CAPITOLATO TECNICO

"Servizio di Consulenza e Supporto per l'Adeguamento dell'Ente al Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"

GRUPPO SALERNO ENERGIA

OGGETTO DEL SERVIZIO

Servizio di consulenza e supporto in materia di protezione dei dati personali per la messa a norma ed il conseguente rispetto degli adempimenti e obblighi previsti dal Regolamento europeo n. 679/2016 (General Data Protection Regulation – GDPR) per il Gruppo Salerno Energia.

Si specifica che nel Gruppo Salerno Energia sono comprese le seguenti società:
- Salerno Energia Holding S.p.A. (Capogruppo);
- Salerno Energia Distribuzione S.p.A.
- Salerno Sistemi S.p.A.
- Sinergia S.u.r.l.

Ogni società stipulerà singolo contratto con l'operatore economico affidatario del servizio ed il referente contrattuale sarà il Responsabile Privacy della singola società.

DESCRIZIONE DEL SERVIZIO DA EROGARE ALLA SINGOLA SOCIETA'

Il servizio di affiancamento/supporto per adeguamento al GDPR comprende servizi di supporto tecnico, informatico, giuridico, in grado di affiancare l'Organizzazione nelle attività di analisi del proprio modello di gestione della privacy onde poterne ricavare tutti gli elementi necessari per la relativa revisione in ottica GDPR in conformità con l'obiettivo dell'accountability normativamente previsto.

L'offerta deve prevedere le seguenti macroattività:

1) **Assessment relativo al General Data Protection Regulation (GDPR)**

Si richiede, alla luce di una verifica puntuale dei dati e dei documenti trattati e della loro classificazione, un'indagine esaustiva sulle attuali modalità di trattamento dei dati personali e sulle modalità con cui la Società li gestisce e li protegge.

E' richiesta, quindi, una Gap Analysis Review per contestualizzare la metodologia prevista rispetto alla specifica realtà di intervento, mappandovi i requisiti previsti dal GDPR, e definendo un Piano di allineamento al Regolamento (UE) 2016/679.

L'esecuzione di un assessment della situazione as-is, comprensiva di gap analysis e valutazione di impatto e di rischio, dovrà prevedere un'ampia rilevazione dell'esistente che necessariamente dovrà verificare la tipologia dei dati trattati suddividendoli secondo le classificazioni del Regolamento

suddetto, e come gli stessi vengono trattati in base alla normativa attualmente vigente (codice della privacy). Si dovrà poi verificare l'operatività posta in essere in merito al trattamento dei dati e se la stessa è in linea con la normativa prevista.

2) ***Definizione dei modelli organizzativi e delle procedure in Materia di Protezione dei Dati Personali***

Sulla base delle rilevazioni effettuate, dovranno essere individuati i soggetti titolati al trattamento dei dati, suddivisi per competenze e ruoli, dovranno essere certificate le procedure interne per la raccolta del consenso, per l'informativa e per tutti gli altri adempimenti previsti dalla normativa vigente; saranno revisionati o redatti i testi delle informative e dei consensi al trattamento dei dati personali, ed alle logiche di conservazione, così come i testi degli incarichi e delle nomine al trattamento secondo il GDPR; dovrà essere redatto il Piano di Valutazione d'impatto sui Dati Personali per quelle funzioni aziendali/strutture che presentano rischi specifici per i diritti degli utenti interessati e tutte le altre procedure previste, con riguardo in particolare alla Data Breach *Notification/Communication Management*.

