SISTEMA SANITARIO REGIONALE

ASL ROMA 5

REGIONE LAZIO

UOC Affari Generali e Legali

SERVIZIO IN MATERIA DI TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI PER LA MESSA A NORMA ED IL RISPETTO DEL DETTATO NORMATIVO DEL REGOLAMENTO UE 679/2016.

CAPITOLATO TECNICO

LOTTO 1 - OGGETTO DEL SERVIZO

Affidamento dei servizi in materia di trattamento e protezione dei dati personali per la messa a norma ed ilrispetto del dettato normativo del Regolamento Europeo 679/2016

LOTTO 1 - ATTIVITÀ RICHIESTE

✓ Attività di raccolta degli elementi informativi utili alla comprensione delle procedure operative aziendaliadottate, al fine di verificare il livello di conformità agli obblighi posti dal GDPR 679/2016;

✓ Raccolta, analisi e valutazione dei documenti afferenti il trattamento dei dati personali;

✓ Analisi e valutazione delle procedure informatiche in uso presso l'azienda e loro livello di protezione;

✓ Individuazione e mappatura dei trattamenti individuati ed effettuati; analisi degli stessi rispetto alla loroannotazione nel registro dei trattamenti di cui all'ART. 30 del GDPR 679/2016;

✓ Raccolta, analisi e valutazione della modulistica adottata in tema della Privacy rispetto agli obblighi previsti dal GDPR 679/2016;

✓ Raccolta ed analisi delle policy di sicurezza adottate in aderenza all'entrata in vigore della normativaeuropea e loro successiva valutazione d'impatto sulla protezione dei dati personali;

✓ D.P.I.A. - DATA PROTECTION IMPACT ASSESTMENT;

✓ Analisi e valutazione delle procedure del processo di data breach adottato;

✓ Revisione e ridefinizione, alla luce dell'analisi condotta, del Remediation Pian con conseguente azionecorrettiva tecnica ed assicurativa atta a ridurre le problematiche rilevate in tema di trattamento del dato;

LOTTO 2 - OGGETTO DEL SERVIZIO

Affidamento del servizio di D.P.O. (data protection officer - responsabile per la protezione del dato) eFormazione ad un soggetto esterno in possesso dei requisiti descritti dal Regolamento Europeo 679/2016.

LOTTO 2 - ATTIVITÀ' RICHIESTE

✓ Informare e fornire la dovuta consulenza al titolare del trattamento in merito agli obblighi previsti intema di protezione del dato, dal GDPR 679/2016. Il servizio di consulenza si intende comprensivo della erogazione di richiesti pareri a fronte di quesiti istituzionali posti in tema della privacy.

✓ Verificare l'applicazione e provvedere alla sorveglianza sull'adozione dei contenuti normativi posti dalGDPR 679/2016 in merito alla protezione dei dati;

✓ Essere punto di contatto dell'autorità di controllo sia in caso di attività ispettiva che per singoli questioni afferenti il trattamento del dato sotto il profilo della privacy;

✓ Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati esorvegliare il corretto svolgimento in aderenza alle indicazioni fomite in proposito dal GDPR 679/2016;

✓ Garantire la propria presenza in tutte le attività relative al trattamento del dato, su richiesta del titolare, al fine di rilasciare un motivato parere sulle procedure di valutazione per la loro adozione;

✓ Programmare l'attività di formazione ed aggiornamento annuale dei dipendenti aziendali, in accordo con le politiche applicate in proposito dall'azienda;

✓ Redigere ed inviare alla D.G. aziendale una relazione annuale delle attività compiute;

✓ Nell'adempimento del proprio compiti, il DPO dovrà attenersi alle norme che regolano il segretod'ufficio e la dovuta riservatezza e svolgere il proprio compito presso l'azienda dedicandogli un tempo adeguato rispetto ai compiti previsti e assegnati;

✓ Al DPO è consentito l'accesso a tutte le strutture aziendali al fine di acquisire, previo accordo per appuntamento, le informazioni relative al suo mandato anche con interviste al personale;

✓ Alla luce di quanto sopra descritto, il DPO dovrà essere in possesso di:

✓ Alte qualità professionali in tema giuridico ed in particolare in tema di privacy, con particolare riferimento alla capacità di assolvere i compiti di cui all'art. 39 del GDPR 679/2016;

✓ Conoscenze comprovate in materia di organizzazione sanitaria;

✓ Esperienze su tematiche connesse alla protezione dei dati, alla privacy afferente agli stessi ed alla protezione della rete in generale;

✓ n. 10 sedute annue di formazione da remoto a tutto il personale ASL.

