# IMPLEMENTAZIONE GDPR (2016/679)
# ASSOCIATI

Vernasca giugno 2018

**MyWay S.r.l.**
Via Osti, 6 - 29010 Vernasca (PC)
P.Iva-Cod. fiscale 01691990335

## 1 - IL NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY UE 2016/679 E LA CYBER SECURITY

Il nuovo Regolamento Europeo (GDPR, General Data Protection Regulation - Regolamento UE 2016/679) in materia di protezione dei dati personali diventerà applicabile, in tutti gli stati membri, a partire dal 25 maggio di quest'anno.

Questa normativa introduce importanti novità non solo per i privati cittadini ma anche per aziende, enti pubblici, associazioni e liberi professionisti. Lo scopo è fornire una risposta concreta alle nuove sfide che le innovazioni tecnologiche e i nuovi modelli di crescita economica impongono, dando seguito a un'esigenza sempre più marcata di rispetto della privacy da parte dei cittadini.

Il GDPR ha lo scopo di tutelare maggiormente i cittadini: detta norme efficaci in merito a informative e consensi sul trattamento dei dati personali, definisce i limiti entro i quali questi possono essere trattati, stabilisce i criteri per il trasferimento dei dati al di fuori dell'Unione Europea. Vengono riconosciuti il diritto all'accesso, alla cancellazione, alla trasferibilità dei dati, all'opposizione ai trattamenti automatici e ad essere informati in caso di gravi violazioni, le cosiddette "data breach".

Il Regolamento si concentra sui doveri e le responsabilità dei titolari e dei responsabili del trattamento dei dati, definendo meglio processi, misure tecniche e organizzative, obblighi e sanzioni.

Aziende, enti pubblici ed organizzazioni avranno quindi nuove e maggiori responsabilità che, se non soddisfatte, potranno essere sanzionate con ammende fino a 20 milioni di euro o fino al 4% del fatturato annuale globale di gruppo per le multinazionali e con obblighi di comunicazione verso tutti i potenziali interessati.

La protezione dei dati diventa quindi centrale non solo nelle politiche di compliance di qualsiasi azienda o ente pubblico, ma anche per garantire la continuità del business.

A livello organizzativo, il GDPR introduce una nuova figura, il Data Protection Officer (DPO), ovvero il Responsabile della protezione dei dati, che dovrà essere presente in tutte le aziende pubbliche e in quelle private in cui il trattamento dei dati personali presenti rischi particolarmente elevati. Un ruolo di grande responsabilità che dovrà riportare direttamente dal top management aziendale.

In un mondo che è oramai fortemente dipendente dalle tecnologie informatiche, la resilienza dei sistemi informativi aziendali assume sempre più un ruolo essenziale per il successo di qualsiasi impresa. La sicurezza delle informazioni (cyber security) è quindi un elemento critico sia per il successo delle organizzazioni sia per l'adeguamento ai requisiti della nuova legislazione europea.

Le aziende che potranno dimostrare di aver adottato tutte le misure richieste dal nuovo Regolamento potranno ottenere dall'Autorità una riduzione delle eventuali sanzioni. Questa limitazione di responsabilità (Accountability) sarà favorita anche dalla predisposizione di un registro delle attività di trattamento dei dati e dalla necessità di svolgere valutazione dei rischi per i dati personali prima di introdurre in azienda nuove applicazioni, tecnologie o processi (Privacy by Design).

## 2 - LA NOSTRA METODOLOGIA

Questa proposta è strutturata in modo da illustrare brevemente il nostro approccio metodologico generale, per poi descrivere in dettaglio le attività che riteniamo necessarie per rispondere alle vostre esigenze, le attività consigliabili e presentare la nostra offerta economica.

La nostra metodologia operativa prevede una prima fase di **analisi**, mirata a individuare gli interventi necessari o consigliabili, seguita da una fase di **implementazione e adeguamento** vero e proprio e da un'attività di **monitoraggio e mantenimento annuale**.

Tutte le attività sono state progettate per poter essere svolte anche singolarmente in modo da adattarsi alle condizioni ed alle esigenze di ogni organizzazione.

