Oggetto dell'incarico: affidamento del servizio di Data Protection Officer (Responsabile della protezione dei dati). (**Regolamento UE/2016/679)**

Tipologia del servizio: servizio professionale con conoscenze giuridiche, informatiche, di *risk management* e di analisi dei processi. Il compito principale sarà quello di osservare, valutare la gestione del trattamento di dati personali e la loro protezione all'interno dell'Ente secondo quanto previsto dall'art. 39 comma 1 del **Regolamento UE/2016/679** e fornire consulenza ai Responsabili indicati dall'Ente.

Dimensionamento
L'Ente si avvale di circa 500 tra dipendenti e collaboratori suddivisi in 45 sedi distribuite nel territorio regionale.
Le sedi sono collegate attraverso una rete intranet denominata MPLS con centro stella posizionato nel Data Center di Regione del Veneto che avrà una uscita unica comune verso Internet.
Sarà adottata una piattaforma con tecnologia Virtual Desktop in cui le postazioni remotizzate saranno posizionate fisicamente nel Data Center di Regione del Veneto.
Gli applicativi ad uso dei dipendenti sono di tipo Web Oriented e saranno localizzati presso Veneto Lavoro o presso Regione del Veneto. Alcune applicazioni quali il software per la gestione presenze e il software per la gestione della contabilità-amministrazione risiedono presso il fornitore del servizio.

Corrispettivo: 39.000,00 euro

Durata incarico: 24 mesi

Interventi minimi:
- Audit, sopralluoghi, controlli e verifiche on-site, interviste, riunioni
- Revisione della documentazione, consulenza off-site, controlli delle informative, ricerche normative, comunicazioni al garante, conference-call
- Analisi documentale
- Audit annuale
- Incontri periodici

Requisiti specifici e funzioni del DPO
In coerenza con le linee guida del Gruppo di lavoro Art. 29 per la protezione dei dati adottate in data 13 dicembre 2016, il Responsabile della protezione dei dati personali designato deve essere in possesso dei seguenti requisiti:

Requisiti del Responsabile della protezione dati (DPO)
Il DPO deve possedere:
- approfondita conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del GDPR;
- approfondita conoscenza normativa inerente all'organizzazione ed al funzionamento degli Enti pubblici, del D.Lgs. 165/2001 e s.m.i. (in particolare le norme che regolano il conflitto di interessi) e della normativa in materia di trasparenza amministrativa di cui al D.Lgs. 33/2013 e s.m.i.;

- conoscenza specifica dei settori di attività di Veneto Lavoro, delle norme e procedure amministrative applicabili
- adeguata competenza in materia informatica e misure di sicurezza dati, con esperienza nel mercato ICT;

Esperienza richiesta al DPO e al Team (staff tecnico)

a) esperienza riguardo le tematiche legate alla privacy, alla gestione e sicurezza informatica dei dati e delle informazioni e della trasparenza;
b) esperienza di consulenza, anche legale, in favore della PA e/o società e enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni, riguardo alle tematiche legate alla privacy, diritto informatico ed internet, amministrazione digitale, accesso e trasparenza.

La valutazione dei curricula concorre all'assegnazione del punteggio tecnico**.**

Al fine di garantire tutte le competenze richieste, il servizio può essere eseguito da un gruppo di lavoro, fermo restando l'obbligo dell'esecutore dell'appalto di individuare un capo progetto che verrà nominato DPO, con apposito provvedimento dell'Amministrazione. I concorrenti devono comprovare tutte le competenze richieste nel presente capitolato mediante la produzione del curriculum del soggetto individuato per il ruolo di DPO e la descrizione dell'eventuale composizione del gruppo di supporto.

Compiti

Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE/679/2016 nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del regolamento UE/679/2016, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il DPO è pertanto tenuto a svolgere funzioni di supporto e di controllo, consultive, formative ed informative in materia di privacy e protezione dei dati personali, e più dettagliatamente:

Fase preliminare

- analisi finalizzata all'identificazione degli obiettivi, alla raccolta delle informazioni, alla verifica del livello di conformità alla normativa in materia di protezione dei dati, misurazione del livello di esposizione dei rischi associati al trattamento dei dati;

- individuazione e mappatura dei trattamenti dei dati personali effettuati con strumenti cartacei, elettronici e/o informatici, analisi della tipologia dei dati trattati, delle finalità per cui sono trattati e degli interessati (**registro dei trattamenti**) e classificazione del rischio privacy, anche dei dati non strutturati;
- predisposizione delle "**valutazioni di impatto**" (Data Protection Impact Assessment - DPIA), particolarmente per quelle considerate "obbligatorie" dalla normativa, e individuazione delle misure idonee atte a garantire le prescrizioni della norma, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento;
- predisposizione della procedura di gestione degli incidenti/data breach e conseguente attivazione del **registro di violazione dei dati**;
- individuazione delle misure organizzative e tecniche che consentano di avere un controllo continuo sulla conformità alla normativa;
- strategia di gestione dei rischi privacy.

