CON IL PATROCINIO DELLA

FONDAZIONE DEL CONSIGLIO NAZIONALE FORENSE

CORSO DI PERFEZIONAMENTO E AGGIORNAMENTO PROFESSIONALE IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI PER *DATA PROTECTION OFFICER*

COMITATO SCIENTIFICO

Prof. Avv. Alberto Gambino (condirettore)
Prof. Avv. Salvatore Sica (condirettore)
Prof. Avv. Valeria Falce
Prof. Avv. Giusella Finocchiaro
Prof. Avv. Giorgio Resta
Avv. Carla Secchieri
Prof. Avv. Andrea Stazi

COORDINATORE DIDATTICO

Avv. Davide Mula

DURATA DEL CORSO

80 ore complessive - 1° ed.: 20 aprile 2018 – 26 maggio 2018

FREQUENZA

Venerdì dalle ore 14:00 alle ore 20:00 - Sabato dalle ore 9:00 alle ore 15:30

COSTO PARTECIPANTE

€ 900, da versare in due tranche di pari importo (€ 450) rispettivamente al momento dell'iscrizione e prima della conclusione del corso.
È possibile seguire anche solo alcuni dei 14 moduli. Il costo di ciascuno modulo è pari a € 80.

SEDE SVOLGIMENTO LEZIONI

Università Europea di Roma, Via degli Aldobrandeschi n. 190, 00163 Roma.

DESTINATARI

Coloro che sono in possesso di laurea quadriennale, specialistica o magistrale.

ATTESTATO DI PARTECIPAZIONE

A coloro che avranno frequentato l'intero corso verrà rilasciato un attestato di conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere ai compiti di cui all'art. 39 del Regolamento (UE) n. 2016/679, recante il Regolamento Generale sulla Protezione dei Dati personali (RGPD).

L'attestato comporta il riconoscimento di 20 crediti per la formazione continua degli avvocati.

CON IL PATROCINIO DELLA

FONDAZIONE DEL CONSIGLIO NAZIONALE FORENSE

DESCRIZIONE DEL CORSO

Il presente corso di perfezionamento e aggiornamento professionale in materia di trattamento dei dati personali ha durata trimestrale e si prefigge di far acquisire ai candidati le competenze necessarie per svolgere la funzione di Responsabili per la Protezione dei Dati (*Data Protection Officer* - DPO) di cui all'art. 37 e seguenti del RGPD.

L'*iter* formativo prevede quindi l'acquisizione di competenze trasversali giuridiche e tecniche in relazione al quadro normativo delineato dal RGPD ed alle *best practices* in materia di sicurezza delle reti.

Il corso ha avuto il patrocinio del Consiglio Nazionale Forense e della Scuola Superiore dell'Avvocatura e la frequenza comporta l'attribuzione di 20 crediti per la formazione continua degli avvocati.

FINALITÀ FORMATIVE

Il Corso si rivolge, in primo luogo, a coloro i quali già operano nel settore del trattamento dei dati personali e necessitano di aggiornamento e/o di una formazione specifica ed avanzata in materia di *privacy* e sicurezza informatica al fine di assolvere ai compiti del DPO di cui all'art. 39 del RGPD.

Il Corso si rivolge, altresì, ai soggetti che intendono accrescere la loro professionalità riguardo le problematiche relative alla sicurezza informatica dei sistemi informativi e delle reti informatiche, dal punto di vista manageriale, organizzativo, normativo e tecnologico.

STRATEGIA DELL'APPRENDIMENTO E DELL'INSEGNAMENTO

I discenti saranno esposti a un programma accademico e professionale interdisciplinare affidato ad accademici, professionisti del settore e rappresentanti delle istituzioni coinvolte nell'applicazione del RGPD.

I discenti potranno essere coinvolti in *case-study*, esercitazioni pratiche, seminari e *workshop*.

La strategia di apprendimento e di insegnamento si fonda sulla ricerca attuale oltre che sui requisiti della pratica professionale e riflette i risultati educativi del programma.

Al termine del corso verrà svolta una prova volta alla verifica dell'acquisizione delle competenze per lo svolgimento delle funzioni di DPO.

CARATTERISTICHE DEL CORSO

Il corso intende soddisfare il forte fabbisogno di accrescimento formativo e specializzazione che proviene da aree professionali emergenti legate ai concetti di corretto trattamento dei dati personali e di sicurezza informatica: di chi risponde della sicurezza dei propri sistemi informativi nei confronti dei propri clienti, di chi ha la necessità di impostare o rafforzare gli schemi e le politiche di sicurezza.

In estrema sintesi, l'obiettivo del presente corso è quello di formare DPO consapevoli.

