CAPITOLATO TECNICO SPECIALE

GARA D'APPALTO NELLA FORMA DELLA PROCEDURA APERTA AI SENSI DEL COMBINATO DISPOSTO DEGLI ARTT. 36 E 60 DEL D.LGS 50/2016 e s.m.i., PER L'AFFIDAMENTO DEI SERVIZI DI CONSULENZA FINALIZZATI A GARANTIRE L'ADEGUAMENTO DELL'ASL DI LATINA AL REGOLAMENTO EUROPEO 679/2016 SULLA PROTEZIONE DEI DATI PERSONALI, DA AGGIUDICARSI SECONDO IL CRITERIO DELL'OFFERTA ECONOMICAMENTE PIU' VANTAGGIOSA EX ART. 95 comma 2 e 10- bis DEL D.LGS 50/2016 e s.m.i., ARTICOLATA IN UN UNICO LOTTO.

N. GARA 7064544

CIG 7467330BA5

OGGETTO DEL SERVIZIO

Oggetto del presente Capitolato è l'affidamento dei servizi, in materia di trattamento e protezione dei dati personali, per la messa a norma ed il conseguente rispetto degli adempimenti e obblighi previsti dal regolamento europeo (di seguito GDPR 2016/679), nonché dell'affidamento dell'incarico di Data Protection Officer (Responsabile della protezione dei dati di seguito RPD/DPO) a Soggetto esterno in possesso dei requisiti previsti dal citato GDPR 2016/679.
Adempimento primario sarà l'analisi dello stato attuale dell'impianto esistente (assetto organizzativo, regole aziendali, trattamenti etc.)
L'aggiudicatario (di seguito: "Aggiudicatario") è tenuto anche a fornire servizi di supporto normativo/giuridico/amministrativo/organizzativo e di formazione, al fine di permettere all'Azienda USL Latina (di seguito: "AUSL di Latina" o "Azienda") di adeguarsi agli adempimenti previsti dalla normativa privacy vigente.

ATTIVITA' RICHIESTE – REQUISITI DI AMMISSIONE A PENA DI ESCLUSIONE

La attività richieste sono rappresentate da tre linee di attività distinte: Prima Linea (Preliminare), Seconda Linea (Successiva) e Terza Linea (Finale).
La fase preliminare tende ad individuare tutte quelle attività richieste al fine di effettuare gli adempimenti e gli obblighi previsti dal nuovo regolamento europeo.
La fase successiva riguarda l'individuazione del DPO/RDP attraverso i requisiti e i compiti richiesti. La fase finale è orientata alla formazione del personale.
Per tutte le predette attività di consulenza dovrà essere garantita l'assistenza on site, secondo le modalità che saranno concordate, per un numero di giornate congrue rispetto alla finalità di pieno adeguamento dell'AUSL di Latina al nuovo GDPR ed alla vigente normativa privacy e, pertanto, alla realizzazione delle attività elencate nei punti precedenti. Pertanto, ciascun Concorrente dovrà presentare il proprio piano di lavoro nel quale saranno elencate le attività da svolgere e le relative tempistiche (cronoprogramma). La Prima Linea di attività dovrà concludersi entro il 31.12.2018.

ASL Latina
C.D.C. "Latina Fiori" Pal. G2 – V.le P. L. Nervi, snc
04100 Latina
t. +39.0773.6551
www.asl.latina.it
p.iva 01684950593

Prima Linea di attività: Definizioni delle Attività preliminari richieste

In questa prima fase, come anzidetto, si richiede all'Aggiudicatario di effettuare tutte quelle attività preliminari volte a definire un modello adeguato di funzionamento della data protection, nonché tutte quelle attività volte a porre in essere tutti i necessari adempimenti previsti per le Pubbliche Amministrazioni, quale l'adozione del Registro dei trattamenti dei dati personali, in specie:

