Corso

Privacy Specialist DPO

IN-FORMAZIONE SRL - Via Riccardo Grazioli Lante, 9 - 00195 Roma
P.IVA 07252070722 - Tel. : 0687153208 - info@musaformazione.it

I° MODULO

- La normativa italiana/europea (Reg. EU. 679/2016) sulla protezione dei dati: excursus normativo e principali definizioni
- Cenni al concetto di privacy ed alla sua evoluzione
- La direttiva UE 95/46/CE
- La normativa previgente: L. 675/1996 e D.lgs. 196/2003
- Il Regolamento UE 679/2016: il percorso di approvazione
- Il Decreto legislativo di attuazione n. 101/2018
- Le finalità del Regolamento
- Ambito di applicazione materiale e territoriale del Regolamento
- Le principali definizioni: analisi dell'art. 4 GDPR
- Dato personale
- Categorie particolari di dati personali
- Dati relativi alla salute, dato biometrico e dato genetico
- Dato giudiziario
- La nozione di trattamento
- La profilazione

II° MODULO

- La normativa italiana/europea (Reg. EU. 679/2016) sulla protezione dei dati: le condizioni di liceità del trattamento
- Le basi giuridiche del trattamento
- Analisi dell'art. 6 GDPR
- Il consenso
- Forma del consenso
- Requisiti del consenso
- Consenso dei minori
- La differenza con il consenso informato
- Il ruolo del consenso nel GDPR
- Divieto di trattamento delle categorie particolari di dati personali
- Analisi dell'art. 9 GDPR

III° MODULO

- La normativa italiana/europea (Reg. EU. 679/2016) sulla protezione dei dati: i principi generali sul trattamento dei dati personali ed il principio di accountability
- I principi generali sul trattamento (art. 5 GDPR)
- Il principio di liceità, correttezza e trasparenza

- Il principio di limitazione delle finalità
- Il principio di minimizzazione dei dati
- Il principio di esattezza
- Il principio di limitazione della conservazione
- Integrità e riservatezza
- Il principio di accountability
- Analisi dell'art. 24 GDPR
- Privacy by design e by default (art. 25 GDPR)
- Dimostrazione dell'accountability
- Le misure tecniche ed organizzative adeguate (art. 32)

IV° MODULO

- I primi adempimenti indispensabili: l'informativa sul trattamento dei dati personali
- Il principio di trasparenza
- L'informativa sul trattamento dei dati personali
- Analisi dell'art. 13
- Modalità di redazione dell'informativa
- L'informativa ai minori
- Casi di esclusione dall'obbligo di rendere l'informativa
- Analisi dell'art. 14
- Esempi di informativa
- Esercitazione: la redazione dell'informativa sul trattamento dati dei clienti e prospect

V° MODULO

- I primi adempimenti indispensabili: il registro delle attività di trattamento
- La mappatura delle attività di trattamento
- Il risk assessment ed il concetto di rischio
- Il registro delle attività di trattamento: analisi dell'art. 30 GDPR
- Gli elementi aggiuntivi rispetto al nucleo minito definito dall'art. 30 GDPR
- Esclusione dall'obbligo di tenuta del registro
- Modalità di compilazione e di tenuta del registro
- L'aggiornamento del registro
- DPS e registro: similitudini e differenze
- Istruzioni sul registro dei trattamenti (FAQ Garante 8 ottobre 2018)
- Esercitazione pratica

VI° MODULO

- I soggetti del trattamento: titolare, contitolari, responsabile del trattamento e rappresentante del titolare del trattamento (parte I)

- Gli interessati
- Il Titolare del trattamento
- I Contitolari del trattamento (art. 26 GDPR)
- Un esempio di accordo di contitolarità
- Casi pratici
- Il responsabile del trattamento (art. 28 GDPR)
- Differenze tra il titolare del trattamento ed il responsabile (EDPB, Guidelines 7/2020 on the concept of data controller and data processor)
- I sub-responsabili del trattamento
- Un esempio di accordo ex art. 28 GDPR
- Gli amministratori di sistema (Ads)
- Casi pratici

