

## PROTEZIONE DATI by Ermes

La tua azienda è già in linea con le  
procedure previste dal nuovo GDPR?

Affidatevi a noi, vi assisteremo con un'attività  
di consulenza a misura per voi

# GDPR



Responsabile della  
Protezione dei dati (DPO)



Conformità



25 Maggio 2018



Violazione  
sicurezza



Dati  
personali

## Come possiamo aiutarvi (attività di consulenza)

L'avvento della GDPR segnerà un "cambio di passo" nella gestione dei dati, si renderà necessario predisporre metodologie specifiche di Data Management atte a monitorare e orchestrare in maniera compliant tutti i dati soggetti a regolamentazione. Prima di affrontare il problema da un punto di vista tecnologico è importante capire a che punto è la vostra azienda, predisporre una roadmap evolutiva e una conseguente crescita sulla cultura del dato che da questa "piccola" rivoluzione è auspicabile attendersi.

Supportiamo le aziende **in tutte le quattro fasi critiche** che coinvolgono la **normativa GDPR**, partendo dalla progettazione e dagli audit di miglioramento fino alla formazione. **L'offerta modulare** permette al cliente di richiedere consulenza per uno o più stadi di un progetto:



### Assessing

Analisi del perimetro, dei processi e profilazione dei trattamenti



### Risk Management & Protection

Risk Analysis, DPIA, Security Assessment



### Modeling

Modello di gestione, profilazione ruoli, creazione registri e informative, requisiti funzionali BD&BD



### Training & Control

Formazione, Awareness, Audit annuali



### Data Protection

Servizi di sicurezza gestita per la protezione dei dati personali

L'attività sarà svolta dal nostro personale altamente qualificato e dotato di certificazione UNI 11697:2017 rilasciata da Accredia.

## Riassumiamo di seguito i passi che vengono solitamente seguiti per l'adeguamento alla GDPR:

Fase 1 - Valutazione della compliance: raccolta di tutte le informazioni sull'organizzazione aziendale, analisi e valutazione della documentazione in uso;

Fase 2 - Creazione del registro dei trattamenti: documento volto a tenere traccia dei trattamenti effettuati da parte del titolare e degli eventuali responsabili, e contenente, tra gli altri, le finalità del trattamento, una descrizione delle categorie di interessati e dei dati personali, i destinatari, gli eventuali trasferimenti verso paesi terzi e una descrizione generale delle misure di sicurezza;

Fase 3 - Stesura/Modifica della documentazione affinché risulti completa ed aggiornata secondo le prescrizioni della nuova normativa;

Fase 4 - Individuazione dei ruoli e delle responsabilità dei soggetti che effettuano il trattamento;

Fase 5 - Definizione delle politiche di sicurezza e valutazione dei rischi: valutazione e attuazione di tutte le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al RGPD. Questa fase è espressione, soprattutto, del principio di responsabilizzazione del titolare (accountability);

Fase 6 - Processo di Data Breach: al fine di assicurarsi di aver adottato tutte le procedure idonee a scoprire eventuali violazioni, generare adeguata reportistica e indagarne le cause nonché gli effetti della violazione subita;

Fase 7 - Valutazione d'impatto sulla protezione dei dati personali: al fine di assicurare trasparenza nelle operazioni di trattamento dei dati personali e adeguata protezione agli stessi, implica che il titolare effettui precise e adeguate valutazioni d'impatto privacy. Attraverso tale istituto è possibile quindi, valutare gli aspetti relativi alla protezione dei dati, prima che questi vengano trattati;

Fase 8 - Implementazione dei processi per l'esercizio dei diritti dell'interessato;

Fase 9 - Individuazione e nomina di un Data Protection Officer (DPO): figura la cui responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento dei dati personali (e dunque la loro protezione) all'interno di un'azienda, affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

## Cos'è il GDPR

Il regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation - Regolamento UE 2016/679) è un Regolamento con il quale la Commissione Europea intende rafforzare e rendere più omogenea la protezione dei dati personali all'interno dei confini dell'Unione Europea (UE). Il regolamento, che riguarderà tutte le aziende che trattano i dati personali dei cittadini dell'UE, richiederà l'implementazione di nuovi processi e di regole più severe per la protezione di tali informazioni. Se si gestiscono, raccolgono o utilizzano dati personali (di dipendenti, client esistenti o potenziali) il GDPR cambierà le pratiche di lavoro usuali.

Il GDPR è entrato ufficialmente in vigore **il 25 Maggio 2018**.

## Cosa cambierà per le aziende

Il GDPR introduce un ampio spettro di novità imponendo di definire un piano di adeguamento alla nuova normativa. Tutte le diverse funzioni aziendali che gestiscono e trattano dati personali sono coinvolte. Alcune di esse impongono un'attenta pianificazione poiché possono comportare modifiche organizzative importanti e investimenti di natura tecnologica, per questo la nuova normativa darà maggior risalto al team IT e ai CIO aziendali, conferendo un ruolo cruciale alle loro mansioni. Il nuovo regolamento sarà causa di severe sanzioni per le aziende che non lo rispettano, con multe fino al 4% del fatturato globale annuo o a 20 milioni di euro, a seconda di quale sia la cifra maggiore tra le due.

Per richiedere maggiori informazioni contattaci alla mail [nicola.madrighali@ordingbo.it](mailto:nicola.madrighali@ordingbo.it)

**ermes** srl

### Ufficio di Roma

Via B. Petrocelli, 228 scala A - 00173 Roma  
Tel. +39 06 87153060

### Ufficio di Milano

Via S. D'Acquisto, 22 - 20037 Paderno Dugnano (MI)  
Tel. +39 02 84963790

### Sede legale ed operativa

Via Grassilli, 11 - 40012 Calderara di Reno (BO)  
Tel. +39 051 757040 - Fax +39 051 6160441