



Oggetto: MASTER DI ALTA FORMAZIONE IN – DATA PROTECTION OFFICER (DPO) - RESPONSABILE AZIENDALE PER LA PROTEZIONE DEI DATI PERSONALI

PROGRAMMA DI STUDIO:

MODULO 1 – IL DPO: DESIGNAZIONE, POSIZIONE E COMPITI

- Introduzione
- La riservatezza e la protezione dei dati personali
- Il Regolamento (UE) 2016/679 Il Data Protection Officer
- La nascita del Data Protection Officer
- Il Data Protection Officer in Italia
- Il Data Protection Officer nel Regolamento europeo sulla privacy Nomina obbligatoria del RPD
- Definizione di «autorità pubblica o di organismo pubblico»
- Definizione di «monitoraggio regolare e sistematico»
- Definizione di «larga scala»
- Definizione di «attività principali»
- Soggetti a cui spetta nominare il RPD
- Nomina di un unico RPD
- Requisiti particolari del RPD
- L'atto di designazione del RPD Posizione del RPD
- Coinvolgimento del RPD
- Sostegno del RPD
- L'autonomia del RPD
- Il conflitto di interessi Compiti del RPD
- Gli ulteriori compiti e funzioni del RPD
- Conoscenze e caratteristiche personali del RPD La privacy by design e la privacy by default
- La privacy «by design»
- La pseudonimizzazione
- La privacy «by default»
- Fonti giuridiche

MODULO 2 – NUOVE TECNOLOGIE: DIRITTI E DANNI

- Le nuove tecnologie e i nuovi danni
- Il danno patrimoniale: danno emergente e lucro cessante
- La risarcibilità del danno non patrimoniale
- Danno alla persona e danno alla lesione dei diritti della personalità
- Il risarcimento del danno non patrimoniale
- Le categorie di danno non patrimoniale: biologico, morale, esistenziale
- I danni bagatellari
- Il danno non patrimoniale delle persone giuridiche
- Gli interessi tutelati



- La lesione all'integrità psico-fisica
- La violazione dell'identità personale
- Il diritto all'immagine
- La libertà di espressione in internet
- La tutela dell'onore e della reputazione
- Il diritto d'autore in internet
- Il diritto all'oblio Il diritto alla riservatezza: evoluzione e tutela giuridica
- Le origini del diritto alla riservatezza
- La legislazione europea in materia di tutela della riservatezza
- Il ruolo delle informazioni e il nuovo concetto di privacy
- Le fonti normative di rango internazionale e comunitario in materia di privacy
- Il Codice della privacy
- Le misure di sicurezza informatica
- Le misure di sicurezza informatica: profili generali
- Le misure minime di sicurezza
- Il trattamento dei dati mediante l'ausilio di sistemi elettronici
- Misure di sicurezza in materia di trattamento dei dati sensibili e giudiziari
- Le violazioni delle misure di sicurezza informatica: profili di responsabilità
- L'intervento del Garante della privacy in materia di misure di sicurezza

MODULO 3 – IL CODICE DELL'AMMINISTRAZIONE DIGITALE

- Il rinnovamento della Pubblica Amministrazione
- Informatizzazione
- Dematerializzazione
- Digitalizzazione
- E-Government
- L'Amministrazione nell'era digitale
- Il CAD e le recenti modifiche L'analisi del Codice dell'Amministrazione Digitale: obiettivi, strategie, effetti
- Principi generali
- La qualità dei servizi resi e soddisfazione dell'utenza
- L'organizzazione delle Pubbliche Amministrazioni
- Gli strumenti dell'informatizzazione: documento informatico e firme elettroniche
- Le novità del D.Lgs 179/2016
- Formazione, gestione e conservazione dei documenti informatici
- La comunicazione e l'accesso ai dati
- Sviluppo, acquisizione e riuso dei sistemi informatici nelle Pubbliche Amministrazioni
- L'informatizzazione e la trasparenza nelle Pubbliche Amministrazioni
- La pubblicazione dei dati e la trasparenza
- L'Agenda Digitale



MODULO 4 – IL REGOLAMENTO UE 679/2016 E LE NUOVE NORME SULLA PRETEZIONE DEI DATI PERSONALI

- Il Regolamento UE 679/2016
- I principi
- I diritti dell'interessato
- I titolari e i responsabili del trattamento
- Sanzioni e rimedi

MODULO 5 – PEC, DOCUMENTI DIGITALI E DEMATERIALIZZAZIONE DEGLI ARCHIVI CARTACEI

- La Posta Elettronica Certificata
- Cos'è la PEC
- Il registro di log
- Messaggi di PEC con virus informatici
- La firma digitale
- Cos'è la firma digitale
- Il contrassegno elettronico e il sigillo elettronico Archiviazione dei documenti digitali
- La digitalizzazione della PA
- Le copie • Il sistema e i requisiti per la conservazione dei documenti informatici

MODULO 6 – IT SECURITY

- Definizioni
- Le finalità dell'IT Security
- Il concetto di privacy
- Misure per la sicurezza dei file Maleware
- Gli strumenti di difesa
- L'euristica La sicurezza delle reti
- La rete e le connessioni
- Navigare sicuri con le reti wireless Navigare in sicurezza
- Il browser e la sicurezza online
- Gli strumenti messi a disposizione da Google Chrome
- Strumenti di filtraggio dei contenuti Sicurezza nella comunicazione online
- La vulnerabilità della posta elettronica
- Come gestire gli strumenti di comunicazione online
- La tecnologia peer to peer Sicurezza dei dati
- Gestire i dati sul PC in maniera sicura
- Il ripristino di sistema
- Eliminare i dati in modo permanente

MODULO 7 – RISK MANAGEMENT: RUOLI E FUNZIONI DEL SECURITY MANAGER

- Norme tecniche di "security risk management"
- Elementi di analisi del rischio: Metodologie e strumenti



- Metodologia di identificazione dei pericoli, di quantificazione e valutazione dei rischi di origine criminosa, di definizione dei criteri di accettabilità. Di identificazione delle misure di mitigazione.
- Procedure, linee guida norme tecniche per la gestione del rischio nel proprio ambito operativo
- Metodologie per la valutazione del grado di security nel territorio e nelle comunità ospitanti
- Identificazione del rischio prevalente nell'area
- Strumenti per valutare l'impatto delle attività di security sul contesto sociale ed economico di riferimento
- L'organizzazione e le sue strutture fisiche
- Modelli e tipologie di organizzazione e gestione della security
- Principi di prevenzione dei rischi di origine criminosa attraverso la progettazione ambientale e urbanistica
- Tecnologie di prevenzione e protezione della security
- Gestione dei servizi integrati di sicurezza
- Elementi di coordinamento della continuità operativa ("business continuità" e "disaster recovery")
- Elementi di coordinamento della gestione della crisi (crisis management")
- Modalità di predisposizione di piani di security
- Sistemi e tecniche di monitoraggio e "reporting"
- Modalità e gestione dei contratti di security
- Procedure di security dell'Organizzazione e modalità di rilevamento di eventuali non conformità rispetto alle esigenze della stessa Organizzazione

Per ulteriori informazioni e/o per le iscrizioni, è possibile contattare dal lunedì al sabato dalle ore 9:00 alle 13:00 e dalle 16:00 alle 20:00 la segreteria studenti della Salerno formazione ai seguenti recapiti telefonici 089.2960483 e/o 338.3304185.

SITO WEB: www.salernoformazione.com