In particolare dovranno essere effettuate le attività di seguito elencate:

- ✓ analisi finalizzata all'identificazione degli obiettivi, alla raccolta delle informazioni, alla verifica del livello di conformità alla normativa in materia di protezione dei dati, misurazione del livello di esposizione dei rischi associati al trattamento dei dati;
- ✓ individuazione e mappatura dei trattamenti dei dati personali effettuati con strumenti cartacei, elettronici e/o informatici, analisi della tipologia dei dati trattati, delle finalità per cui sono trattati e degli interessati e classificazione del rischio privacy, anche dei dati non strutturati;
- ✓ predisposizione delle "**valutazioni di impatto**" (Data Protection Impact Assessment - DPIA), particolarmente per quelle considerate "obbligatorie" dalla normativa, e individuazione delle misure idonee atte a garantire le prescrizioni della norma, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento;
- ✓ predisposizione della procedura di gestione degli incidenti/data breach e conseguente attivazione del **registro di violazione dei dati**;
- ✓ analisi dei sistemi di videosorveglianza e aggiornamento alla normativa vigente;
- ✓ individuazione delle misure organizzative e tecniche che consentano di avere un controllo continuo sulla conformità alla normativa;
- ✓ strategia di gestione dei rischi privacy;
- ✓ attivazione del registro dei trattamenti eseguiti dalle terze parti;
- ✓ predisposizione/aggiornamento della regolamentazione aziendale in tema di trattamento dei dati personali;
- ✓ elaborazione, redazione od aggiornamento dei moduli per il consenso, delle informative sul trattamento dei dati personali, degli atti di nomina dei responsabili, degli incaricati;
- ✓ consulenza sugli obblighi derivanti dal GDPR e dalle ulteriori disposizioni legislative, provvedimenti e linee guida del Garante e conseguente aggiornamento del sistema privacy;
- ✓ strutturazione di un organigramma privacy finalizzato alla distribuzione

delle responsabilità interne all'azienda del trattamento dati.

Si richiede al concorrente di specificare le modalità di lavoro (organizzazione, interlocutori coinvolti, ecc.) per la copertura delle fasi sopra citate.
In particolare si richiede di indicare come si intende operare al fine di procurare il minor aggravio possibile all'operatività della Società.
Il concorrente indichi inoltre i deliverable che intende rilasciare e gli eventuali elementi migliorativi offerti.
Tra gli elementi migliorativi offerti sarà presa in particolare considerazione la possibilità di: una adeguata modalità di supporto continuativo per lo svolgimento delle attività previste dal GDPR e la possibilità di arricchire quanto sopra richiesto con un adeguato ausilio ai ruoli particolari, identificati dal GDPR, presenti in Azienda.

3) ICT Assessment

In questa fase dovrà essere analizzato lo stato attuale dell'infrastruttura della Società, valutando nel dettaglio l'organizzazione, i processi presenti, le policy applicate, l'infrastruttura fisica e le funzionalità applicative dei sistemi al fine di produrre un inventario degli asset utile anche per le fasi successive.
Per quanto riguarda la parte "Infrastruttura ed Applicazioni" sono richieste le attività di verifica delle Postazioni di Lavoro (sia in termini di sicurezza che di gestione), delle modalità di inventariazione delle componenti ICT e definizione delle best practices operative, la valutazione dell'adeguatezza dei controlli sull'infrastruttura nella logica della gestione, evoluzione e governo degli asset; dovrà essere verificata la presenza di procedure appropriate per il governo dei processi, ed un'analisi dei criteri di sicurezza degli applicativi dal punto di vista della robustezza e protezione dei dati; dovrà essere effettuata una valutazione omnicomprensiva del processo di assistenza ICT nella sua completezza, indicandone le falle operative o le carenze e indicando le possibili evoluzioni di processo verso un sistema di troubleticketing per la registrazione di Incidenti e Problemi.
Per quanto riguarda la Sicurezza, viene richiesta un'analisi del rischio informatico e delle attuali pratiche adottate per la protezione dei dati, incluse le metodologie in uso per Disaster Recovery/Business Continuity, con l'obiettivo di mitigare il rischio identificato intraprendendo le azioni che vanno descritte nel ***Piano delle Azioni Correttive***.
Sono incluse in questa fase specifiche indagini tipiche della "***Sicurezza Informatica***", che si rilascia al committente indicare e definire nel dettaglio.
In relazione alle attività di "***Gestione del Rischio***" si richiede l'individuazione della prassi migliore per l'attenuazione del rischio informatico e con quali modalità tracciarlo e mitigarlo, sia per le applicazioni in esercizio che per le nuove iniziative.

