CAPITOLATO TECNICO

AFFIDAMENTO DELL'INCARICO DI DATA PROTECTION OFFICER (DPO) E ATTIVITA' DI SUPPORTO ALLA CORRETTA APPLICAZIONE DEL REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI PERSONALI (GDPR) 2016/679 PER LA ASL DI LATINA.

OGGETTO DEL SERVIZIO

Oggetto del presente Capitolato è l'affidamento a Soggetto esterno (di seguito Aggiudicatario), persona giuridica, dell'incarico di Data Protection Officer/Responsabile della protezione dei dati (di seguito DPO), nonché per le attività di supporto alla corretta applicazione del Regolamento Europeo sulla protezione dei dati personali n. 679 del 27/04/2016 (GDPR).

La disciplina in materia di trattamento dei dati personali, introdotta dal nuovo Regolamento UE 2016/679 (GDPR), ha avuto un notevole impatto sull'organizzazione della P.A. La ASL di Latina ha già intrapreso un percorso organizzativo di adeguamento delle proprie strutture sanitarie ed amministrative, al fine dell'applicazione dei principi sanciti dal citato GDPR. Tale adeguamento non si configura come una azione organizzativa compiuta, ma deve intendersi come una continua e ininterrotta manutenzione e aggiornamento del "sistema privacy", sia sotto l'aspetto procedurale che tecnico, anche in considerazione della complessità del territorio dell'Azienda Sanitaria di Latina.

L'incarico di DPO, consulenza e supporto in materia di protezione dei dati personali GDPR 679/2016, dovrà svolgersi in piena autonomia ed indipendenza, espletando i compiti e le funzioni proprie previste dalla figura professionale, di cui all'art. 39 del GDPR e secondo le linee guida tracciate nel Documento di indirizzo n. 186 del 29 aprile 2021, emanato dal Garante, sulla designazione, posizione e compiti del Responsabile della Protezione dei Dati (RPD) in ambito pubblico.

Stante la complessità della struttura (comprendente, tra l'altro, strutture ospedaliere e territoriali), la funzione di DPO dovrà essere svolta anche attraverso le competenze di uno Staff tecnico multidisciplinare specializzato, composto da figure interne alla società aggiudicataria, in cui dovranno confluire professionalità con competenze in materie giuridiche e informatiche.

COMPITI DEL DPO/RPD

Il DPO, ai sensi art. 39 par 1 del GDPR, "*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 GDPR citato, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
- sorvegliare l'osservanza del GDPR 679/2016, delle disposizioni nazionali o dell'Unione 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 delle responsabilità, 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 del GDPR;
- fungere da punto di contatto con il Garante per la protezione dei dati personali e cooperare con lo stesso, in merito a tutte le 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.

ATTIVITA' RICHIESTE

Oltre ai compiti previsti per il DPO al punto precedente, si elencano, di seguito, le ulteriori attività richieste al DPO e al suo Staff di supporto, oggetto del presente capitolato:

- verificare l'esattezza e la completezza dei trattamenti inseriti nel Registro dei Trattamenti, provvedendo ai necessari aggiornamenti e tenuta del Registro stesso;
- effettuare una revisione di tutte le Procedure Aziendali ad oggi utilizzate, come evidenziate di seguito a titolo esemplificativo e non esaustivo: Audit – Data Breach – Diritti Interessato – Conservazione Dati e RPD-DPO;
- verificare ed aggiornare le policy per la pubblicazione sul sito aziendale;
- valutare i sistemi informatici e la rete telematica, per la parte relativa alla protezione dei dati, in caso di attacchi, intrusioni, violazioni dall'esterno, nonché l'efficacia e il rispetto delle norme di sicurezza interne (back-up, password, etc.), anche per l'effettuazione di una valutazione dell'impatto (DPIA);
- esaminare e aggiornare tutta la modulistica aziendale (informative, informative e consenso privacy, modello autorizzati/incaricati, modello nomine Delegati, modello Responsabile del Trattamento Dati, modello di nomina ad amministratore di sistema, etc.), con valutazione delle modalità con le quali viene rilasciata;
- redigere eventuale nuova modulistica in relazione alle disposizioni del Garante;
- supporto alla ASL di Latina nella redazione di documentazione sulla protezione dei dati, ai fini di esibizione a terzi, tesa a dimostrare in modo oggettivo e trasparente le attività poste in essere per la compliance al GDPR, in linea con il principio di accountability;
- facilitare 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;
- supportare il Titolare nella redazione della DPIA;
- assistere il Titolare nella compilazione e invio della Notifica al Garante e nella redazione e invio della Comunicazione agli interessati e nella compilazione del Registro di data breach;
- garantire la presenza, presso la ASL di Latina, per almeno 4 giornate/mese nei primi 6 mesi del servizio, e per almeno 2 giornate/mese per i periodi successivi;
- garantire, in caso di emergenza o in questioni attinenti la protezione dei dati, nei casi in cui il Titolare lo ritenga necessario o opportuno (data breach, visite dell'Autorità Garante, etc), la presenza del DPO

presso la sede aziendale ASL entro le ore 12, del giorno successivo alla richiesta telefonica o tramite posta elettronica, per il tempo necessario alla risoluzione della problematica;

