

# PRIVACY

## Regolamento UE 2016 679



---

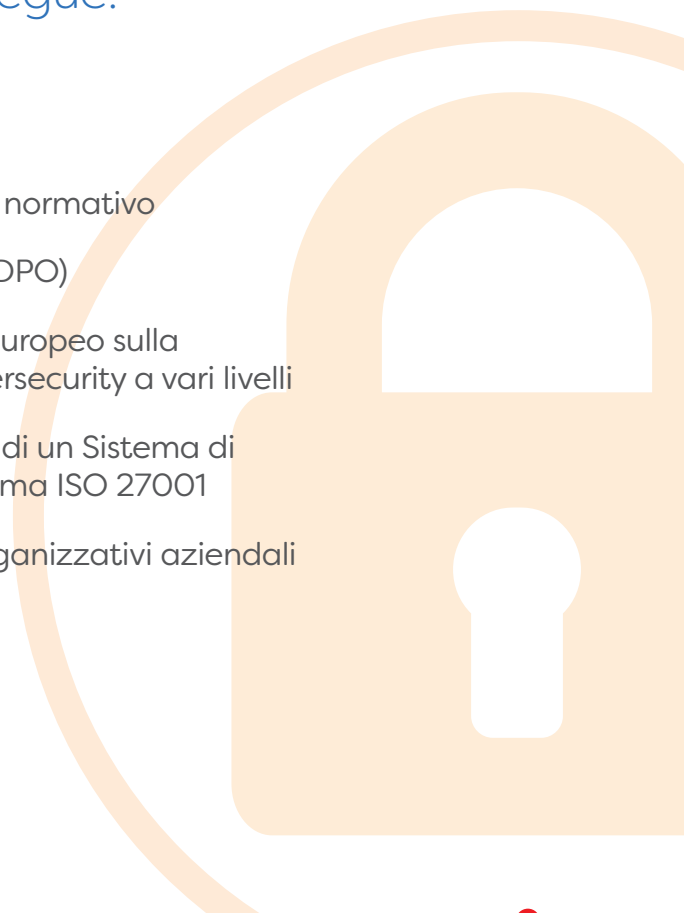
Attraverso questo servizio si persegue l'obiettivo di fornire strumenti, supporto metodologico, consulenza e affiancamento necessari per permettere ai nostri Clienti di essere a norma entro il 25 maggio 2018 (data di piena applicazione del GDPR).

Il servizio consiste in attività di audit e valutazione presso il Cliente finalizzate all'esecuzione dell'assessment, all'attuazione dei piani di attività, di formazione e di produzione della documentazione privacy necessari a conseguire la compliance al GDPR.

Inoltre, saranno approfondite le modalità di attuazione della "Privacy by design e by default", della valutazione dell'impatto sui dati (DPIA - Data Protection Impact Assessment), della notificazione delle violazioni, dell'analisi e valutazione dei rischi, anche in ottica SGSSI ISO 27001.

### I servizi EcoSafe si sviluppano come segue:

- 1 Gap analysis e audit periodici
- 2 Consulenza e sviluppo della compliance al GDPR
- 3 Contratto annuale di assistenza tecnica e supporto normativo
- 4 Assunzione dell'incarico di Data Protection Officer (DPO)
- 5 Sessioni di formazione in materia di Regolamento Europeo sulla Protezione dei Dati Personali - GDPR 679/16 e Cybersecurity a vari livelli
- 6 Supporto nella progettazione ed implementazione di un Sistema di gestione per la sicurezza dei dati conforme alla Norma ISO 27001
- 7 Integrazione della sicurezza dei dati nei Modelli Organizzativi aziendali (Risk management e D. Lgs 231)





A livello operativo la proposta EcoSafe si articola come segue:

**FASE  
1**

Assessment iniziale per verificare lo stato dell'arte, con elaborazione di gap analysis, mappatura dei trattamenti effettuati in qualità di Titolare o di Responsabile del trattamento, dei ruoli e dell'organigramma (titolari, responsabili, addetti al trattamento).

**FASE  
2**

Progettazione e sviluppo del Sistema di Gestione della Data Protection:

- compilazione dei registri dei trattamenti;
- identificazione dei responsabili interni;
- redazione dei documenti di designazione dei responsabili esterni;
- designazione degli Amministratori di Sistema
- predisposizione registro degli incidenti (Data Breach)
- analisi dei rischi;
- regolarizzazione del sistema di videosorveglianza;
- revisione della documentazione privacy: informative, incarichi, policy, designazioni;
- piano di auditing e di mantenimento.

**FASE  
3**

DPIA e Codice di comportamento. Quest'ultima fase comprende:

- elaborazione e stesura della Data Protection Impact Assessment (DPIA);
- analisi e revisione delle applicazioni software e dei processi di trattamento in ottica "Privacy by Design e Privacy by default";
- analisi del fabbisogno formativo e predisposizione del piano formativo;
- erogazione della formazione.