Le fasi previste sono riportate nel seguente schema:


Le attività di implementazione sono relative a:

- Aspetti legali e documentali;
- Interventi organizzativi;
- Adozione di misure tecniche per l'incremento della sicurezza informatica.

### 2.1 ANALISI E PROGETTAZIONE

Si tratta di un intervento rapido ma intenso, condotto dai nostri esperti in organizzazione, information security e problematiche legali.

Parte dall'analisi della documentazione disponibile in azienda, dalla somministrazione di questionari on line alle funzioni aziendali coinvolte nella gestione e nel trattamento dei dati personali (Marketing, HR, Legal/Compliance, IT, Customer Service, Produzione/erogazione servizi, ufficio crediti).

L'analisi si concentra sugli aspetti di Privacy, Cyber Security e resilienza dei sistemi informativi e permette di avere una visione generale della situazione aziendale e della distanza (gap analysis) rispetto ai requisiti previsti dal Regolamento Europeo.

In questa fase saranno progettati gli interventi necessari in base alle aree di miglioramento individuate ed alle specifiche esigenze organizzative dell'azienda e sarà definito il programma di adeguamento al GDPR.

## 2.2 ADEGUAMENTO

La fase di adeguamento ai nuovi requisiti è suddivisa in tre settori distinti, che vengono affrontati in parallelo o disgiuntamente a seconda delle necessità dell'azienda.

Le aziende che presentano una **minore complessità organizzativa e tecnologica** e che non trattano dati personali particolarmente critici (es. dati sanitari) potranno **concentrarsi sugli adempimenti documentali** e formali, prima di approfondire gli aspetti legali alla sicurezza logica.

La prima area d'intervento è quindi relativa all'adeguamento degli aspetti formali, che abbiamo incluso nell'**Area Documentale**:

- Ricostruzione processi e flussi dei dati personali
- Rielaborazione informative Privacy
- Aggiornamento procedure raccolta consensi al trattamento e modulistica
- Aggiornamento deleghe e nomine (responsabili e incaricati)
- Definizione relazioni e/o contratti tra Titolare (eventuali contitolari) e eventuali Responsabili del trattamento
- Predisposizione Cyber Security Policy e Codice Disciplinare aziendale
- Predisposizione registro trattamento dati (se necessario)

Nell'**Area organizzativa** prevediamo le seguenti attività specifiche:

- Predisposizione/aggiornamento dell'organigramma Privacy
- Attività di formazione e informazione
- DPO, Data Protection Officer (se necessario)

Infine, tutti gli aspetti cruciali legati alla sicurezza informatica, sono stati da noi raggruppati nell'**Area IT:**

- Mappatura dei dati personali e dei flussi operativi
- Vulnerability Assessment – Penetration Test (se necessari)
- Data Protection Impact Assessment – DPIA (se necessaria)
- Supporto per l'applicazione delle misure tecniche minime di protezione dei dati personali (criptazione, anonimizzazione, pseudonimizzazione)
- Assessment procedure di Backup e Disaster Recovery IT

**MyWay** è a disposizione dell'azienda per eseguire anche **approfondimenti** per valutare la robustezza e la maturità dei sistemi informativi ed **interventi diretti** per implementare, insieme al personale IT aziendale, le misure di protezione dei dati (criptazione, anonimizzazione, pseudonimizzazione), procedure di backup o piani di disaster recovery. Tutte queste attività sono però **escluse dal presente incarico** e saranno effettuate **solo ed esclusivamente su specifica richiesta.**

## 2.3 MONITORAGGIO

Al fine di mantenere un livello adeguato di sicurezza nel trattamento dei personali è necessario, come d'altronde previsto dal GDPR stesso, che le aziende svolgano opportune attività di monitoraggio e di manutenzione del "sistema" di protezione dei dati, anche dopo la data del 25 Maggio 2018.