VII° MODULO

- I soggetti del trattamento: gli autorizzati al trattamento e i soggetti designati. Introduzione alla figura del Data Protection Officer (DPO) o Responsabile della protezione dei dati (RPD) (parte II)
- L'autorizzato al trattamento dei dati personali (art. 29)
- Esempio di atto di nomina
- L'istruzione e la formazione dell'autorizzato
- Un esempio di istruzioni agli autorizzati
- I soggetti designati ex art. 2quaterdecies D.lgs 101/2018
- Il rappresentante del Titolare
- Il Data Protection Officer: ruolo e funzioni
- Autonomia e indipendenza del DPO
- Le risorse necessarie da attribuire al DPO
- La professionalità del DPO e l'obbligo di formazione continua
- DPO interno e DPO esterno
- La pubblicazione dei dati del DPO e la comunicazione all'Autorità di controllo
- Il DPO persona giuridica
- La possibilità di designare un unico DPO

VIII° MODULO

- I soggetti del trattamento: il Data Protection Officer (DPO) o Responsabile della protezione dei dati (RPD) (parte III)
- Il processo di designazione del DPO
- Le linee guida WP29 sul Responsabile della protezione dei dati
- I compiti del DPO (ART. 39)
- I compiti "aggiuntivi" del DPO
- Il rapporto con gli interessati, il vertice aziendale e l'Autorità di controllo
- La relazione annuale

- La stesura del piano di lavoro del DPO
- Le questioni “aperte” sulla figura del DPO
- Il conflitto di interesse
- Le situazioni di conflitto di interesse in ambito pubblico e privato
- DPO e Odv (Organismo di vigilanza): similitudini e differenze
- La possibile assunzione del duplice ruolo di DPO e Odv?
- La qualifica soggettiva dell’Odv
- La diligenza del DPO
- Il Documento di indirizzo sulla designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico (GPDP)

MODULO IX

- Le sanzioni e le ispezioni dell’Autorità di controllo
- Il mancato rispetto del principio di accountability
- Le sanzioni amministrative pecuniarie
- I criteri per la determinazione dell’ammontare delle sanzioni
- Il ruolo dell’Autorità di controllo
- I poteri dell’Autorità di controllo
- Come gestire un’ispezione?
- La documentazione rilevante
- Simulazione di una ispezione

MODULO X

- I diritti degli interessati
- I diritti esercitabili dagli interessati
- La trasparenza nell’esercizio dei diritti degli interessati
- L’obbligo di riscontro del titolare del trattamento
- I tempi di riscontro
- I casi di inottemperanza
- Il diritto ad essere informato
- Il diritto di accesso
- Il diritto di limitazione del trattamento
- Il diritto di rettifica
- Il diritto alla cancellazione
- Il diritto alla portabilità
- Il diritto di opposizione
- Eccezioni ai diritti
- Un esempio di procedura per la gestione dei diritti degli interessati
- I diritti delle persone decedute

MODULO XI

- La gestione di un data breach
- La nozione di data breach
- La violazione della riservatezza, della disponibilità e dell'integrità del dato
- La temporanea non disponibilità del dato
- La notifica all'Autorità di controllo
- Il contenuto della notifica
- La comunicazione agli interessati
- Casi di esclusione dall'obbligo di notifica e di comunicazione agli interessati
- Il provvedimento n. 157/2019
- Casistica rilevante
- Il processo di gestione di un data breach
- La rilevazione della violazione
- La presa in carico dell'evento
- La valutazione del rischio
- La gestione della fase post-evento
- La registrazione delle violazioni
- Il ruolo del DPO nella gestione di un data breach
- La metodologia ENISA per la valutazione del livello di gravità della violazione
- La redazione di una procedura per la gestione di un data breach

MODULO XII

- La valutazione di impatto sulla protezione dei dati (DPIA)
- I considerandi 84 e 89- 95 GDPR
- Analisi dell'art. 35 GDPR
- Lo scopo di una valutazione di impatto ed i soggetti coinvolti
- Il concetto di rischio elevato
- Le Linee guida WP29 sulla valutazione di impatto: 9 criteri di analisi
- Il provvedimento dell'Autorità Garante dell '11 ottobre 2018, n. 467
- Casi di esclusione dall'obbligo di condurre una DPIA
- La consultazione preventiva
- Gli strumenti per lo svolgimento di una DPIA
- Come condurre una valutazione di impatto