- analisi finalizzata alla raccolta di tutte le informazioni sull'organizzazione aziendale, alla verifica del livello di conformità alla nuova normativa in materia di protezione dei dati ed alla misurazione del livello di esposizione dei rischi associati al trattamento dei dati;
- analisi e valutazione di tutta la documentazione che impatti sul trattamento dei dati (es.: i contratti con i fornitori che trattano dati);
- analisi e valutazione dei processi e delle procedure di gestione dei sistemi informativi, degli strumenti per la gestione della sicurezza informatica e dei sistemi di controllo esistenti all'interno dell'Azienda;
- individuazione e mappatura dei trattamenti effettuati, analisi delle tipologie dei dati trattati, delle finalità per cui sono trattati, dei termini di conservazione dei dati, delle categorie degli interessati e classificazione del rischio privacy, anche dei dati non strutturati. In particolare, l'Aggiudicatario dovrà effettuare la mappatura dei processi aziendali, dei trattamenti, svolgere interviste con il necessario grado di profondità nell'organizzazione aziendale al fine di predisporre il Registro dei Trattamenti dei dati personali.
  Il Registro dei trattamenti dovrà avere i contenuti minimi di cui all'art. 30 del GDPR 2016/679 e dovrà contenere una descrizione generale delle misure di sicurezza tecniche ed organizzative di cui all'art. 32 del GDPR 2016/679. Il Registro dei Trattamenti dovrà essere predisposto su apposito applicativo con memorizzazione su DBMS relazionale (Oracle, MS SQL o MySQL), strutturato in maniera tale da poter essere aggiornato e messo a disposizione dall'Aggiudicatario in favore dell'AUSL di Latina.
  Il registro dovrà essere strutturato in maniera tale da consentire le successive attività di risk assestment e impact assestment;
- elaborazione, redazione od aggiornamento/revisione di tutta la documentazione/modulistica affinché risulti completa ed aggiornata secondo la nuova normativa (es. testi delle informative e dei moduli per il consenso al trattamento dei dati, etc.);
- elaborazione, redazione o revisione delle clausole contrattuali standard da inserire nei testi dei contratti, degli atti e dei disciplinari di gara;
- individuazione di eventuali situazioni di contitolarità, l'Aggiudicatario dovrà assistere l'AUSL di Latina nell'individuare eventuali soggetti contitolari, ad esempio nell'ambito dei nuovi modelli organizzativi di tipo trasversale adottati per il trattamento della cronicità (denominati PDTA) e provvedere alla messa a disposizione di modelli standard di accordi di contitolarità;
- mappatura della esternalizzazione dei trattamenti, individuazione dei Responsabili esterni; l'Aggiudicatario, per quanto concerne i rapporti con i fornitori che trattano dati, dovrà assistere l'AUSL di Latina nell'individuare i Responsabili Esterni e dovrà provvedere alla messa a disposizione del modello standard di contratto che contenga la nomina e la disciplina del rapporto tra la AUSL di Latina e Responsabile esterno;
- mappatura della sub-esternalizzazione dei trattamenti, individuazione dei Sub-Responsabili Esterni dei trattamenti e regolarizzazione della designazione di Sub-Responsabili Esterni, mediante apposite previsioni nei contratti con i Responsabili Esterni oppure stesura e sottoscrizioni di nuovi contratti;

ASL Latina
C.D.C. "Latina Fiori" Pal. G2 – V.le P. L. Nervi, snc
04100 Latina
t. +39.0773.6551
www.asl.latina.it
p.iva 01684950593