In questo senso, riteniamo che sia necessario prevedere attività di manutenzione per un periodo minimo di almeno tre anni nelle diverse aree precedentemente descritte:

- Area Documentale, per identificare le evoluzioni legate alla interpretazioni e alle comunicazioni prodotte dall'Authority per la Privacy;
- Area Organizzativa, con la formazione regolare degli utenti;

- Area IT, con l'esecuzione di test periodici (vulnerability assessment e penetration test) sull'infrastruttura tecnologica e tramite la formazione specifica verso il personale specialistico.

## 3 - SVOGLIMENTO DELL'INCARICO

Come anticipato nelle sezioni precedenti, le attività da noi proposte sono state strutturate in modo da permettere alla Società di implementare rapidamente i requisiti necessari a **ridurre significativamente il rischio di inadempimenti e sanzioni entro la data di applicabilità** del Regolamento Europeo (25 maggio 2018).

L'incarico iniziale si concentrerà sulle vostre esigenze e sarà svolto secondo quanto specificato nei paragrafi successivi.

## ATTIVITA' PROPOSTE PER IL 2018

**3.1 – Inserimento dati azienda e audit (procedura di assessment).**

a) Raccolta delle informazioni
- L'azienda compilerà un questionario elaborato da parte dei nostri esperti.

b) Gap analysis
- Grazie alle informazioni fornite, sarà predisposto un Report sul livello di conformità della situazione attuale valutando l'eventuale Gap (carenze) rispetto alle prescrizioni della nuova normativa.

c) Approfondimenti
- Saranno identificate eventuali aree di criticità per le quali sia necessario un approfondimento specifico e, se opportuno, saranno proposte azioni specifiche.

**3.2 – Programmazione attività**

**MyWay** fornirà il piano di azione da seguire e guiderà l'azienda nell'approfondimento e/o adeguamento dei processi di trattamento dei dati, degli aspetti legali e di quelli tecnologici con indicazione di tempi e budget.

**3.3 – Adeguamento documentale.**

**MyWay** preparerà la documentazione finale per la Conformità standard al GDPR comprendente:
- Informativa trattamento dati;
- Consenso al trattamento dei dati personali;
- Nomina amministratore di sistema;
- Nomina responsabile del trattamento dei dati personali;
- Comunicazione Garante della Privacy in caso di violazione dei dati personali.
- Cyber Security Policy e Codice Disciplinare aziendale.

**3.4 – Formazione.**

**MyWay** somministrerà corsi di formazione on line, per tutti gli utenti della società italiana, per fornire ai dipendenti gli elementi che consentano di perfezionare la propria conoscenza e sensibilità sul GDPR.

I corsi sono modulati in relazione ai ruoli e alle competenze dei partecipanti, e prevedono una verifica di apprendimento. Permetteranno di approfondire gli aspetti legali, tecnici e gestionali della sicurezza informatica e della data protection:

- Corso introduttivo al GDPR
- Corso per i responsabili
- Corso per gli incaricati

**3.5 – Consulenza.**

**MyWay** metterà a disposizione dell'azienda un Help Desk, formato da esperti legali, informatici e Data Protection Officer per fornire assistenza nell'applicazione dei nuovi principi di Privacy by Design e Privacy by Default.

## ATTIVITA' DI MANUTENZIONE E ASSISTENZA PER 2019 E 2020

Al fine di mantenere un livello adeguato di sicurezza nel trattamento dei personali è necessario, come d'altronde previsto dal GDPR stesso, che le aziende svolgano opportune attività di monitoraggio e di manutenzione del "sistema" di protezione dei dati, anche dopo la data del 25 Maggio 2018.

In questo senso, riteniamo che sia necessario prevedere le seguenti attività di manutenzione per i 2019 e i 2020:

- Area Documentale:
  - La documentazione aziendale sarà aggiornata in funzione delle eventuali evoluzioni legate all'interpretazione e armonizzazione della normativa ed alle comunicazioni prodotte dall'Autorità Garante;
- Area Organizzativa
  - La formazione regolare degli utenti sarà aggiornata annualmente (e-learnig);
- Area IT
  - Anche la formazione del personale IT sarà aggiornata annualmente.
  - Su richiesta dell'azienda, **MyWay** sarà lieta di eseguire anche test periodici (vulnerability assessment e penetration test) sull'infrastruttura tecnologica.