- cooperare e supportare le strutture aziendali nella valutazione delle richieste di accesso agli atti, che comportino riflessi sulla protezione dei dati personali, nell'ottica di contemperare il diritto di accesso al diritto di riservatezza dei dati trattati;
- redigere e trasmettere alla Direzione Generale dell'ASL di Latina, una relazione annuale delle attività svolte;
- redigere e trasmettere alla Direzione Generale dell'ASL di Latina, entro i primi 60 giorni dalla aggiudicazione della gara, una relazione riferita al livello di conformità al GDPR nonché tempestiva comunicazione all'Azienda dell'avvio delle azioni, indicazioni e raccomandazioni correttive proposte al fine del miglioramento continuo e della riduzione dei rischi;
- organizzare specifici audit privacy presso le strutture aziendali (almeno 6 audit in 18 mesi);
- programmare ed erogare l'attività di formazione ed aggiornamento annuale in favore dei dipendenti dell'ASL di Latina, in accordo con la UOC Formazione, in attuazione alla normativa privacy. Le sessioni formative si rivolgeranno a tutti i dipendenti della ASL (secondo gli specifici ruoli ricoperti in Azienda), dovranno essere della durata di almeno 4 ore e potranno essere erogate in presenza oppure online, con il rilascio di un attestato di frequenza e partecipazione;
- programmare ed erogare, una formazione a distanza, in modalità asincrona, tramite video-tutorial, organizzati per argomenti in sessioni da un'ora (1) (es. gestione privacy del paziente, gestione delle risorse umane, gestione del data breach, gestione del Responsabile del Trattamento, etc.);
- evadere i quesiti in materia di privacy richiesti dall'ASL di Latina entro il termine massimo di 96 ore.

Per quanto attiene all'espletamento delle attività evidenziate, il DPO, pur avvalendosi di uno staff tecnico, sarà il contatto principale per la ASL Latina, rapportandosi con la P.O. Coordinamento Privacy, il Team Aziendale Privacy e il Direttore della U.O.C. Affari Generali e Controllo Interno, fuorché ogni necessario confronto richiesto direttamente dalla Direzione Generale dell'AUSL Latina.

Nell'adempimento dei propri compiti, il DPO ed i componenti dello Staff, dovranno attenersi al segreto e alla riservatezza.

I dati di contatto del DPO saranno pubblicati sul sito aziendale e comunicati alle competenti autorità di controllo affinché possa essere contattato, sia dagli interessati che dalle autorità di controllo, in modo facile e diretto.

Al DPO sarà consentito l'accesso a tutte le strutture aziendali al fine di acquisire notizie, informazioni e documenti necessari per lo svolgimento dei propri compiti, anche mediante interviste al personale. L'accesso alle strutture aziendali sarà preceduto, di norma, da apposita comunicazione ai responsabili delle strutture medesime.

REQUISITI DI AMMISSIONE

Ai fini della partecipazione alla procedura di affidamento l'Aggiudicatario, a pena di esclusione, dovrà dichiarare il possesso dei seguenti requisiti:

- essere operatore economico legalmente costituito;
- avere esperienza pluriennale in attività di formazione e/o docenza, concernente le tematiche della protezione dei dati;
- avere erogato corsi di formazione, sulle tematiche della protezione dei dati, in almeno una azienda sanitaria pubblica;
- esperienza di consulenza, anche legale, riguardo alle tematiche legate alla privacy,
- non trovarsi in situazioni di inconferibilità/incompatibilità previste dal D.lgs. n. 39/2013;
- l'Aggiudicatario, il DPO nominato e i componenti dello staff tecnico di supporto al DPO, non siano stati destituiti o dispensati dall'impiego presso una pubblica amministrazione e/o presso soggetti privati, per persistente insufficiente rendimento, ovvero licenziati a seguito di procedimento disciplinare o per la produzione di documenti falsi o viziati da invalidità non sanabile;

Alla luce di quanto esposto l'Aggiudicatario, a pena di esclusione, dichiara che il DPO è in possesso di:

- alte qualità professionali, tra le quali, competenze giuridiche ed in particolare avere un'approfondita conoscenza in materia di Privacy della vigente normativa così come richiamato nell'art. 37 par. 5 del GDPR: "*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'articolo 39.*";
- laurea in legge o informatica o ingegneria (specialistica nuovo ordinamento o vecchio ordinamento);
- conoscenze in materia di organizzazione sanitaria;
- esperienza in materia di gestione e sicurezza informatica dei dati e delle informazioni nonché in materia di amministrazione digitale;
- esperienza di consulenza, anche legale, in favore di enti pubblici sanitari, riguardo alle tematiche legate alla privacy, diritto e sicurezza in materia di informatica ed internet, accesso e trasparenza in ambito sanitario;
- adeguata conoscenza delle norme e delle procedure amministrative applicabili;
- capacità di promuovere una cultura di protezione dei dati all'interno dell'organizzazione di una Azienda Sanitaria Locale e, dunque, sotto il profilo delle qualità personali, deve possedere elevati standard deontologici, quali la correttezza, lealtà ed integrità di condotta;
- competenze in materia di risk management e di analisi dei processi;
- un master universitario specifico sul Regolamento UE2016/679 o il possesso di un corso di almeno 120 ore con attestazione finale sulla gestione della privacy e sicurezza informatica o di precedenti incarichi relativi alla gestione dei dati personali ai sensi della Direttiva 95/46/CE.

L'Aggiudicatario partecipante, deve inoltre presentare, a pena di esclusione, la documentazione seguente:

- attestazione riferita ai nominativi dei componenti dello staff che affiancherà il DPO, alla quale dovranno essere allegati i rispettivi curricula ed evidenza del nominativo di un componente dello staff che, in caso di emergenza e di momentanea irreperibilità del DPO stesso, possa essere contattato dall'Azienda (n. cellulare e-mail etc.);

L'Aggiudicatario dovrà attestare altresì, che i componenti dello Staff sono in possesso di professionalità con competenze in materie giuridiche e informatiche.

CRITERI PER L'ATTRIBUZIONE DEI 50 PUNTI RELATIVI ALLA QUALITA'

MAX Punti 20: se l'Aggiudicatario, oltre ai requisiti richiesti, ha svolto incarichi di DPO in Aziende Sanitarie Pubbliche, altri Enti Pubblici o Privati:

La valutazione e la relativa attribuzione del punteggio avverrà secondo i seguenti parametri:

- 4 punti per ogni esperienza maturata in Aziende Sanitarie Pubbliche per periodi pari o superiori ai 18 mesi;
- 2 punti per ogni esperienza maturata in Aziende Sanitarie Pubbliche per periodi dai 12 ai 18 mesi;
- 1 punto per ogni esperienza maturata in altre Amministrazioni Pubbliche per periodi pari o superiori ai 18 mesi;
- **0,50** punto per ogni esperienza maturata in Enti Privati per periodi pari o superiori ai 18 mesi.

MAX Punti 15: se tutti i professionisti/collaboratori indicati partecipanti allo Staff dispongono di un master universitario specifico sul Regolamento UE2016/679 o il possesso di un corso di almeno 120 ore con attestazione finale sulla gestione della privacy e sicurezza informatica o di precedenti incarichi relativi alla gestione dei dati personali ai sensi della Direttiva 95/46/CE, altrimenti il punteggio di 15 sarà parametrato percentualmente per numero di laureati su numero componenti dello Staff.

MAX Punti 10: per il Progetto organizzativo delle attività che comprenda il Piano della formazione. La Commissione valuterà l'organizzazione del Piano della formazione e la metodologia degli incontri. Saranno valutati in modo favorevole i miglioramenti e le innovazioni apportate alle richieste (aumento dei partecipanti, ampliamento ore, etc.).

MAX Punti 5: relativamente alle pubblicazioni tecnico/scientifiche presentate in materia di applicazione delle norme di sicurezza ai sensi del Regolamento UE 2016/679, quali articoli su quotidiani e riviste specializzate, commenti, abstract. Il punteggio assegnato sarà di 1 punto per ogni pubblicazione.

Affinché il concorrente sia ammesso alla fase successiva della presente procedura è necessario che consegua un punteggio qualità pari o superiore a punti 26/50.

Saranno, pertanto, esclusi i concorrenti che conseguano punteggio qualità inferiore a punti 26.

DURATA - IMPORTO A BASE D'ASTA

Il contratto, avrà durata di 24 mesi, con possibilità di proroga per ulteriori 6 mesi.

La base d'asta è di euro 50.000,00 più IVA.

Paola Bellei

P.O. Coordinamento Privacy

ASL Latina