- definizione dell'organigramma privacy finalizzato alla distribuzione dei ruoli e delle responsabilità interni all'azienda ai fini del trattamento dati e definizione dei flussi informativi tra le diverse figure coinvolte nel modello organizzativo di data protection;
- redazione di linee guida aziendali che contengano istruzioni operative e organizzative per tutte le figure aziendali coinvolte in materia di data protection (ad es. Manuale per l'adeguamento privacy);
- valutazione dei rischi e definizione delle politiche di sicurezza: attività di valutazione, individuazione dei rischi ed attuazione di tutte le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare che i trattamenti siano effettuati conformemente al GDPR;
- attività di valutazione d'impatto sulla protezione dei dati (DPIA "Data Protection Impact Assessment"), l'Aggiudicatario deve assistere l'AUSL di Latina nell'individuare tutti quei trattamenti dai quali possa derivare un rischio elevato per la libertà e per i diritti degli utenti interessati, nell'individuare i rischi derivanti da tali trattamenti e gli strumenti più idonei per contrastarli (misure tecniche e organizzative da adottare e implementare);
- predisposizione e implementazione del processo di gestione e comunicazione Data Breach con conseguente stesura e attivazione del Registro di Violazione dei dati;
- individuazione e monitoraggio nuove pratiche operative (monitorare pratiche organizzative per identificare nuovi processi o modificare quelli esistenti, al fine di garantire l'attuazione della Privacy by design);
- predisposizione e implementazione dei processi per la gestione delle richieste di accesso ai dati personali oggetto di gara e di esercizio degli altri diritti da parte degli interessati (es.trasportabilità dei dati ed oblio);
- predisposizione e definizione del Remediation Plan: individuazione delle azioni correttive tecniche ed organizzative, atte a ridurre i gap individuati e le relative priorità, con particolare riferimento alla sicurezza informatica ed alle misure organizzative e tecniche adeguate da implementare;
- predisposizione/aggiornamento della regolamentazione aziendale in tema di trattamento dei dati personali (a titolo esemplificativo e non esaustivo: predisposizione di protocolli interni che regolamentano il corretto utilizzo di internet, posta elettronica e social network da parte dei dipendenti e/o collaboratori, il corretto utilizzo da parte dei dipendenti e/o collaboratori dei device aziendali, della realizzazione e diffusione delle riprese audio-video all'interno delle strutture sanitarie da parte degli utenti, dell'utilizzo di firme grafometriche);
- analisi del sistema di videosorveglianza e proposta di aggiornamento alla normativa vigente.

<u>Seconda Linea di attività: Affidamento del DPO/RDP. Compiti e Requisiti-Affiancamento Team</u>

Oltre alle attività indicate nei punti precedenti, si riportano i compiti del DPO/RDP previsti dall'art. 39 del GDPR, di seguito indicati (a titolo non esaustivo):

- redigere un piano di lavoro;
- informare e fornire consulenza, informazione ed indirizzo al Titolare del trattamento ed al Referente aziendale privacy in merito agli obblighi vigenti relativi alla protezione dei dati; il servizio di consulenza assolve altresì alla finalità di rispondere a singoli quesiti istituzionali in materia di privacy;
- sorvegliare l'osservanza della nuova normativa in materia, nonché delle politiche del Titolare del trattamento relative alla protezione dei dati personali;

ASL Latina
C.D.C. "Latina Fiori" Pal. G2 – V.le P. L. Nervi, snc
04100 Latina
t. +39.0773.6551
www.asl.latina.it
p.iva 01684950593

- assistere il Titolare del trattamento nel controllo del rispetto a livello interno del GDPR;
- supportare l'AUSL di Latina nella gestione documentale prodotta 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;
- cooperare e fungere da punto di contatto con l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR 2016/679 ed effettuare, se del caso, consultazioni relativamente ad ogni altra questione;
- 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. In ogni caso il DPO può consultare l'autorità di controllo con riguardo a qualsiasi altra questione;
- rappresentare un punto cardine per gli interessati in merito al trattamento dei loro dati personali e/o sensibili e all'esercizio dei diritti, comunicando con gli interessati in modo efficiente;
- cooperare e supportare il Responsabile della Trasparenza e dei singoli RUP aziendali (Responsabile Unico del Procedimento) 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;
- considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo: il DPO deve definire un ordine di priorità nell'attività svolta e concentrarsi sulle questioni che presentino maggiori rischi in termini di protezione dei dati, senza trascurare di sorvegliare altri trattamenti associati ad un livello di rischio inferiore;
- 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 2016/679 e supportare il titolare nell'esecuzione delle attività necessarie per effettuare la valutazione d'impatto e l'eventuale riesame;
- 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 secondo le esigenze della AUSL Latina;
- riferire direttamente alla Direzione Generale dell'AUSL di Latina riguardo alle indicazioni e raccomandazioni fornite nel quadro delle sue funzioni, nonché un reporting riferito al livello di conformità al GDPR;
- redigere e trasmettere alla Direzione Generale dell'AUSL di Latina, una relazione annuale delle attività svolte;
- supportare l'AUSL di Latina nella predisposizione e gestione di specifici audit privacy sia interni che esterni;
- programmare l'attività di formazione ed aggiornamento annuale dei dipendenti dell'AUSL di Latina, in accordo con la UOC Formazione, per le problematiche e la legislazione concernente la materia del trattamento dei dati;
- evadere i quesiti in materia di privacy richiesti dall'AUSL di Latina entro il termine massimo di 7 (sette) giorni (di calendario).

