LE FASI IN CUI SI ARTICOLA IL PROGETTO ADEGUAMENTO AL GDPR

Area: Sicurezza/Privacy

Ulteriori informazioni sui servizi consulenziali e prodotti specifici, sono disponibili sul nostro sito – o richieste direttamente alla Segreteria COMSEC - segreteria@comsecservizi.com o telefonando direttamente a Tel. 02 57518448 – Mobile 335-6463024.

COS'E' IL GDPR? General Data Protection Regulation

General Data Protection Regulation è il REGOLAMENTO generale del Parlamento Europeo per il TRATTAMENTO DEI DATIPERSONALI.

Richiede l'analisi e l'adeguamento dei PROCESSI AZIENDALI per il trattamento dei dati non solo dal punto di vista ICT, ma anche legale/organizzativo.

Prevede l'eventuale obbligo di nominare un DATA PROTECTION OFFICER (ruolo esternalizzabile) e di denunciare le violazioni di dati entro 72 ore.

LA SCADENZA 25 maggio2018 - termine ultimo per adeguarsi

Solo 1 azienda italiana su 5 conosce nel dettaglio le implicazioni del General Data Protection Regulation. (*Fonte: ricerca del Politecnico di Milano 2017 - Osservatorio Information Security & Privacy*).

Di seguito le fasi in cui si articola il **Progetto di adeguamento al GDPR secondo la Metodologia MAPS (**Metodologia di Analisi e Progettazione di Sistemi Organizzativi Aziendali**) COMSEC:**

1) ASSESSMENT PRE-AUDIT,

2) PIANO DI LAVORO E CREAZIONE PROGETTO,

3) IMPLEMENTAZIONE DEL SISTEMA DI SICUREZZA INFORMATICA E PRIVACY

4) RILASCIO DELLA DICHIARAZIONE DI CONFORMITA'

1) ASSESSMENT ICT PRE-AUDIT LEGAL & TECH Aspetti legali e tecnologici

E' necessario conoscere l'**infrastruttura tecnologica e applicativa del Clienti** (organizzazione, processi e tecnologie aziendali).

Effettuare una **Analisi della Sicurezza** (**Risk Assessment** dettagliato dei processi aziendali e del S.I. e individuazione delle adeguate misure di sicurezza. Più in dettaglio si valuta la situazione di conformità **"as is"** e **"to be"** individuando le eventuali **non conformità presenti** e le **aree critiche** dove occorre definire ed implementare nuove misure di sicurezza o adeguare quelle preesistenti.

L'analisi della sicurezza riguarda prioritariamente i processi aziendali dove sono trattati dati personali e per i quali è necessario progettare e realizzare misure adeguate di sicurezza sulla base dei requisiti del GDPR. Le attività principali di questa fase sono:

a) *RISK ASSESSMENT LEGAL* - l'attività di Risk Assessment Legal considera gli "*aspetti legali*" dove vengono normalmente acquisiti e analizzati i seguenti documenti di base:

- Analisi legale del Documento Programmatico della Sicurezza aziendale
- Organigramma con la descrizione delle funzioni
- Campionamento dei processi aziendali.

b) *RISK ASSESSMENT TECH* - analisi degli "*aspetti tecnici*" dove vengono raccolte informazioni e analizzati gli accessi degli utenti alle procedure software del sistema informativo.

- Rilevazione delle misure tecniche attuate per la sicurezza dei dati

- Analisi dei sistemi per la protezione dei dati
- Controllo delle attività di logging del sistema.

c) REPORTING DIREZIONALE COMPLIANCE GDPR

- Descrizione delle attività compiute
- Esposizione rischi potenziali legali e tecnici
- Presentazione delle nuove misure per aderire ai criteri della normativa GDPR.

2) PIANO DI LAVORO E CREAZIONE PROGETTO

- Mappatura delle transazioni e attività degli utenti sull'intero Sistema Informativo
- Definizione del quadro normativo e redazione di un report con la valutazione del rischio
- Definizione e presentazione del Piano di Lavoro per adeguarsi alla normativa GDPR.

3) IMPLEMENTAZIONE DEL SISTEMA DI SICUREZZA INFORMATICA E PRIVACY

- Pianificazione delle attività di GDPR Compliance
- Rilascio della dichiarazione di conformità a GDPR
- Governance Management della soluzione a regime
- Gestione delle ispezioni da parte dell'Autorità Garante Privacy.

4) RILASCIO DELLA DICHIARAZIONE DI CONFORMITA'

Con la verifica finale delle «*adeguate misure di sicurezza*», sia nei processi di Governance che ICT, al Cliente verrà rilasciata una *DICHIARAZIONE DI CONFORMITA'*.

Una buona stima dei tempi e quindi dei costi per la realizzazione delle attività relative alle fasi 2) 3) 4 si ottiene utilizzando le risultanze della fase di ASSESSMENT PRE-AUDIT.

Riferimenti per consulenze ed approfondimenti: Dott. Vittorio Trinetta – vtrinetta@comsecservizi.com