MODULO 11 - *Cybercrime*
- Sistemi informatici e misure di sicurezza alla luce del framework normativo europeo (NIS Directive e GDPR)
- Digital crimes
- L. 48/2008 e DLgs. 231/2001 - modelli organizzativi
- La disciplina del Whistleblowing, L. 79/2017 e DLgs. 231/2007, come modificato da L.90/2017 e
- Principi di digitalforensics in azienda e rapporti con le Autorità Giudiziarie

MODULO 12 - *Privacy in Sanità pubblica e privata: impatti GDPR*
- Privacy e sanità: tematiche ricorrenti in ambito pubblico e privato
- FSE, dossier sanitario e trattamento dei dati personali
- Cartella clinica e dati sanitari

Periodo di svolgimento:
- Ottobre/Novembre 2019
- per un monte ore di 80

Luogo di svolgimento:
Palermo
Numero partecipanti: min 30, max 50
- Costo: € 700 da versare tramite bonifico presso: UNICREDIT - Agenzia 100, Palermo
- Beneficiario: DEMS, Università degli Studi di Palermo
- Causale: Nome Cognome - D20 DPO
- IBAN : IT 09 A 02008 04682 000300004577

Il modulo di iscrizione è disponibile sul sito:
wwww.dipartimentodems.unipa.it

Comitato scientifico:
Nadia Arnaboldi - Coordinatore Scientifico ASSO DPO
Alessandro Bellavista - Università di Palermo
Fabio Ferrara - Vicepresidente ASSO PDO
Graziano Garrisi - Privacy Consultant e Responsabile Dati
Marco Mancarella - Università del Salento
Gabriella Marcatajo - Università di Palermo
Antonello Miranda - Università di Palermo

Responsabili organizzativi
Dott. **Mario Gagliano**
Dott.ssa **Maria Rita Di Stefano**
Tel: +39.09123892515 - 3208514987
dems@unipa.it
www.dipartimentodems.unipa.it
Dipartimento di Scienze Politiche e delle Relazioni Internazionali - DEMS
Via Ugo A. Amico 2/4 90134 - PALERMO (PA)

UNIVERSITÀ DEGLI STUDI DI PALERMO

grafica: alessandro.paranunzio@unipa.it

Data Protection Officer

Presentazione del Corso di Alta Formazione per

RESPONSABILE PROTEZIONE DATI - DPO

Una nuova professione per una reale conformità privacy degli Enti alla luce del Regolamento UE 2016/679

dems

Dipartimento di Scienze Politiche e delle Relazioni Internazionali - DEMS
Via Ugo A. Amico 2/4

Obiettivo del corso è offrire una percorso formativo caratterizzato da livelli elevati di qualità formativa e professionale nel campo della gestione delle problematiche privacy, in enti pubblici e privati, concentrandosi essenzialmente sulla formazione della figura professionale del Responsabile della Protezione dei Dati personali (Data ProtectionOfficer – DPO), sempre nel rispetto delle prescrizioni di cui alla Norma UNI 11697:2017 "Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza" (rif. Punto 5.1 della citata Norma).In ogni caso, il discente acquisirà nozioni che possano supportarlo anche in caso di semplice nomina quale Designato o Autorizzato al trattamento dei dati personali all'interno dell'ente in cui opera o in altre mansioni connesse al settore (ad es. componente Ufficio privacy o componente Team DPO o semplice consulente).

Profilo professionale che si intende formare: il professionista del settore Privacy che sia in grado di governare la materia e gestire al meglio il ruolo di RPD/DPO all'interno di enti pubblici o privati, con solide basi teoriche e adeguati strumenti operativi.

Programma del corso e contenuti generali

MODULO 1 - *Introduzione*

- Genesi ed evoluzione storica della protezione dei dati personali
- La nuova normativa europea: Regolamento UE n. 679/2016 (GDPR)
- La normativa italiana: il D.Lgs. n. 196/2003 (come modificato dal D.Lgs. 101/2018)
- Cenni sulle connessioni ulteriori normative impattanti sulla privacy in ambito europeo e italiano
- Le specifiche norme attinenti al sistema sanitario

MODULO 2 - *Reg. UE 2016/679 e Codice Privacy: aspetti generali*

- Ambiti di applicazione della nuova normativa
- Le principali novità introdotte dal GDPR
- Definizioni
- Basi giuridiche del trattamento
- Categorie particolari di dati (sensibili e giudiziari)
- Informativa e consenso - artt. 13 e 14 GDPR
- Il consenso in ambito santario
- I soggetti – ruoli nella nuova disciplina
- L'Individuazione del Titolare autonomo
- Il soggetto interessato: nuovo ruolo e nuovi diritti
- Il principio di accountability
- Modelli organizzativi e procedure indispensabili (con focus in Sanità)
- Privacy by design e privacy by default
- Registro dei trattamenti (con focus in Sanità)
- L'Organismo nazionale di accreditamento: per l'Italia, Accredia