Nell'adempimento dei propri compiti, il DPO dovrà attenersi al segreto e alla riservatezza.
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.

ASL Latina
C.D.C. "Latina Fiori" Pal. G2 – V.le P. L. Nervi, snc
04100 Latina
t. +39.0773.6551
www.asl.latina.it
p.iva 01684950593

Il DPO dovrà svolgere il proprio ruolo dedicando all'AUSL Latina un tempo adeguato rispetto ai compiti previsti e assegnati, utilizzando le risorse umane e strumentali interne alla propria Società.
Il DPO si rapporta con il Dirigente responsabile della U.O.C. Affari Generali e Controllo Interno, fuorché ogni necessario confronto richiesto direttamente dalla Direzione Generale dell'AUSL Latina
Al DPO è 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.

Alla luce di quanto esposto il DPO deve possedere:

- alte qualità professionali, tra le quali, competenze giuridiche ed in particolare avere un'approfondita conoscenza in materia di Privacy, sia della vigente normativa sia del nuovo GDPR, nonché delle prassi nazionali ed europee in materia di tutela, protezione e trattamento dei dati;
- conoscenze in materia di organizzazione sanitaria;
- esperienza su tematiche legate alla privacy, alla gestione e sicurezza informatica dei dati e delle informazioni e della trasparenza in ambito sanitario;
- esperienza di consulenza, anche legale, in favore di enti pubblici/privati accreditati con il SSN, riguardo alle tematiche legate alla privacy, diritto informatico ed internet, amministrazione digitale, accesso e trasparenza;
- 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.
- Il DPO non deve trovarsi in situazione che potrebbe anche potenzialmente configurare un conflitto di interessi.

L'Aggiudicatario, al fine di una maggior efficienza del servizio erogato in favore dell'AUSL di Latina e stante la complessità della struttura (comprendente, tra l'altro, Strutture Ospedaliere e Strutture Distrettuali), dovrà affiancare al DPO un team specializzato in grado di completare il profilo professionale del DPO come sopra definito e di svolgere le attività di consulenza e formative previste nel presente Capitolato Speciale.
Si specifica che l'Aggiudicatario deve garantire nel Team specializzato di supporto (Staff tecnico) la presenza di competenze professionali in materie giuridiche e materie informatiche.
Si specifica che anche il singolo componente del team specializzato non deve trovarsi in situazione che potrebbe anche potenzialmente configurarsi un conflitto di interesse.
Per garantire le prestazioni previste, il DPO, pur potendosi avvalere di un team (staff tecnico), funge da contatto principale; per tale ragione è necessaria una chiara ripartizione dei compiti del team.

Terza linea di attività: la Formazione

In questa terza linea si chiede all'Aggiudicatario di effettuare l'attività di formazione del personale dipendente e/o dei collaboratori coinvolti nel modello organizzativo di Data Protection, con la previsione di corsi di diverso livello per le figure interessate;
La formazione proposta sarà articolata al termine della Seconda Linea di attività di cui ai precedenti punti. I destinatari del corso saranno max 200 partecipanti. L'evento avra la durata minima di 6 ore per

ASL Latina
C.D.C. "Latina Fiori" Pal. G2 – V.le P. L. Nervi, snc
04100 Latina
t. +39.0773.6551
www.asl.latina.it
p.iva 01684950593

gruppi omogenei di non oltre 30 partecipanti e dovrà prevedere, oltre ad una sintesi del contesto giuridico di riferimento, l'illustrazione delle azioni attuate e da attuare da parte dell'AUSL Latina, ai fini di compliance GDPR, nonché l'illustrazione di casi pratici/esercitazioni volte a coinvolgere e sensibilizzare i Destinatari del corso.
Nel corso degli eventi sarà presentato il DPO, il quale dovrà illustrare i propri compiti ed il tipo di supporto che può fornire agli interessati.
L'evento formativo in aula sarà ripetuto una seconda volte nell'arco dei 18 mesi.

