NUOVO REGOLAMENTO EUROPEO PRIVACY

Come adeguarsi al GDPR in 4 passi

1. MAPPATURA E CENSIMENTO

Identifica i dati

1. Da dove provengono i dati che raccogli
2. Dove sono archiviati: data base, archivi doc

Definisci Scopi e modalità

1. Perchè raccogli dati
2. Fino a quando vengono conservati
3. Vengono trasferiti fuori UE?

Mappa i processi

1. Quali sono le attività di trattamento
2. Quali sono i ruoli e gli attori
3. Quali applicazioni utilizzi

Prepara il registro dei trattamenti: ricorda che ogni registro deve contenere delle informazioni minime

Il DPO: valuta se nominare il Responsabile della Protezione dei Dati. Può essere nominato anche se non obbligatorio e può essere sia interno che esterno.

2. ADEGUARSI E PROTEGGERE

Procedure e Strumenti

1. Informativa e Consenso
2. Accesso, Oblio, Rettifica
3. Opposizione e limitazione
4. Portabilità dei dati

Rischi e Impatti

1. Distruzione, perdita, alterazione, accessi non autorizzati, sottrazione
2. Adotta procedure per valutare gli impatti di tali rischi

Adottare Contromisure

1. Controllo accessi
2. Protezione, cifratura
3. Resilienza, Disaster Recovery

Non esistono più le misure minime di sicurezza, si tratterà di scegliere le misure di sicurezza «ragionevoli» in funzione del contesto aziendale

Per valutare l'impatto si possono usare metodologie standard: es. ISO 31000:2009 e ISO/IEC 29134

3. CONTROLLO E REAZIONE

Monitoraggio

Per essere pronti a gestire situazioni di violazione è necessario tracciare preventivamente le operazioni di trattamento

Strumenti

E' necessario predisporre degli strumenti di monitoraggio della sicurezza e generazione di alert per attuare le contromisure opportune

Procedure

In caso di violazione (DATA BREACH) predisporre procedure per notifiche a Garante e ad interessati

4. VERIFICA ED AGGIORNA

Privacy by Design

Privacy by Default

Il GDPR non è un progetto una-tantum, ma neanche una serie di adempimenti puramente formali: è un processo che continua nel tempo.

Il volume e le tipologie di dati raccolti muteranno e cambieranno i trattamenti necessari; il sistema informativo dell'azienda si evolverà seguendo la innovazione tecnologica e le nuove esigenze di prestazioni e sicurezza; le minacce alla sicurezza informatica e le tecniche di attacco si evolveranno e ne nasceranno di nuove.

E' necessario quindi predisporre delle modalità di revisione ed aggiornamento delle procedure e delle soluzioni tecnologiche per il corretto trattamento dei dati personali e gestione della sicurezza di tali dati.