sorvegliarne lo svolgimento (Registro dei trattamenti/PIA);
- **cooperare con le autorità di controllo** e fungere da loro punto di contatto per facilitare l'accesso, da parte di queste, ai documenti ed alle informazioni, nonché ai fini dell'esercizio dei poteri di indagine e correttivi.

Il Regolamento sancisce che:

“Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'art. 39

(..) deve possedere

- conoscenza specialistica in materia di privacy e legislazione sulla protezione dei dati nell'UE e degli altri rilevanti strumenti giuridici di protezione dei dati e conoscenze in materia di IT e sicurezza IT
- buona conoscenza del funzionamento dell'istituzione [in cui il DPO viene designato], delle attività di trattamento dei dati da essa operate e abilità interpretativa delle norme relative alla protezione dei dati in tale contesto.”

“Per quanto riguarda l'informatica, si richiede una buona comprensione della terminologia, delle attività [IT] e delle diverse forme di trattamento dei dati. Un DPO deve possedere, ad esempio, conoscenze in materia di gestione dei dati e sistemi di utilizzo degli stessi, tipologie di software, sistemi di stoccaggio dei dati e dei file, normative in materia di riservatezza e politiche di sicurezza (cifatura dei dati, firma elettronica, dati biometrici, ...). Tali conoscenze devono permettere [al DPO] di controllare la realizzazione dei progetti IT e fornire utili pareri al titolare responsabile del trattamento”

“Il DPO deve dimostrare una buona comprensione delle attività di trattamento svolte [nel settore o nell'organizzazione di appartenenza], dei sistemi di informazione, dei sistemi di protezione dei dati, e delle necessità di tutela dei dati del titolare.

Nel caso di autorità o organismo pubblico, il DPO deve possedere solide conoscenze delle procedure e delle regole amministrative [interne] dell'organizzazione

I DPO devono usufruire della possibilità di rimanere aggiornati sugli sviluppi che riguardano la protezione dei dati.

\*\*\*

La proposta in oggetto vuole offrire all'Ente, la messa a disposizione di un consulente esperto che espleti per lo stesso l'incarico di DPO.

Tale incarico sarà conferito ad un soggetto capace e responsabile che ha maturato sufficienti competenze in materia di Privacy (GDPR 2018) e di Organizzazione delle Procedure degli Ordini Professionali. nello specifico le attività saranno prestate da Monica Barreca, che ha maturato le competenze necessarie per assisterVi in tal senso.

Con l'obiettivo di **assicurare il costante monitoraggio** delle procedure di sicurezza in merito al trattamento dei dati si conviene che il DPO, riferendosi direttamente al vertice gerarchico, in modo che quest'ultimo possa venire a conoscenza delle indicazioni e delle raccomandazioni dal primo fornite nell'esercizio delle sue funzioni di informazione e consulenza, riservi all'organizzazione **interni periodici per verificare lo stato dei fatti, l'attuazione delle procedure di sicurezza per prevenire situazioni di vulnerabilità**. Il DPO verificherà con i sub-responsabili del trattamento – gli addetti alla segreteria dell'Ordine, trimestralmente, la correttezza dell'implementazione di tutte le misure di sicurezza e l'applicazione puntuale del Regolamento.

Tali attività saranno indirizzate a **verificare i settori funzionali a maggiore rischio** di incidenti o violazioni (DATA BREACH), a garantire le attività di formazione interna per il personale che tratta dati personali, a rilevare eventuali aggiornamenti da inserire nel **registro dei trattamenti** eventualmente definendo un ordine di priorità nell'attività da svolgere, incentrato sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati.

Qualora si verificassero, al di fuori degli audit periodici previsti nel presente contratto, situazioni di potenziale rischio, il Titolare e/o il Responsabile del trattamento si assicureranno che il DPO sia **tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e lo stesso sarà immediatamente a disposizione dell'Ordine**.

In concreto:

- il DPO dovrà sempre e tempestivamente disporre di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del DPO sulle decisioni che impattano sulla protezione dei dati sarà obbligatorio ma non vincolante (nel caso di decisione difforme si procederà ad un verbale da allegare alla documentazione privacy);
- il DPO dovrà essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente;
- il Titolare e/o il Responsabile forniranno, attraverso le risorse dell'organizzazione, supporto adeguato in termini di infrastrutture (attrezzature, strumentazione) e accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

Al fine di cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per l'organizzazione che l'ha incaricato, **il nominativo del DPO è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante Privacy.**

Dopo la designazione, i dati di contatto del DPO devono essere indicati anche nell'Informativa privacy fornita agli interessati e ufficialmente comunicati all'interno dell'organizzazione.

Queste disposizioni mirano a garantire che tanto gli interessati (all'interno o all'esterno dell'ente o dell'azienda), quanto le Autorità di controllo possano contattare il DPO in modo facile e diretto senza doversi rivolgere a un'altra struttura e che i dipendenti possono presentare reclami in totale riservatezza.

Il contratto avrà durata annuale e prevederà i seguenti servizi:

- incarico di **DPO (Data Protection Officer)**,
- n. 4 **verifiche annuali, cadenza trimestrale** con i sub-responsabili dei dati,
- supporto al Titolare del Trattamento nella **revisione del registro dei trattamenti** (post-audit, ove necessario), in relazione alle modifiche interne in merito al trattamento dei dati,
- **rapporto di audit annuale** (RELAZIONE ANNUALE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI ), che sintetizza l'esito degli audit e contiene:
  - ✓ Parere di Audit;
  - ✓ Obiettivi;
  - ✓ Principali accertamenti;
  - ✓ Azioni necessarie;
  - ✓ Raccomandazioni.

Il documento sarà presentato al Consiglio Direttivo dell'Ordine e reso disponibile all' Autorità Garante su richiesta.

I corrispettivi dovuti a Getmoon per l'esecuzione dei servizi, oggetto della presente, proposta sono stati stabiliti a corpo per un **importo totale di € 800,00+IVA**.

L'importo del contratto sarà fatturato alla data dell'incarico.

Eventuali attività aggiuntive legate all'eventualità di violazioni, che prevedano l'intervento urgente e straordinario del DPO, per tutelare gli interessati al trattamento e parallelamente l'Ordine, nonché il Titolare dei dati (Legale Rappresentante dell'Ente), connesse alle verifiche ispettive del Garante saranno quotate ad hoc (con un costo massimo a giornata di € 800,00, iva esclusa).

Le trasferte presso la vostra sede, per la realizzazione del presente incarico, vi saranno presentate a piè di lista con esposizione di costi kilometrici e autostradali, con fatturazione progressiva.

Augurandoci che la proposta risulti completa e interessante, ci auguriamo di poter continuare una collaborazione in tal senso.

L'occasione è gradita per inviare i nostri migliori saluti.

Getmoon & Partners  
Monica Barreca  
*Amministratore Delegato*

