PROGRAMMA

Data Protection Officer

Percorso completo per DPO

Obiettivo

L'obiettivo primario del corso, strutturato in tre moduli, è quello di fornire ai partecipanti le conoscenze per poter svolgere i ruoli di: Titolare del trattamento dei dati, Responsabile della protezione dei dati (DPO), consulente sulle tematiche della protezione dei dati in relazione al Regolamento Europeo sulla protezione dei dati (REG. EU 2016/679).
Inoltre il corso risponde al requisito formativo per accedere all'esame di certificazione così come previsto dalla UNI 11697:2018 "*Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali- requisiti di conoscenza, abilità ed esperienza*".

Programma

Modulo A: ***Area Giuridica Il nuovo Regolamento Europeo e aspetti giuridici del Ruolo del DPO (32 ore)***

Il modulo consente l'acquisizione delle necessarie conoscenze di carattere giuridico con riferimento alla normativa nazionale ed europea in materia di protezione dei dati personali ed il ruolo del DPO.

- Principi e regole per il trattamento dei dati personali nel nuovo quadro normativo europeo Regolamento Europeo REG EU 2016/679
  - Disposizioni generali e principi
  - Diritti degli interessati, diritto all'oblio e minori
- Approfondimento di tematiche specifiche
  - Titolare, responsabile, contitolare ed incaricato/autorizzato del trattamento: designazioni e nomina
  - Registro dei trattamenti ed analisi dei rischi
  - Privacy by design e privacy by default
  - La gestione del rischio
  - La PIA privacy impact assessment
  - Profilazione
  - Trasferimento di dati verso paesi terzi
  - Procedure di data breach
  - Trattamenti di dati specifici
- L'armonizzazione tra il Codice della Privacy ed il Regolamento
- Autorità di controllo e one stop shop
- Il sistema sanzionatorio, i ricorsi, le responsabilità ed i risarcimenti
- Il ruolo del DPO nel contesto del GDPR e secondo la UNI 11697:2018
  - Il ruolo del DPO nel contesto del GDPR:
    - Nomina, incarico e comunicazione della funzione
    - Posizione organizzativa, rapporti con le altre funzioni aziendali e conflitti di interesse, il ruolo con gli interessati e con il Garante
    - Attività in carico
  - Strumenti operativi al ruolo del DPO
- Case study
- Test di fine modulo

Modulo B: **Area Data Security (24 ore)**

Il modulo consente l'acquisizione delle necessarie conoscenze di carattere tecnico-informatico con particolare riferimento alla sicurezza informatica:

- I principi della sicurezza informatica: Riservatezza; Integrità; Disponibilità; Resilienza; Non ripudio; Tecniche di anonimizzazione; Tecniche crittografiche; Tecniche di pseudonimizzazione; Sistemi e tecniche di monitoraggio (KPI)
- Accountability e Governance IT: Policy; Regolamenti; Gestione del log, Gestione delle infrastrutture hardware; software e di telecomunicazione e rete; Gestione degli applicativi; Best practices.
- Cloud e privacy: Tipologie di Cloud e servizi; Problematiche Cloud; Cloud e privacy; Cloud e sicurezza; Contratti Cloud
- BYOD: Bring your own device: Vantaggi e svantaggi; Rischi; ; Misure di sicurezza; Policy interne.
- Data breach: strumenti per l'identificazione della violazione: IDS; Firewall; Threat Intelligence; Threat Analysis
- Incident Response e Digital Forensics: cosa fare in caso di incidente:
  - Introduzione alla Forensics: cosa è, Strumenti e Norme
- Incident response: Preservare; Acquisire; Analizzare
- Case study: Ramsonware in banca; Insider e furto dati; Sito PA bucato
- La valutazione di impatto in materia di protezione dei dati (aspetti tecnici)
- Valutazione preliminare
- Esecuzione DPIA
- Metodologia di valutazione di impatti e rischi
- Finalizzazione e decisione finale
- Consultazione preventiva
- Case study
- Test di fine modulo

Modulo C: **Il sistema privacy in azienda: le attività di audit (24 ore)**

- Il sistema di gestione della privacy:
  - Il sistema dinamico per la gestione della privacy: finalità, obiettivi e benefici
  - Presidio dei principali processi aziendali che impattano sulla protezione dei dati (personale, approvvigionamenti, infrastrutture, sviluppo, ecc.)
  - Le procedure a supporto della attività di gestione della privacy
- Gli audit:
  - Vantaggi e finalità dell'attività di audit nel contesto del GDPR
  - Pianificazione, programmazione, esecuzione e valutazione di audit di conformità legislativa e sul sistema di gestione della privacy
  - La gestione delle azioni correttive e di mitigazione dei rischi
- Case study
- Test di fine modulo

Al termine di ogni singolo modulo è previsto un test di apprendimento finale e la somministrazione di case study utili a mettere in pratica gli insegnamenti teorici.

Destinatari

Liberi professionisti e funzioni aziendali che rivestono, devono rivestire o valutano di rivestire il ruolo del DPO nell'ambito di aziende private e pubbliche.

Prerequisiti

E' preferibile possedere una delle seguenti opzioni:

- conoscenza generale del GDPR (es. corso cod. GEUP)
- basi per i sistemi di sicurezza informatica (es. corso cod. IBS27)
- la norma UNI 11697:2017 nei punti: D1 Sviluppo della Strategia per la Sicurezza Informatica, E8 Gestione della sicurezza dell'informazione e E9 Governance dei sistemi informativi

Materiale didattico

- Dispensa, contenente le slides e i materiali utilizzati durante il corso
- Norme ad uso didattico (da riconsegnare al termine del corso): Norma UNI 11697:2018

Durata del corso

80 ore + verifica dell'apprendimento

Docente

Il corso viene svolto da docenti qualificati TÜV Italia.

Attestati

Al termine verrà rilasciato:

- Attestato di Competenza (a fronte del superamento del test finale)
- Attestato di Frequenza (in caso di non superamento del test finale)