Fase successiva

- riesame/aggiornamento delle "valutazioni di impatto" (DPIA) e rischi privacy in allineamento alle evoluzioni interne e/o alle direttive dell'Autorità Garante Privacy (Garante), nuove leggi, regolamenti etc.;
- attivazione del registro dei trattamenti eseguiti dalle terze parti;
- predisposizione/aggiornamento della regolamentazione aziendale in tema di trattamento dei dati personali;
- elaborazione, redazione od aggiornamento dei moduli per il consenso, delle informative sul trattamento dei dati personali, degli atti di nomina dei responsabili, degli incaricati;
- consulenza sugli obblighi derivanti dal GDPR e dalle ulteriori disposizioni legislative, provvedimenti e linee guida del Garante e conseguente aggiornamento del sistema privacy.

Per le predette attività di consulenza deve essere garantita ***la presenza on site*** secondo modalità da concordarsi con la committenza, quantificate nella misura minima di 30 ore/annue di cui **15 ore** da erogarsi nei primi 60 giorni. Il numero di ore aggiuntive concorre all'assegnazione del punteggio tecnico.

Oltre alle attività indicate alle 2 fasi descritte, al DPO, quale responsabile della protezione dei dati, competono le seguenti prestazioni previste dall'art. 39 del GDPR (a titolo esemplificativo e non esaustivo):

- redigere un piano di lavoro;
- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
- sorvegliare l'osservanza della normativa vigente in materia nonché delle politiche del titolare o del responsabile del trattamento relative alla protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- assistere il titolare o responsabile del trattamento nel controllo del rispetto a livello interno del regolamento europeo n. 679/2016;
- garantire attività di informazione, consulenza e indirizzo nei confronti del titolare, del responsabile e del personale che partecipa ai trattamenti e alle connesse attività di controllo;

- cooperare e fungere da punto di contatto con l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva ed effettuare, se del caso, consultazioni relativamente ad ogni altra questione: il DPO facilita l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei suoi compiti, nonché ai fini dell'esercizio dei suoi poteri di indagine, correttivi, autorizzativi e consultivi. In ogni caso il DPO può consultare l'autorità di controllo con riguardo a qualsiasi altra questione;
- fungere da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti, comunicando con gli interessati in modo efficiente;
- considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo;
- riferire riguardo alle indicazioni/raccomandazioni fornite nel quadro delle sue funzioni;
- fornire il reporting riguardo al livello di conformità al GDPR;
- redigere una relazione annuale delle attività svolte;
- programmare l'attività di formazione ed aggiornamento annuale degli operatori della Società, in accordo con la stessa, sulle problematiche e la legislazione concernente la materia del trattamento dei dati;
- evadere i quesiti di natura legale in materia di privacy richiesti dalla committenza entro il termine massimo di 7 (sette) giorni o quello migliorativo indicato nell'offerta; il termine migliorativo per evadere i quesiti di cui al presente punto concorre all'assegnazione del punteggio tecnico

Nell'adempimento dei propri compiti, il DPO dovrà attenersi al segreto e alla riservatezza: tali vincoli non precludono la possibilità per il DPO di contattare e chiedere chiarimenti all'autorità di controllo.
Per garantire le prestazioni previste dal presente articolo e dalle disposizioni in materia, il DPO, pur potendosi avvalere di un team (staff tecnico), funge da contatto principale; per tale ragione è necessaria una chiara ripartizione dei compiti.
I dati di contatto del DPO sono pubblicati e comunicati alle pertinenti autorità di controllo affinché possa essere contattato sia dagli interessati che dalle autorità di controllo in modo facile e diretto.

Attività di formazione
Il servizio comprende l'attività di formazione obbligatoria a favore del management aziendale, dei dirigenti di struttura e del personale addetto sulle responsabilità connesse con la sicurezza e protezione dei dati.
L'operatore economico deve presentare un programma di formazione elaborato sulla base di un numero di dipendenti pari a 60 unità
L'attività di **formazione minima** da erogarsi nel primo anno, in aula presso la sede di Veneto Lavoro in Venezia-Mestre, è di 3 (tre) sessioni della durata di 4 (quattro) ore con la partecipazione di ca. 20 unità di personale ciascuna.
Il numero di edizioni aggiuntive offerte concorre all'assegnazione del punteggio tecnico.
Le date delle edizioni saranno da concordare con la committenza.