CRITERI PER L'ATTRIBUZIONE DEI PUNTI RELATIVI ALLA QUALITA'

70 PUNTI

MAX Punti 10: per l'esperienza maturata "in toto" dalla Società/Gruppo partecipante, relativamente ad affidamenti in materia di privacy presso Amministrazioni Pubbliche/Enti o Privati. La valutazione e la relativa attribuzione del punteggio avverrà secondo i seguenti parametri:

- 2 punti per ogni esperienza maturata nelle Pubbliche Amministrazioni o Enti Pubblici o Privati a carattere sanitario;
- 1 punto per ogni esperienza maturata nelle altre Amministrazioni Pubbliche o Enti Privati.

MAX Punti 10: per la qualità del progetto sviluppato attraverso le tre Linee di Attività. La Commissione valuterà in modo particolare il Cronoprogramma e la tempistica relativa alla prima linea di attività, secondo i criteri di seguito riportati:

- 5 punti per la conclusione della prima linea di attività entro il 31 ottobre 2018
- 2 punti per la conclusione della prima linea di attività entro il 30 novembre 2018
- 0 punti per la conclusione della prima linea di attività entro il 31 dicembre 2018.

MAX Punti 10: se il DPO, oltre ai requisiti richiesti, ha svolto incarichi relativi alla gestione dei dati personali ai sensi della Direttiva 95/46/CE in pubbliche amministrazioni;
MAX Punti 10: se il DPO, oltre ai requisiti richiesti, svolge incarichi relativi alla gestione dei dati personali ai sensi del Regolamento UE 2016/679 in pubbliche amministrazioni;
MAX Punti 10: se tutti i professionisti/collaboratori indicati partecipanti al team di lavoro, compreso il DPO sono in possesso di una delle seguenti lauree: economia e commercio, ingegneria informatica, ingegneria gestionale, informatica, giurisprudenza, scienze politiche, altrimenti il punteggio di 10 sarà parametrato percentualmente per numero di laureati su numero componenti del team;
MAX Punti 5: per la qualità del software offerto per il mantenimento del Registro dei Trattamenti e il supporto all'attività di analisi del rischio. La Commissione procederà ad attribuire tale punteggio in base alla valutazione: della semplicità d'uso, della gestione interfaccia utente e della integrabilità del software di terze parti;
MAX Punti 5: se tutti i professionisti/collaboratori indicati partecipanti al team di lavoro, compreso il DPO, dispongono o di precedenti incarichi relativi alla gestione dei dati personali ai sensi della Direttiva 95/46/CE, o un master universitario specifico sul Regolamento UE2016/679, o superamento di un corso di almeno 120 ore con attestazione finale sulla gestione della privacy e sicurezza informazioni altrimenti il punteggio di 5 sarà parametrato percentualmente per numero di laureati su numero componenti del team;

ASL Latina
C.D.C. "Latina Fiori" Pal. G2 – V.le P. L. Nervi, snc
04100 Latina
t. +39.0773.6551
www.asl.latina.it
p.iva 01684950593

MAX Punti 5: a soggetti che presentano pubblicazioni tecnico/scientifiche 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;
MAX Punti 5: per il Piano della formazione. La Commissione valuterà l'organizzazione del Piano della formazione, la metodologia degli incontri. Saranno valutati in modo favorevole i miglioramenti e le innovazioni apportate alle richieste (aumento dei partecipanti, ampliamento ore, etc.).

Firmato

Dr. Andrea Verrillo
Coll. Tecn. Prof. Programmatore

Paola Bellei
Coll. Amm. Prof

Latina, lì 23 aprile 2018

ASL Latina
C.D.C. "Latina Fiori" Pal. G2 – V.le P. L. Nervi, snc
04100 Latina
t. +39.0773.6551
www.asl.latina.it
p.iva 01684950593