LOTTO 1: SERVIZIO ASSESSMENT PRIVACY Importo annuo €.34.000 IVA esclusa

Requisiti richiesti e relativi punteggi:

✓ Avere svolto attività di legal assessment in materia di privacy alla luce dell Reg. UE 2016/679, codiceprivacy come MOD dal D. Lgs 101/2018, in via preferenziale in favore di aziende sanitarie e sociosanitarie siapubbliche che private e aziende multinazionali esclusivamente operanti nell'ambito del device sanitario - MAX PUNTI 3;

✓ Avere svolto, anche attraverso l'opera di propri consulenti, attività di messa in compliance mediante legal assessment report e data protection impact assessment in favore di due o più aziende sanitarie pubbliche, preferibilmente in contesti regionali diversi - MAX PUNTI 7;

✓ Avere svolto attività di messa in compliance privacy in favore di istituti di ricerca scientifica (IRCCS -Istituto di ricovero e cura a carattere scientifico) - MAX PUNTI 15;

✓ Avere collaborato alla sottoscrizione di accordi - e/o attività di studio e divulgazione sotto ogni forma della cultura della protezione del dato personale - con enti nazionali e/o internazionali - MAX PUNTI 10;

✓ Avere svolto, anche attraverso propri consulenti, attività di formazione al personale sanitario di governance, dirigente, infermieristico, tecnico - MAX PUNTI 3;

✓ Avere, comprovatamente, approvato e fornito alle stazioni appaltanti sue clienti, un modello di privacy (di cui ai punti precedenti) afferente strutture sanitarie pubbliche con espressa e puntuale descrizione delle parti che lo compongono - MAX PUNTI 3;

✓ Essere in grado di comprovare la fruizione di consulenze - in ambito e materia di privacy - da parte di professionisti di elevato profilo già impegnati nell'ambito della compliance privacy sia in ambito pubblico sia in ambito privato - MAX PUNTI 3;

✓ Svolgere attività di messa in compliance direttamente o mediante consulenti di comprovato profilo scientifico (autori di pubblicazioni, con codice ISBN nella specifica materia), nonché altre pubblicazioni in riviste specializzate di settore in ambito nazionale - MAX PUNTI 10;

✓ Conoscenza delle norme e delle procedure di natura amministrativa applicabili; Competenze in materia di Risk Management di analisi dei processi; Capacità di promuovere una cultura della protezione del dato all'interno dell'azienda e possesso dei più elevati standard deontologici quali: correttezza, serietà, affidabilità ed integrità di condotta - MAX PUNTI 3;

✓ Esperienze connesse con le attività di organismi nazionali ed internazionali, operanti nel settore dell'information technology ed in particolare quello della protezione delle reti informatiche rispetto alle minacce poste dal cyber crime - MAX PUNTI 3;

✓ Possesso certificazione ISO/UNI in tema di protezione dati personali - MAX PUNTI 10.

<u>LOTTO 2: SERVIZIO DPO</u> Importo annuo €.39.000 IVA esclusa:

Requisiti richiesti e relativi punteggi:

✓ Esperienza maturata dalla società incaricata in materia di privacy presso strutture pubbliche e private e società multinazionali con particolare preferenza per le attività espletate a favore di strutture sanitarie sia pubbliche che private - MAX PUNTI 5;

✓ Possesso di una delle seguenti lauree magistrali da parte del DPO incaricato dalla società incaricata: Giurisprudenza, Economia, Ingegneria Informatica, Informatica, Scienze politiche, nonché ulteriori titoli di studio rilevanti per il settore - MAX PUNTI 5;

✓ Esperienza maturata dal DPO incaricato dalla Società incaricata in amministrazioni pubbliche o privatein materia di gestione e protezione dei dati - MAX PUNTI 5;

✓ Esperienza maturata dal DPO incaricato dalla società incaricata relativamente alle attività di formazione condotte a favore di enti pubblici e privati con descrizione dei contenuti erogati e dei relatori intervenuti, nonché con la specifica dei profili personali dei team di formatori dedicati allo scopo - MAX PUNTI 10;

✓ Pubblicazioni a firma dei docenti componenti il team di formatori della società incaricata, in tema di sanità, di privacy nella sanità e sulla protezione dei dati in generale (articoli stampa, volumi con codice ISBN)
- MAX PUNTI 10;

✓ Collaborazioni tenute dalla società incaricata o dai soci incaricati, con organismi nazionali o internazionali in materia di sicurezza dei dati personali e delle reti sui quali gli stessi vengono elaborate e conservati - MAX PUNTI 10;

✓ Esperienza maturata dal DPO della società incaricata, presso istituiti sanitari dediti alla ricerca scientifica (IRCCS - Istituto di ricovero e cura a carattere scientifico) - MAX PUNTI 10;

✓ Rapporti di prestazione professionale con consulenti di elevato profilo in materia di privacy nella sanità
- MAX PUNTI 5;

✓ Possesso certificazione ISO/UNI in tema di protezione dati personali - MAX PUNTI 10.

Il Direttore ff UOC Affari Generali e Legali
Enzo Fasani