Si richiede al concorrente di specificare le modalità di lavoro (organizzazione, interlocutori coinvolti, ecc.) per la copertura delle fasi sopra citate.
In particolare si richiede di indicare come si intende operare al fine di procurare il minor aggravio possibile all'operatività della Società.
Il concorrente indichi inoltre i deliverable che intende rilasciare e gli eventuali elementi migliorativi offerti.

4) AUDIT

Il processo di audit degli adempimenti connessi al GDPR è necessario per poter verificare tutte le misure tecniche ed organizzative adottate, con particolare attenzione alla documentazione ed alle registrazioni da conservare per poter dimostrare il rispetto e l'applicazione del principio di "accountability" sia del titolare sia dei responsabili del trattamento dei dati.

Il servizio deve, pertanto, comprendere almeno n. 1 audit sul sistema di Governance della Privacy implementato.

5) ATTIVITA' DI FORMAZIONE

Il servizio comprende l'attività di formazione obbligatoria a favore del management aziendale, dei dirigenti di struttura e del personale addetto sulle responsabilità connesse con la sicurezza e protezione dei dati.

Il concorrente deve presentare uno specifico programma di formazione. Le attività di formazione dovranno essere erogate presso la sede della Società.

Sarà cura del concorrente definire il numero minimale di sessioni, la relativa durata ed il numero massimo di partecipanti.

Le sessioni di formazione saranno oggetto di specifico accordo tra la Società ed il concorrente.

DELIVERABLE

Costituiranno deliverable minimale i seguenti documenti:

- *Elenco banche dati;*
- *Inventario degli archivi cartacei;*
- *Identificazione delle tipologie documentali gestite;*
- *Identificazione dei fascicoli, dei fascicoli ibridi, dei fascicoli informatici e delle aggregazioni documentali;*
- *Copia di tutti i contratti in essere con i consulenti esterni con i quali intercorre uno scambio di dati personali;*
- *Censimento dei trattamenti dei dati personali;*
- *Individuazione dei "responsabili" del trattamento dei dati e predisposizione dei nuovi documenti di designazione da parte degli organi competenti;*
- *Individuazione dei "responsabili esterni" e predisposizione dei nuovi documenti contrattuali;*
- *Individuazione dei profili di autorizzazione degli incaricati al trattamento dei dati;*
- *Predisposizione di un Regolamento Aziendale in materia di utilizzo dei sistemi informatici e di trattamento dei dati personali;*
- *Redazione delle procedure per l'esercizio dei diritti dell'interessato di cui agli artt. 12 - 22 del Regolamento EU 2016/679;*
- *Implementazione del processo di data breach ai sensi degli artt. 33 e 34 Regolamento EU 2016/679;*
- *Redazione del Registro delle attività di trattamento ex art. 30 Regolamento EU 2016/679;*
- *Redazione delle Informative e gli altri documenti necessari per ottemperare agli obblighi di legge;*
- *Organizzazione degli Audit interni sulla gestione del "**Sistema di Gestione della Protezione dei Dati**" per la fase di adeguamento ed a regime,*

fondamentali per rilevare le situazioni di non Conformità ed attivare le necessarie Azioni Correttive al fine di garantire la piena conformità normativa;
- *Piano delle Azioni Correttive;*
- *Piano di Formazione del personale e relativa documentazione di supporto.*

TEMPISTICHE E PIANIFICAZIONE

È richiesto al concorrente la definizione di un piano operativo in cui cadenzare le attività su indicate e che dovrà aver luogo a partire al più tardi dopo una settimana dall'aggiudicazione del procedimento e al massimo avrà durata di **3 mesi solari**.

Elementi migliorativi saranno valutati, ma senza che questi inficino la qualità dei servizi o richiedano alla Società un gravoso impegno di persone.