SERVIZIO DI CONSULENZA SULLA PROTEZIONE DEI DATI PERSONALI E DATA PROTECTION OFFICER (DPO) AI SENSI DEL REGOLAMENTO EUROPEO UE/2016/679

CAPITOLATO TECNICO

ART. 1 OGGETTO DEL SERVIZIO

L'appalto ha per oggetto l'affidamento del servizio di consulenza e supporto in materia di protezione dei dati personali per la messa a norma ed il conseguente rispetto degli adempimenti e obblighi previsti dal Regolamento europeo n. 679/2016 (General Data Protection Regulation – GDPR) e servizio di Data Protection Officer (Responsabile della protezione dei dati).

1.1. ATTIVITA' PRINCIPALI

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;

- strutturazione di un organigramma privacy finalizzato alla distribuzione delle responsabilità interne all'azienda del trattamento dati;

- analisi del sistema di videosorveglianza e aggiornamento alla normativa vigente.

Per le predette attività di consulenza deve essere garantita **la presenza *on site*** secondo modalità da concordarsi con la committenza, quantificata nella misura minima di **160 ore/annue** di cui **80** da erogarsi nei primi 60 giorni. Il numero di ore aggiuntive concorre all'assegnazione del punteggio tecnico.

Resta inteso che, eventuali ore di presenza on site non utilizzate nel primo anno per esigenze di S.C.R. Piemonte S.p.A., incluse quelle riferite ai primi due mesi, saranno godute dalla Società nel periodo contrattuale successivo.
Qualora nel corso dell'esecuzione del contratto si rendesse necessario ricorrere all'assistenza *on site* per un numero di ore superiore a quello minimo complessivamente previsto (*o a quello complessivo migliorativo indicato nell'offerta tecnica*), sarà corrisposto il costo orario pari a quello indicato nell'offerta economica.

1.2. ATTIVITA' DI DATA PROTECTION OFFICER (DPO)
Oltre alle attività indicate al precedente art. 1.1, 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 tecnica*).

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.

Requisiti del Responsabile della protezione dati (DPO)
Il DPO deve possedere:

- conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del GDPR;

- conoscenza specifica dei settori di attività di S.C.R. Piemonte, delle norme e procedure amministrative applicabili.

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.

1.3 ATTIVITA' 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 committenza, 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.

ART. 2 DURATA DEL SERVIZIO
Il servizio avrà durata biennale.