Servizio di Assistenza tecnico-giuridica e soluzione software a supporto per l'attuazione del nuovo regolamento europeo 2016/679/UE in materia di Privacy

Il servizio deve consentire nell'ambito delle seguenti fasi:

FASE 1) l'acquisizione delle informazioni, mediante le seguenti attività:

1. Mappatura degli archivi elettronici, web e cartacei, individuazione e definizione degli schemi di trattamento dei dati rispetto alle singole unità di archiviazione;
2. Verifica della liceità dei trattamenti, delle modalità tecniche e delle misure di protezione adottate;
3. Individuazione dei soggetti interessati al trattamento (utenti, cittadini - persone fisiche e referenti delle persone giuridiche, dipendenti/collaboratori, fornitori, etc.);
4. Individuazione delle figure gerarchiche di responsabilità quali:
5. titolare del trattamento/responsabile del trattamento;
6. affidatari esterni e/o cotitolari;
7. responsabili esterni del trattamento/clausole per l'affidamento di servizi esternalizzati;
8. amministratori di sistema;
9. incaricati al trattamento;
10. fornitori di servizi esterni - verifica ed eventuale integrazioni nella contrattualistica;
11. trattamenti dati intra/extra UE.

FASE 2) l'elaborazione dei documenti mediante la predisposizione della seguente documentazione:

1. Stesura delle informative per il trattamento dei dati;
2. Verifica dei requisiti dei fornitori di servizi per i quali vi è un trattamento (e/o implementazione di misure di protezione dei dati) e stesura delle clausole contrattuali minime per garantire adeguata protezione dei dati;
3. Stesura del registro dei trattamenti, procedura per la gestione del Data Beach, implementazione dei principi di accountability, privacy by design, privacy by default e relative evidenze ove applicabili - NUOVI adempimenti richiesti dal Regolamento Europeo;
4. Revisione dell'analisi dei rischi che incombono sui dati e, ove applicabile valutazione d'impatto - NUOVO adempimento richiesto dal Regolamento Europeo;
5. Verifica dell'applicazione delle "misure minime" di sicurezza (ex allegato B) D.Lgs. n.196/03 e individuazione di ulteriori misure "adeguate" - NUOVO adempimento richiesto dal Regolamento Europeo;
6. Definizione delle modalità di gestione degli adempimenti relativi al Provvedimento a carattere generale del Garante per la protezione dei dati personali inerenti alla figura dell'Amministratore di sistema;
7. 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);
8. Verifica delle modalità di gestione inerenti a videosorveglianza, trasparenza, regolamenti, geolocalizzazione, dati biometrici;
9. Eventuali integrazioni di aspetti giuslavoristici inerenti all'utilizzo degli strumenti di lavoro aziendali in affidamento al personale dipendente;
10. Verifica ed eventuale integrazione del Regolamento per il trattamento dei dati personali sensibili e giudiziari;
11. Consegna dei documenti seguente al necessario lavoro di back-office.

Fornitura software amministrativo-gestionale

Il software deve consentire di elaborare tutti gli adempimenti amministrativi imposti dal nuovo Regolamento Europeo, compresa la creazione del registro del trattamento in capo al titolare e a tutti i responsabili, consentendo di effettuare le seguenti attività:

- Analisi del rischio: definizione dell'Elenco dei processi/attività dell'Ente raggruppati in indici di trattamento che presentino rischi analoghi in termini di natura, ambito di applicazione, contesto, finalità e rischi.
  Gli *Elenchi Trattamenti* dei dati personali devono consentire di applicare una "singola valutazione" del rischio ad una pluralità di trattamenti (art. 35 GDPR).
  Il software deve consentire la generazione ed il costante aggiornamento delle informazioni essendo gli elenchi strumentali alla valutazione e al trattamento del rischio.
  Il sw deve consentire la definizione della mappatura, della struttura organizzativa, dei soggetti, luoghi e risorse.
  Il sw deve consentire di generare e tenere costantemente aggiornate le Mappe/Elenchi della struttura organizzativa, dei soggetti e delle relative responsabilità e profilazioni, dei luoghi e delle risorse. Tali mappe/elenchi sono strumentali alla valutazione e al trattamento del rischio e vanno conservate agli atti del sistema di sicurezza o allegate al Piano della sicurezza dei dati personali.
- Valutazione del rischio: il sw deve consentire la determinazione preliminare della possibilità che il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, effettuata sulla base dei criteri previsti dalle linee guida, con formazione dell'elenco dei trattamenti da sottoporre a DPIA (valutazione d'impatto); le informazioni precaricate devono consentire di attuare le seguenti attività:
  - descrizione sistematica del contesto,
  - valutazione della necessità e proporzionalità dei trattamenti,
  - valutazione dei rischi per i diritti e le libertà degli interessati,
  - individuazione delle misure previste per affrontare ed attenuare i rischi,
  - monitoraggio e riesame.
- Trattamento del rischio: il sw deve gestire il registro dei trattamenti, la sua compilazione e il costante aggiornamento. Oltre alle informazioni obbligatorie il sw deve consente di inserire nel registro ulteriori informazioni che il titolare intende evidenziare quali almeno:
  - Descrizione e del flusso informativo;
  - Finalità;
  - Categoria di dati/interessati/destinatari;
  - Misure di sicurezza tecniche logistiche ed informatiche;
  - Misure di sicurezza organizzative e procedurali.

Servizio di Responsabile della Protezione dei Dati Personali (RDP) ovvero Data Protection Officer (DPO) per l'attuazione del Regolamento UE 2016/679

1. Il servizio dovrà prevedere lo svolgimento dei compiti del Responsabile della Protezione dei Dati Personali (RDP) ovvero Data Protection Officer (DPO), in riferimento all'art. 39 del Regolamento UE 2016/679 per le attività di seguito indicate:
   a) Informare e fornire assistenza al titolare del trattamento o dal responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento europeo 2016/679 non che da altre disposizioni relative alla protezione dei dati;
   b) Sorvegliare l'osservanza del regolamento, di altre disposizioni 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 della responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   c) Fornire, se richiesto, un parere in merito alla valutazione dell'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento;
   d) Cooperare con l'autorità di controllo;

e) 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, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
f) Si preventivano n. 3 (tre) visite annuali, a fronte delle quali saranno redatte altrettante relazioni in funzione alle attività contrattualizzate;

2. Verifica per l'attuazione dei livelli di sicurezza in merito alle "misure minime per la sicurezza ICT" emanate dall'AGID (Agenzia dell'Italia Digitale) in attuazione della Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri.
3. Formazione presso l'Ente degli operatori incaricati e responsabili con rilascio di attestato di partecipazione;
4. Affiancamento all'Ente in sede di verifiche o ispezioni del garante.