CON IL PATROCINIO DELLA

FONDAZIONE DEL CONSIGLIO NAZIONALE FORENSE

CORPO DOCENTE

avv. Giuseppe Busia, Segretario generale del Garante per la tutela dei dati personali
avv. Bruno Carotti, Agcom
prof. Gianluigi Ciacci, Luiss Guido Carli
avv. Giorgio Giannone Codiglione, Università di Salerno
dott. Cosimo Comella, Dirigente del Garante per la tutela dei dati personali
avv. Paolo Del Vecchio, Agcom
dott. Claudio Filippi, Vice-Segretario generale del Garante per la tutela dei dati personali
prof. Corrado Giustozzi, Agenzia per l'Italia Digitale
avv. Roberta Guizzi, Avvocatura dello Stato
avv. Elena Maggio, Studio legale Gambino
prof. Alessandro Mantelero, Politecnico di Torino
dott. Francesco Modafferi, Dirigente del Garante per la tutela dei dati personali
dott. Massimo Montanile, DPO
avv. Davide Mula, Università Europea di Roma
avv. Martina Provenzano, Università Europea di Roma
prof. Giovanni Riccio, Università di Salerno
n.b. non tutti i docenti invitati hanno già confermato la loro disponibilità

PROGRAMMA DEL CORSO

Le lezioni del Corso si svolgeranno il venerdì (dalle ore 14:00 alle ore 20:00) ed il sabato (dalle ore 9:00 alle ore 15:30), a partire dal 20 aprile p.v. e sino al 26 maggio 2018, secondo il seguente programma.

EVOLUZIONE NORMATIVA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI

1. La direttiva 95/46/Ce: principi generali
2. Il recepimento della direttiva: dalla legge 675/1996 e al Codice Privacy
3. Il Regolamento Ue n. 679/2016
4. Entrata in vigore e termine di adeguamento
5. Rapporto tra Regolamento europeo e normative nazionali

AMBITO DI APPLICAZIONE DEL REGOLAMENTO

1. Il trattamento per finalità esclusivamente personali o domestiche
2. Il titolare stabilito nel territorio EU
3. L'interessato residente nel territorio EU

TIPOLOGIE DI DATI PERSONALI

1. I dati delle persone fisiche
2. I dati delle persone giuridiche

3. Il trattamento dei dati sensibili
4. Il trattamento di dati giudiziari
5. Il trattamento dei dati genetici
5. Il trattamento dei dati biometrici
6. L'anonimizzazione e la pseudoanonimizzazione di dei dati personali
7. Il trattamento dei dati personali di persona deceduta

I PRINCIPI GENERALI DEL REGOLAMENTO

1. Il principio di liceità
2. Il principio di correttezza
3. Il principio di trasparenza
4. Il principio di pertinenza
5. Il principio di necessità
6. Il principio di *accountability*
7. Il principio della *privacy by design* e *by default*

IL CONSENSO

1. Il consenso al trattamento
2. L'informativa preventiva
    - 2.1. L'informativa da fornire quando i dati personali sono raccolti presso l'interessato
    - 2.2. L'informativa da fornire quando i dati personali non sono raccolti presso l'interessato
    - 2.3. L'informativa e consenso al trattamento necessario per adempiere a contratto
    - 2.4. L'informativa e consenso al trattamento necessario per obbligo di legge
    - 2.5. L'informativa e consenso al trattamento necessario per salvaguardia interessi vitali dell'interessato o di altra persona fisica
    - 2.6. L'informativa e consenso al trattamento necessario per interesse pubblico
    - 2.7. L'informativa e consenso al trattamento in ambito sanitario
3. La prestazione del consenso
    - 3.1. Il consenso dei minori di anni 16
    - 3.2. Il consenso obbligatorio e facoltativo
    - 3.3. Il consenso dei dati sensibili
4. Le modalità di acquisizione del consenso
5. La dimostrazione dell'acquisizione del consenso
6. La revoca del consenso

I DIRITTI DELL'INTERESSATO

1. Il diritto alla conoscenza delle fonti dei dati
2. Il diritto all'aggiornamento dei dati
3. Il diritto alla cancellazione (diritto all'oblio)
4. Il diritto di limitazione del trattamento

5. Il diritto alla portabilità dei dati
6. Il diritto di opposizione
7. Il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione
8. Le modalità e le condizioni di esercizio dei diritti dell'interessato

I SOGGETTI PREPOSTI AL TRATTAMENTO

1. Il titolare del trattamento
    1.1. La responsabilità del titolare
    1.2. Le ipotesi di contitolarità
2. Il responsabile del trattamento
    2.1. Il responsabile del trattamento e la designazione di sub-responsabili
3. Gli incaricati del trattamento
4. Gli amministratori di sistema
5. Il Data Protection Officer
    5.1. L'obbligo di nomina del DPO
    5.2. I requisiti di professionalità del DPO
    5.3. Le garanzie e gli obblighi del DPO
    5.4. Il DPO interno ed esterno
    5.5. La designazione del DPO e la notifica al Garante
    5.6. I compiti del DPO
    5.7. Il DPO delle PA
6. L'organigramma privacy e i registri delle attività di trattamento

