Unione dei Comuni di Bientina, Buti, Calcinaia, Capannoli,
Casciana Terme Lari, Palaia, Pontedera

Zona Valdera - *Provincia di Pisa*

Capitolato prestazionale per il servizio di data protection office

Le attività principali dell'Unione Valdera e dei comuni aderenti comportano il trattamento di dati personali e sensibili, anche giudiziari, tali da rendere necessaria la designazione e il supporto di un Data Protection Officer (D.P.O.), ai sensi dell'art. 37 del Regolamento UE 2016/679 sulla protezione dei dati (d'ora in avanti GDPR), come meglio specificato nel prosieguo. Relativamente all'Unione, l'Ente individuerà, tra le risorse umane proprie, un gruppo di lavoro composto da diverse professionalità, che svolgerà le funzioni richieste in collaborazione con il Data Protection Officer [o Responsabile della Protezione dei Dati]. In generale, il DPO non svolgerà direttamente le attività necessarie, ma guiderà il personale nella loro esecuzione, fatte salve le competenze in materia di supervisione e verifica.
Il presente affidamento è pertanto finalizzato ad attribuire il ruolo di Responsabile della Protezione Dati (D.P.O.) per l'Unione e gli enti aderenti, nonché a supportare, formare e indirizzare il gruppo di lavoro costituito in ambito Unione, in modo che sia in grado di gestire al meglio gli adempimenti e le misure previste dal GDPR. Le prestazioni indicate all'articolo successivo potranno essere richieste al soggetto aggiudicatario da ulteriori enti convenzionati con l'Unione Valdera (oltre cioé quelli aderenti).
Il servizio consiste nella definizione del processo per il mantenimento e l'implementazione del sistema di gestione della Privacy e nella nomina del D.P.O. Data Protection Officer- Responsabile della Protezione dei Dati dell'Unione e dei Comuni associati, per una durata di due anni e in particolare:
a) consulenza e/o formazione ai responsabili del trattamento sugli obblighi derivanti dal GDPR e dai provvedimenti e linee guida dell'Autorità Garante Privacy, nonché sul bilanciamento di queste con le disposizioni vigenti in tema di trasparenza e accessibilità amministrativa;
b) supervisione della mappatura degli archivi elettronici, web e cartacei, individuazione e definizione degli schemi di trattamento dei dati rispetto alle singole unità di archiviazione;
c) valutazione sulla completezza e correttezza degli adempimenti effettuati in materia di trattamento e sicurezza dei dati, fornendo un report generale che evidenzi il relativo grado di conformità o di parziale o totale non conformità e il percorso proposto di adeguamento;
d) supporto e consulenza per i rapporti eventuali con il Garante Privacy;
e) assistenza nell'aggiornamento della regolamentazione sul trattamento dati personali;
f) somministrazione di formazione specifica sulle tematiche della protezione dei dati a favore dei dipendenti;
g) formazione e/o informazione specifica, per le diverse professionalità che compongono i gruppi di lavoro in materia di protezione dei dati (formazione giuridica, formazione in campo informatico);
h) collaborazione e supervisione nella predisposizione di linee guida, disposizioni operative, modulistica e policy applicative relative alla protezione dei dati personali;
i) controllo circa la corretta individuazione dei soggetti interessati al trattamento (utenti, cittadini-persone fisiche e persone giuridiche, dipendenti/collaboratori, fornitori, etc.);
l) verifica e indicazioni per l'adeguamento delle informative per il trattamento dei dati;
m) verifica dei requisiti dei fornitori di servizi per i quali vi è un trattamento e definizione delle clausole contrattuali minime per garantire adeguata protezione dei dati;
n) stesura del prototipo del registro dei trattamenti;
o) supporto alla predisposizione o revisione dell'analisi dei rischi che incombono sui dati;
p) individuazione di ulteriori misure "adeguate" ai sensi dell'art.32 GDPR;
q) verifica del sito internet ed implementazione adempimenti conseguenti (indicazioni delle modalità e testi per le informative, cookie law, privacy policy, form di raccolta dati ecc);
r) verifica delle modalità di gestione dei sistemi di videosorveglianza, trasparenza, geolocalizzazione,dati biometrici;
s) stesura del registro violazioni di sicurezza.

Le attività sopra indicate saranno svolte attraverso:
• lo sviluppo di un corso di formazione specifico, progettato insieme al Dirigente responsabile, i cui partecipanti interagiranno con i rispettivi enti di appartenenza allo scopo di rilevare la situazione esistente nei diversi ambiti operativi, valutarla all'interno del percorso di formazione, individuando soluzioni tipo relativamente ai diversi adempimenti per il mantenimento/ implementazione del sistema di gestione della privacy, da 'riportare' nei rispettivi enti.
Tale corso, della durata indicativa di 12 ore, articolato in un minimo di 3 diverse giornate;
• la partecipazione alle riunioni del gruppo di lavoro appositamente costituito, in un numero complessivo indicativo di 5 incontri di 3 ore ;
• numero 42 mezze giornate (4/5 ore) da effettuarsi presso i diversi enti interessati, anche in successione nella stessa giornata, per la supervisione e verifica dei processi di adeguamento alla normativa di cui ai punti sopra riportati;
• una consulenza a distanza, a mezzo posta elettronica, da svolgersi in forma continuativa nel periodo dell'affidamento.