



Il Regolamento UE Generale sulla protezione dei dati personali n. 679/2016

Il Data Protection Officer DPO

Descrizione

Il 4 Maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il “Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)”.

Il Regolamento entrerà in vigore il 25 Maggio 2016 e sarà concretamente operativo nei Paesi UE a decorrere dal 25 maggio 2018, lasciando a tutti i soggetti interessati un biennio di tempo per gli adeguamenti necessari alle proprie politiche del trattamento dei dati.

Per quanto riguarda l'Italia, il Regolamento sostituirà il “Codice Privacy” in vigore dal 1° Gennaio 2004.

Il D.P.O. deve essere designato sulla base dell'approfondita conoscenza della normativa sulla protezione dei dati e sulla capacità di svolgere i compiti previsti all'Articolo 39 del nuovo Regolamento UE con, inoltre, un background tecnico ed organizzativo in merito al trattamento dei dati personali; può essere un soggetto interno all'azienda oppure un soggetto esterno che assolve i propri compiti sulla base di un contratto di servizi.

Durata: 3 giorni

A chi si rivolge

- funzionari e dirigenti che svolgano il ruolo di Responsabile Privacy, Data Protection Officer, Responsabile IT, Security Manager, Compliance Officer;
- liberi professionisti che svolgano attività di consulenza

Contenuti

Modulo 1: Principi e nozioni per il “DPO”

- La normativa italiana cogente: il D.Lgs. 196/03, ambito di applicazione, definizioni, principi generali
- Il nuovo Regolamento Europeo della Privacy (UE) 2016/679
- Il Data Protection Officer o Responsabile della Protezione dei dati personali art. 37 GDPR, cenni
- Trattamento e tipologia di dati
- I diritti dell’interessato, informativa e consenso
- Come redigere un’informativa
- Come redigere un’informativa per un sito web
- Organigramma Privacy nelle aziende, Ruoli e Responsabilità
- Come nominare un responsabile ed individuare un incaricato del trattamento
- Analisi dei rischi
- Sistema di Gestione della Sicurezza delle Informazioni (ISMS)
- Misure di Sicurezza, minime e idonee
- L’Amministratore di Sistema
- Notificazione del trattamento al Garante
- Il Garante della Privacy: compiti e funzioni
- Sanzioni, violazioni amministrative e penali, risarcimento del danno
- La Videosorveglianza
- Come predisporre una Notifica all’Autorità Garante ai sensi dell’art. 37 TU Privacy

Modulo 2: Provvedimenti, Linee Guida e Trattamenti Particolari

- Amministratori di Sistema e Log
- Marketing e Telemarketing: il Registro delle Opposizioni
- Cookie e Privacy: istruzioni per l’uso
- WP 29 e linee guida sulle app
- Policy e Privacy sul lavoro (uso della posta elettronica aziendale ed internet)
- Privacy e Statuto dei Lavoratori
- La videosorveglianza in Azienda

- Data Breach (Violazioni della sicurezza), provvedimenti del Garante e artt. 33 e 34 del GDPR

Modulo 3: La nuova figura del “DPO”

- La figura del Data Protection Officer
- Professionalità ed esperienza per un ruolo da leader
- Casi complessi e regole vigenti
- Conservazione dei dati di traffico per fatturazione o repressione dei reati
- Regole per la sicurezza dei dati in rete e nelle telecomunicazioni

Modulo 4: Regole vigenti e pianificazione delle attività del “DPO”

- Il Sistema di Gestione della Privacy
- Il Cloud Computing: profili privacy
- Dati e Dossier Sanitari
- Data Breach
- Il trasferimento di dati all’estero: BCR e autorizzazioni del Garante
- Safe Harbor, Sentenza della Corte di Giustizia dell’Unione Europea e Privacy Shield
- Conservazione sostitutiva
- Regolamento Europeo sulla protezione dei dati personali (GDPR)
- Il lavoro del Data Protection Officer o Responsabile della Protezione dei dati personali
- Individuare un organigramma Privacy
- Attività di reporting; PIA, Privacy Impact Assessment;
- Predisporre una policy sul trattamento dati
- Nominare e verificare i responsabili privacy esterni (art. 28 GDPR)
- Gestione informative, consensi e richieste agli interessati (artt. 13 e 14 GDPR)
- Registro dei trattamenti (art.30 GDPR)

Modulo 5: Sistemi di Gestione Integrati

- L’integrazione del Sistema di Gestione della Privacy con il Sistema di Gestione Qualità (ISO 9001) ed il Sistema di Gestione della Sicurezza informatica (ISO 27001)
- Il D.Lgs. 231/01 ed i reati informatici
- Integrazione del modello organizzativo 231 (ex D.Lgs.231/01) e modello Privacy
- La norma ISO 19011 applicata all’attività di audit sui processi di trattamento dei dati personali