**MyWay**, inoltre, manterrà a disposizione dell'azienda un Help Desk, formato da esperti legali, informatici e Data Protection Officer per fornire assistenza nell'applicazione dei nuovi principi di Privacy by Design e Privacy by Default.

## 4 - OBBLIGHI DELL'AZIENDA, ESCLUSIONI E MANLEVA

L'azienda si impegna a collaborare con **MyWay**, fornendo ogni dato e informazione che si renda necessario od opportuno per la corretta e puntuale prestazione dei servizi in conformità ed assumendosi piena responsabilità per la veridicità e correttezza di informazioni, dati, documenti o notizie forniti sui quali **MyWay** non effettuerà nessuna attività di verifica.

Al fine di migliorare l'efficienza lavorativa si richiede che le informazioni di cui sopra siano fornite ad **MyWay**, quando possibile, in formato editabile (.doc, .xls, .pdf.).

L'Azienda esonera espressamente **MyWay** da ogni responsabilità per eventuali errori, omissioni ed inesattezze dei servizi prestati, così come per eventuali sospensioni e/o ritardi nei termini di consegna dei servizi, indipendenti dalla volontà di **MyWay** o comunque determinati da cause ad essa non imputabili.
L'Azienda, inoltre, esonera espressamente **MyWay**, i suoi amministratori, soci, collaboratori, consulenti e dipendenti da ogni responsabilità per qualsivoglia tipo di danno, diretto o indiretto (quale, a titolo esemplificativo ma non esaustivo, l'eventuale mancata conclusione di contratti o eventuali mancati guadagni) che dovesse verificarsi in forza dell'illecito utilizzo dei servizi resi, da parte dell'Azienda o di terzi.
**MyWay** non sarà ritenuta responsabile per i dati, le notizie e le informazioni forniti dall'Azienda, che nel tempo dovessero risultare inesatti o errati, né per le conseguenze che dovessero derivare dall'utilizzo da parte di **MyWay** di tali dati nella prestazione dei servizi.

## 5 - LA NOSTRA OFFERTA ECONOMICA

La seguente tabella sintetizza gli onorari fissati, per le attività concordate come perimetro dell'incarico ed indicate in precedenza.

| Attività | Totale onorari |
|---|---|
| Anno 2018<br>**Analisi, Progettazione, Adeguamento Documentale e formazione in e-learning del Vostro personale** | € 800 |
| Anno 2019<br>**Manutenzione e assistenza** | € 400 |
| Anno 2020<br>**Manutenzione e assistenza** | € 400 |

A completamento della gamma di servizi che MyWay è in grado di offrire, elenchiamo alcune **attività integrative** che sono **espressamente escluse** dalla presente offerta ma che potranno essere quotate ed eseguite, su richiesta del cliente, in un successivo momento.

- Predisposizione registro trattamenti
- DPIA – Data Protection Impact Analysis
- Servizio DPO esterno
- Vulnerability Assessment e penetration test
- Applicazione delle misure tecniche minime di protezione
- Predisposizione di procedure di backup e piani di disaster recovery.

**Note:**

- Gli onorari sono da considerarsi al netto dell'IVA;
- La fatturazione sarà effettuata alla consegna della documentazione;
- Eventuali spese vive di trasferta saranno addebitate separatamente sulla base di quanto effettivamente sostenuto dai nostri consulenti.

Si evidenzia che gli importi descritti in questo paragrafo sono indicati e si fondano su stime effettuate sulla base della documentazione in nostro possesso e utilizzando la nostra esperienza maturata in contesti simili. **MyWay** è disponibile a rettificare tali importo di una revisione congiunta delle effettive attività richieste che potrà essere concordata con il Management d'azienda.

VALIDITA' DELL'OFFERTA

La presente offerta ha validità di 30 gg dalla data di presentazione.

**MYWAY SRL**

Guido Mondelli

Amministratore Delegato

Per Accettazione

_____

Data

In caso di gradimento della presente Proposta di Consulenza e Servizi, Vi preghiamo di volercene restituire copia firmata per accettazione a cui seguirà il contratto di consulenza sulla base dei livelli dei servizi scelti.