MODULO XIII

- Trasferimenti internazionali di dati
- I trasferimenti di dati verso paesi terzi ed infragruppo
- Il sistema decisionale di adeguatezza.
- Trasferimenti tramite garanzie appropriate.
- Clausole contrattuali

- Norme d'impresa
- Il regime di trasferimento dei dati negli USA dopo la sentenza Shrems II
- Il regime di trasferimento dei dati nel Regno Unito dopo la Brexit
- Le eccezioni secondo l'European Data Protection Board

MODULO XIV

- I reati in materia di protezione dei dati
- Trattamento illecito dei dati
- Comunicazione e diffusione illecita di dati personali
- Acquisizione fraudolenta di dati personali
- Interruzione dell'esecuzione dei compiti o dell'esercizio dei compiti del Garante
- Inosservanza dei provvedimenti del Garante
- Violazioni in materia di controlli a distanza dei lavoratori
- D.lgs. 231/01 e GDPR: la gestione integrata della compliance
- Modello organizzativo di gestione (MOG231) e Modello di data protection (MOP)
- I reati informatici di cui al catalogo dei reati-presupposto
- Protocolli di prevenzione e procedure

MODULO XV

- L'autorità di controllo e i profili di responsabilità
- L' Autorità di Controllo
- Compiti, competenza e poteri
- Procedure di competenza del garante
- Il Comitato europeo per la protezione di Dati
- I compiti del Comitato
- La tutela dell'interessato
- I profili di responsabilità
- Il reclamo
- Il ricorso giurisdizionale
- Il danno risarcibile

MODULO XVI

- Il trattamento dei dati nell'ambito del rapporto di lavoro
- Il trattamento dei dati nella fase precedente l'assunzione del dipendente
- La gestione del personale dipendente
- Lo statuto dei lavoratori dopo la riforma del Job Act
- Gli strumenti di controllo del datore di lavoro
- La videosorveglianza
- Il ruolo delle procedure sul trattamento dei dati personali

- La policy per l'utilizzo della casella di posta elettronica
- La gestione della casella di posta elettronica
- La policy per l'utilizzo degli strumenti informatici
- I dipendenti e lo smart working

MODULO XVII

- Il processo di audit
- Come condurre l'audit ai fini della compliance normativa
- Le fasi dell'audit
- I soggetti coinvolti nell'audit
- Domande generali e approccio alla verifica.
- Caratteristiche di base dell'Audit.
- L' audit dei sistemi Informativi.
- Preparazione del rapporto di audit.
- Follow-up
- Le azioni correttive
- Standard internazionali di sicurezza applicabili ai processi di gestione
- La gestione della sicurezza dei trattamenti: le norme ISO/IEC
- Codici di condotta e meccanismi di certificazione

MODULO XVIII

- Il trattamento dei dati nell'e-commerce, marketing e profilazione
- Il trattamento dei dati nell' E-commerce
- Privacy policy e cookie policy: elementi strutturali
- La nuova disciplina dei cookie alla luce del provvedimento dell'Autorità garante del 10 giugno 2021
- Marketing
- Processi decisionali automatizzati
- Profilazione on line

MODULO XIX

- Il trattamento dei dati personali in settori specifici: il settore sanitario
- Gli adempimenti indispensabili in materia di trattamento
- La redazione dell'informativa sul trattamento dei dati in ambito sanitario
- La perdita di centralità del consenso
- Il provvedimento del Garante del 7 marzo 2019
- La sanità digitale
- Il Fascicolo sanitario elettronico (FSE)
- Il Dossier sanitario elettronico (DSE)
- La refertazione on line
- E-prescription

- La telemedicina
- Le app mediche

MODULO XX

- Il trattamento dei dati nella pubblica amministrazione
- Le basi giuridiche del trattamento a seguito della modifica dell'art. 2ter Codice privacy
- Comunicazione e diffusione dei dati personali
- Il trattamento delle categorie particolari di dati personali da parte della P.A.
- Analisi dell'art. 2sexies e art. 2octies Codice privacy
- L'accesso ai documenti amministrativi e l'accesso generalizzato
- Il DPO nel settore pubblico