ASLNuoro
Azienda socio-sanitaria locale

**Spett.le Ditta**

**OGGETTO:** Richiesta preventivo per l'affidamento del Servizio di Data Protection Officer – DPO (Responsabile Protezione Dati Personali) per la durata di tre anni.

Questa ASL n. 3 di Nuoro intende procedere all'affidamento diretto dei servizi in oggetto previo interpello di più operatori economici.

Di seguito sono dettagliate le competenze e funzioni del DPO di cui al presente consulto:

Al DPO si richiederà di svolgere le attività e compiti propri del Responsabile per la protezione dei dati personali, avuto specifico riguardo a quanto allo stesso imputato dalla normativa vigente, e nello specifico:

a) informare e fornire consulenza al titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. Fanno parte di questo compito, a titolo indicativo e non esaustivo, le seguenti attività: promuovere la cultura della protezione dei dati all'interno dell'azienda dedicando alcune giornate alla formazione e momenti di incontro, anche attraverso tavoli di lavoro con i responsabili delle unità organizzative e/o con gruppi di dipendenti incaricati del trattamento;

b) dare indicazioni operative per il rispetto delle normative vigenti in materia di protezione dei dati personali;

c) rispondere a specifici quesiti posti dal Titolare, dagli Autorizzati e Responsabili al trattamento;

d) supportare, ove richiesto, i responsabili del procedimento dell'accesso documentale e dell'accesso civico per valutare la presenza e la posizione di eventuali controinteressati che si oppongano all'accesso per ragioni di tutela della riservatezza dei dati;

e) sorvegliare l'osservanza del GDPR e di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, nonché delle politiche del titolare 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. In particolare fanno parte di questo compito, a titolo indicativo e non esaustivo, le seguenti attività:

- raccolta di informazioni per individuare i trattamenti di dati personali svolgendi dall'Azienda, anche attraverso l'esame di documenti aziendali, l'accesso diretto agli uffici ed il confronto con il Titolare del trattamento e i Dirigenti incaricati;

- analisi dell'attuale modello organizzativo aziendale ("sistema privacy") e valutazione della sua conformità con il GDPR e con le altre disposizioni comunitarie e nazionali vigenti;

- attività di informazione, consulenza ed indirizzo nei confronti del Titolare. La suddetta attività si esplica anche mediante la formulazione di eventuali proposte di adeguamento del modello organizzativo o mediante la redazione di un nuovo modello;

- analisi e verifica della conformità dei trattamenti effettuati, rispetto alla designazione dei responsabili del trattamento, delle persone autorizzate ("incaricati") al trattamento e degli amministratori di sistema, rispetto alle modalità di implementazione dei diritti degli interessati (con particolare attenzione alle modalità in uso per l'informativa ed il consenso), rispetto alla adeguatezza delle policy di sicurezza adottate e concretamente attuate, rispetto alle modalità di pubblicazione di dati e documenti contenenti dati personali effettuata dall'Azienda per le varie finalità previste dalla legge, rispetto alle procedure di gestione delle violazioni dei dati.

f) fornire un parere in merito alle valutazioni d'impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment) e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR. In particolare fanno parte di questo compito, a titolo indicativo e non esaustivo, le seguenti attività:

- supportare il titolare del trattamento nella individuazione dei casi in cui sia necessario effettuare la DPIA;

- fornire indicazioni metodologiche per lo svolgimento delle DPIA ritenute necessarie e supportare il titolare nella stesura delle DPIA;

- valutare le salvaguardie da applicare, comprese le misure tecniche ed organizzative, per attenuare i rischi per i diritti delle persone interessate;

- valutare la correttezza delle DPIA effettuate dal titolare e se le conclusioni raggiunte siano conformi con i requisiti in materia di protezione dei dati;

- riesaminare periodicamente le DPIA effettuate e la eventuale necessità di effettuarne di ulteriori.

- cooperare con l'autorità di controllo. Oltre che con l'autorità di controllo il DPO dovrà supportare, promuovere e coordinarsi con i DPO eventualmente designati dai Responsabili esterni del trattamento che trattano dati per conto dell'Azienda;

g) 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 del GDPR, ed effettuare, ove necessario, consultazioni relativamente ad altre problematiche nell'ambito della protezione dei dati personali. Il DPO dovrà inoltre fungere da punto di contatto per gli interessati;

h) ove richiesto, dovrà partecipare ad incontri con ARES e il gruppo di lavoro dei DPO delle Aziende del SSR e supportare e promuovere nell'attuazione dei piani e progetti regionali di adeguamento al GDPR.

Il DPO è incaricato inoltre dei seguenti compiti:

- garantire la propria presenza fisica presso la sede della ASL e, se necessario, nelle varie strutture aziendali, secondo le modalità concordate con la Direzione;

- assicurare la propria presenza presso la sede Legale e, se richiesto, nelle varie strutture aziendali, ove ricorrano casi di avvio di attività ispettive da parte dell'Autorità Garante o di d*ata breach*;

- garantire il segreto e la riservatezza nell'adempimento dei propri compiti ai sensi dell'art. 38 par. 5 del Regolamento UE 2016/679 (GDPR);

- supportare e promuovere all'individuazione e valutazione dei rischi e definire le politiche di sicurezza: attività di valutazione, individuazione dei rischi ed attuazione di tutte le misure tecniche e organizzative adeguate per garantire e poter dimostrare che i trattamenti siano effettuati conformemente al GDPR;

- supportare e promuovere alla tenuta ed aggiornamento, per conto del Titolare, del registro delle attività di trattamento;