I TRASFERIMENTI DI DATI PERSONALI INFRAGRUPPO E VERSO PAESI TERZI

1. I presupposti e le condizioni del trasferimento dei dati
2. Le norme vincolanti d'impresa – Binding corporate rules (Bcr)

I TRATTAMENTI DEI DATI PER FINALITÀ DI POLIZIA, GIUSTIZIA E SICUREZZA

1. I trattamenti per finalità di sicurezza nazionale, politica estera e sicurezza dell'unione
2. Le finalità di indagini o perseguimento dei reati (rinvio alla direttiva 680/2016)
3. Il trattamento dei dati personali da parte delle autorità giurisdizionali
4. La responsabilità degli intermediari della società dell'informazione nel trattamento dei dati per finalità di polizia, giustizia e sicurezza

ARCHITETTURE IT E SICUREZZA DEI DATI

1. Le architetture IT preposte al trattamento dei dati
    1.1 Le architetture standard internazionali (COBIT 5 e ITIL v3)
    1.2. Le architetture per paradigmi Privacy-by-Design e Security-by-Design
2. Le qualità tecniche dei dati

3. Le tecniche di pseudoanonimizzazione
4. Le tecniche di criptazione dei dati
5. Le tecniche per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
6. Le tecniche di backup e recovery
7. Le principali ipotesi di data breach
8. L'analisi e la documentazione del data breach
9. L'importanza della cifratura ai fini della notifica del data breach
10. Le tecniche di simulazione: penetration test

STANDARD INTERNAZIONALI DI SICUREZZA

1. Lo standard di gestione per la sicurezza delle informazioni: ISO 27001:2013
    1.1. L'analisi dei rischi delle informazioni
    1.2 La pianificazione degli obbiettivi della sicurezza
    1.3. Le procedure di controllo operativo
    1.4. Il riesame periodico delle attività
    1.5. Il monitoraggio del rispetto degli adempimenti Privacy
2. Lo standard di conduzione degli audit: ISO 19011:2011
    2.1. La pianificazione e la gestione degli audit
    2.2. La nozione di Non conformità e di Osservazioni
    2.3. Le tipologie di azione correttive

LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI E LA CONSULTAZIONE PREVENTIVA

1. L'obbligo della valutazione d'impatto sulla protezione dei dati
2. I Codici di condotta e la valutazione d'impatto
3. Le modalità di valutazione d'impatto sulla protezione dei dati
4. La documentazione delle valutazioni
5. La consultazione preventiva per i trattamenti

LA PROTEZIONE DEI DATI PERSONALI NELLA PA

1. La protezione dei dati personali e la disciplina dell'accesso ex l. 241/90
2. Il D.Lgs. 33/2013 e l'accessibilità totale
3. L'accesso civico e accesso civico generalizzato (FOIA)
4. L'Open data e il riutilizzo
5. Il bilanciamento tra obblighi di trasparenza

MEZZI DI RICORSO, RESPONSABILITÀ E SANZIONI

1. Il reclamo a un'autorità di controllo
    1.1. Il principio del *One Stop Shop*
2. Il ricorso giurisdizionale effettivo

2.1. Nei confronti dell'autorità di controllo
2.2. Nei confronti del titolare o del responsabile del trattamento
3. Il procedimento del ricorso giurisdizionale effettivo
4. L'azione di responsabilità
5. Le condizioni generali per le sanzioni

MODALITÀ D'ISCRIZIONE

L'iscrizione potrà essere compilata utilizzando esclusivamente il sistema informatico Esse3

La domanda d'iscrizione, debitamente compilata online, andrà stampata, sottoscritta e spedita mediante **raccomandata con ricevuta di ritorno** al seguente indirizzo:

Università Europea di Roma

Segreteria Amministrativa

Via degli Aldobrandeschi n. 190 – 00163 ROMA

Alla domanda d'iscrizione va, inoltre, allegata la seguente documentazione:

- n.1 fotografia formato tessera
- n.1 marca da bollo da Euro 16,00
- fotocopia di un documento d'identità
- fotocopia del codice fiscale
- certificazione sostituiva del titolo conseguito
- ricevuta di pagamento della I rata (che può avvenire esclusivamente tramite MAV generato da sistema)

La documentazione sopra elencata potrà essere inviata anche **tramite PEC** al seguente indirizzo di posta certificata: ***postlaurea@unier.postecert.it***
Il candidato dovrà successivamente depositare copia in originale di quanto inviato tramite pec, inclusa la marca da bollo da euro 16,00, alla Segreteria amministrativa dell'Università.

La mancata presentazione dei documenti richiesti precluderà il rilascio dell'attestato finale di partecipazione al corso.