MODULO 3 - *Reg. UE 2016/679 e Codice Privacy: misure di sicurezza*

- Sicurezza dei dati e misure adeguate - art. 32 GDPR
- Data Breach: definizione e notificazione - artt. 33 e 34 GDPR
- Trasferimenti di dati all'estero e condizioni di adeguatezza
- Data Protection Impact Assessment (DPIA)
- Provvedimento Garante privacy 11 ottobre 2018 e sistema sanitario
- Tecniche di pseudonimizzazione, crittografiche e dianonimizzazione

MODULO 4 – *Tutela giurisdizionale*

- Autorità Garante ruolo, provvedimenti e sistema di controlli
- Fase di transizione e sanzioni
- Reclamo all'Autorità Garante
- Responsabilità e sanzioni per il Titolare, Co-Titolare ed il Responsabile
- Tutele e danno risarcibile (Italia/Europa)
- Garanti Europei e Comitato Europeo protezione dati

MODULO 5 - *Compliance aziendale*

- La leadership nella gestione del rischio
- Analisi di rischi e misure (con focus in Sanità)
- Riskbasedapproach e approccio ISO 31000:2018
- Misure di sicurezza secondo l'art. 32 GDPR – gap analysis
- Privacy by design and default in un'azienda, policies ed organizzazione aziendale
- Violazioni dei dati - Data breach, artt. 33 e 34 GDPR – policy e procedura
- Diritto dell'interessato, diritto all'oblio, portabilità dei dati – procedure di riscontro
- Social media e dati personali, approfondimento sui diritti dell'interessato e portabilità
- Codici di condotta e certificazioni
- Proprietà intellettuale e GDPR

MODULO 6 - *Data ProtectionOfficer (DPO)*

- Nuovi profili introdotti con il GDPR a confronto
- Profilo e compiti del DPO
- Il DPO in ambito sanitario
- La norma UNI 11697:2017 e i diversi ruoli
- Designazione: la scelta, l'esperienza e le competenze (requisiti minimi)
- Indipendenza e conflitti d'interesse del DPO
- Pianificazione delle attività del DPO
- Rapporti con il Garante, attività, compiti, ispezioni e sanzioni
- Casi di studio, monitoraggio su larga scala, sistematico, gruppi di imprese
- Case history: ruolo del DPO in un ente pubblico o privato

MODULO 7 - *Privacy e tutela dei lavoratori*

- Videosorveglianza nei luoghi di lavoro, criticità e sfide (art. L.300/1970 e Jobs Act)
- Controlli sul lavoro e tecnologie (e-mail, devices aziendali e policy interne)
- Trattamenti dati del personale di lavoratori (medico competente ed altri soggetti esterni)
- Privacy in azienda: criticità nell'ambito del rapporto di lavoro (mappatura trattamenti, autorizzati di diversi livelli)
- Controlli difensivi e indagini sui dipendenti infedeli e disciplina privacy

MODULO 8 - *WP 29 ed EDPB : focus tematici*

- WP 29 ed EDPB: direttive per l'applicazione del GDPR
- WP 29 ed EDPB: guidelines sulle app
- Amministratori di sistemi e Log: il provvedimento generale del GdP
- Internet of things, Privacy by design nel IoT e Big Data
- ePrivacyRegulation
- Smart City
- Cloudcomputing
- Cookies policy
- Blockchain e smartcontracts
- eCommerce

MODULO 9 - *Privacy e Reg. UE eIDAS/Codice dell'Amministrazione Digitale*

- Impatti privacy con il Regolamento eIDAS e il Codice dell'Amministrazione digitale
- Impatti privacy con la conservazione documentale a norma ed i termini di conservazione.
- Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (eIDAS)
- Privacy e Trasparenza
- Privacy e Pubblicazione legale online
- Privacy e diritto di accesso documentale e civico
- Privacy ed "eredità digitale" dei cittadini

MODULO 10 - *Cybersecurity*

- Best practice e standard di cybersecurity
- L'importanza dell'approccio architetturale rispetto al solito patchwork di security
- Tipi di Attacco e Vulnerabilità dei sistemi ICT ("Infrastructure Malware")
- Minacce avanzate e persistenti (APT)
- Stato attuale delle principali minacce informatiche
- Autenticazione, Autorizzazione e Sicurezza Perimetrale
- Multi-factorauthentication (vedi DUO o PING)
- Dalla Sicurezza Perimetrale al concetto di Sicurezza Estesa: Endpoint, Infrastructure, Cloud
- Progettazione e Governance della Sicurezza dell'Organizzazione
- SOC e/o i team di INFOSEC
- Normative sulla Sicurezza dei Sistemi ICT e sulla Protezione dei Dati
- Risk Analysis e Risk Management
- Incident Management
- Case studies in tema di Data Breach