- dare consulenza nella stesura/aggiornamento/implementazione della documentazione relativa al sistema aziendale privacy: linee guida, misure minime di sicurezza, documenti e/o convenzioni con terze parti per la regolamentazione all'utilizzo dei dati, individuare eventuali situazioni di con titolarità, nell'ambito dei nuovi modelli organizzativi di tipo trasversale, aggiornamento o revisione delle clausole contrattuali standard da inserire nei testi dei contratti, degli atti e dei disciplinari di gara;

- supportare e promuovere alla individuazione e predisposizione di nuove pratiche operative (monitorare pratiche organizzative per identificare nuovi processi o modificare quelli esistenti al fine di garantire l'attuazione della Privacy by design);

- individuare le azioni correttive tecniche ed organizzative, atte a ridurre i gap e le relative priorità, con particola re riferimento alla sicurezza informatica ed alle misure organizzative e tecniche adeguate da implementare;

- effettuare l'analisi del sito web e l'eventuale predisposizione/aggiornamento della Privacy Policy del sito web aziendale conformemente alla normativa e revisione della Cookie Policy;

- supportare l'Azienda nella gestione documentale per tutta la documentazione prodotta sulla protezione dei dati, ai fini di esibizione a terzi, in linea con il principio di accountabily;

- 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;

- garantire la propria partecipazione nei casi in cui il Titolare coinvolga il DPO in questioni attinenti la protezione dei dati, sin dalla fase di progettazione di dette attività e comunque garantire la propria pronta reperibilità;

- riferire direttamente alla Direzione riguardo alle indicazioni raccomandazioni fornite nel quadro delle sue funzioni e fornire un report in riguardo al livello di conformità al GDPR;

- redigere una relazione annuale delle attività svolte da sottoporre alla Direzione;

- programmare l'attività di formazione ed aggiornamento annuale degli operatori, in accordo con l'Azienda, sulle problematiche e la legislazione concernente la materia del trattamento dei dati;

- supportare e promuovere nella mappatura della esternalizzazione dei trattamenti per quanto concerne i rapporti con i fornitori di servizi che trattano dati personali;

- fornire supporto nella predisposizione ed implementazione del processo di gestione e comunicazione dei c.d. *Data Breach*, di cui agli articoli 33 e 34 del GDPR;

I dati di contatto del DPO sono pubblicati e comunicati alle pertinenti autorità di controllo.

Il DPO non deve trovarsi in situazione che potrebbero anche potenzialmente configurare un conflitto di interessi.

Il Soggetto Aggiudicatario deve garantire competenze giuridiche e informatiche (es. in ambito di sicurezza informatica e cyber risk) oltre che organizzative.

L'importo annuale massimo posto a base del servizio di cui trattasi è ipotizzato in € 40.000,00;

Al netto delle attività obbligatorie sopra descritte che dovranno essere garantite, si richiede pertanto a Codesta Spett.le Società, se interessata, l'invio di una proposta nella quale dovranno essere dettagliate le modalità di espletamento del servizio richiesto e i relativi costi.
Si specifica quindi che le competenze e funzioni del DPO sopra descritte costituiscono un punto di riferimento non vincolante in ordine alla proposta di espletamento del servizio, pur con la ovvia e irrinunciabile garanzia che il risultato atteso consenta di adempiere ai relativi obblighi di legge.

**Requisiti generali richiesti ai soggetti che intendano presentare istanza di partecipazione;**

- Possesso dei requisiti per l'affidamento dei contratti pubblici ex artt. 94, 95, 96, 97, 98 e 100 del codice dei contratti (D. Lgs n. 36/2023);

**Requisiti professionali specifici richiesti ai soggetti che intendano presentare istanza di partecipazione**

- Possesso di diploma di laurea magistrale/specialistica in materie giuridiche/economiche/informatiche;
- Possesso di una conoscenza specialistica della normativa e delle prassi di gestione dei dati personali sia sotto l'aspetto giuridico che sotto quello informatico;
- Possibilità di adempiere alle proprie funzioni in piena indipendenza e in assenza di conflitti di interesse;
- Disponibilità di risorse umane e finanziarie necessarie all'adempimento dei suoi compiti;
- Eventuale attestato di esperto privacy e/o Data Privacy Officer DPO/responsabile della protezione dati –RPD rilasciato da ente indipendente possibilmente secondo la norma UNI 11697:2017;
- Eventuali ulteriori certificazioni nell'ambito della sicurezza informatica;
- Precedente espletamento di analoghe attività presso enti pubblici sanitari;

All'atto di presentazione della proposta di cui alla presente richiesta e ad integrazione della stessa, al fine di facilitare le fasi successive del procedimento, Codesta Ditta dovrà pertanto presentare idonea autocertificazione (ai sensi dell'art. 52 del D. Lgs 36/2023) redatta ai sensi dell'art. 47 del T.U. n. 445/2000, in ordine al possesso dei requisiti generali richiesti nella presente richiesta. In

tale autocertificazione dovranno altresì essere indicati i dati identificativi della ditta e dei rispettivi rappresentati legali e direttori tecnici. Lo schema di autocertificazione è allegato alla presente richiesta.

Analoga autocertificazione dovrà essere presentata relativamente al possesso dei requisiti specifici richiesti.

**Procedura di affidamento**

A seguito di un esame complessivo di ciascuna delle istanze pervenute, in mancanza di altri importanti elementi di valutazione che potranno essere desunti dalle proposte delle ditte interpellate, si darà rilevanza all'aspetto economico privilegiando l'offerta più bassa.

Si fa presente che, una volta individuato l'operatore economico che ha proposto l'offerta ritenuta più aderente ai fabbisogni della ASL di Nuoro, si procederà ad istruire la trattativa diretta su piattaforma MePa/SardegnaCat/Nert4Market per acquisire la restante documentazione finalizzata alla formalizzazione dell'affidamento e alla stipula del contratto.

Cordiali Saluti