Digital & Law Department

Euroconference
Centro Studi Forense

con il patrocinio scientifico di

ANORC Professioni

CORSO PROFESSIONALIZZANTE – 1^ EDIZIONE

DATA PROTECTION OFFICER

Ruolo e compiti della nuova figura prevista dal Regolamento 2016/679/UE

8 incontri in aula + e-learning con esame finale

BOLOGNA • MILANO • PADOVA • ROMA

DATA PROTECTION OFFICER: IL RICONOSCIMENTO DELLE COMPETENZE

IL NUOVO RUOLO SECONDO I GARANTI EUROPEI

Il 24 maggio 2016 è entrato in vigore il Regolamento europeo n. 2016/679 (General Data Protection Regulation – GDPR) che dal 25 maggio 2018 diventerà direttamente applicabile in tutti i Paesi UE. I soggetti che svolgono attività di trattamento di dati personali hanno a disposizione un "periodo di adattamento", **fino al 25 maggio 2018, data in cui le nuove regole avranno applicazione diretta e cogente nel nostro ordinamento** (così come in tutti gli Stati membri).
Per quella data, l'allineamento alle prescrizioni del GDPR dovrà essere completa, senza sconti: per rendere effettiva la "protezione delle persone fisiche con riguardo al trattamento dei dati personali" e "la libera circolazione dei dati personali medesimi" sono previsti più penetranti poteri di controllo in capo alle Autorità Garanti e un inasprimento delle sanzioni pecuniarie per un'ampia platea di soggetti, destinatari degli obblighi e delle responsabilità stabilite dal Regolamento.

Il ruolo di DPO può essere rivestito da una persona fisica, da un'organizzazione o da un team, in possesso di idonee competenze professionali. Ai sensi all'art. 37, par. 6 del Regolamento, il Responsabile della Protezione dei dati: "può essere un dipendente del Titolare del trattamento o del Responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi".
Dalle disposizioni contenute nel Regolamento europeo (art. 39 e considerando n. 97) e nelle Linee guida del WP 29, emendate e adottate il 5 aprile 2017, emerge che il DPO, in sintesi, dovrebbe:

- **raccogliere informazioni per identificare le attività di trattamento;**
- **analizzare e verificare la conformità delle attività di trattamento;**
- **informare, consigliare e fornire raccomandazioni al Titolare e al Responsabile del trattamento.**

ATTESTATO DI QUALIFICAZIONE* DELLE COMPETENZE PER IL DATA PROTECTION OFFICER

La frequenza al Corso è valida ai fini del riconoscimento delle competenze inerenti al ruolo previsto dal Regolamento europeo. Al termine del Corso il professionista sarà in grado di svolgere le funzioni di controllo, coordinamento e supervisione della corretta gestione e tutela dei dati personali contenuti nei sistemi informativi dell'organizzazione in cui opera, delineando e implementando, difatti, le misure di privacy e sicurezza.
Il Corso è valido ai fini dell'accesso all'esame per l'iscrizione all'**Elenco dei Professionisti della Privacy di ANORC Professioni**, ai sensi della Legge del 14 gennaio 2013 n. 4 sulle professioni non organizzate in Ordini o Collegi.

ANORC Professioni è un'Associazione professionale, indipendente e senza scopo di lucro, nata con l'obiettivo di dare regolamentazione e riconoscimento ai Professionisti della digitalizzazione documentale e della privacy, figure ormai necessarie in ogni moderna organizzazione, sia pubblica che privata.
ANORC Professioni attribuisce riconoscimento a questi Professionisti e alle loro competenze attraverso l'iscrizione a un elenco nazionale, in ottemperanza a quanto stabilito dalla Legge n.4 del 14/01/13 sulle professioni non organizzate in Ordini o Collegi. È inserita nell'elenco delle Associazioni Professionali presso il Ministero dello Sviluppo Economico, nella sezione dedicata alle Associazioni che rilasciano l'attestato di qualità e di qualificazione professionale dei servizi prestati all'associato.
Tale legge apre nuovi importanti orizzonti e riconoscimenti alla nuova professione, già richiesta dal mercato e ora prevista dalla normativa.
Per maggiori informazioni, si consiglia di consultare la pagina del sito web:
https://www.anorc.eu/anorc-professioni/chi-siamo-anorc-professioni

*** Regolamento Ue e certificazione in materia di dati personali**
Il Garante Privacy e ACCREDIA richiamano l'attenzione sulla necessità di attendere la definizione di criteri e requisiti comuni per la conformità delle certificazioni in materia di protezione dati al Regolamento UE 2016/679.
Per ulteriori dettagli, si rimanda al seguente link: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6621723

CARATTERISTICHE DEL CORSO PROFESSIONALIZZANTE DPO

OBIETTIVI E DESTINATARI

Il Corso per il "Data Protection Officer" fornirà ai partecipanti una preparazione manageriale completa e multidisciplinare secondo quanto previsto dal Regolamento UE per la protezione dei dati personali.
Il Corso è rivolto alle seguenti categorie professionali:

- Dipendenti pubblici e privati che svolgono ruoli di Responsabile privacy, Responsabile della protezione dei dati, Responsabile IT, Security Manager, Responsabile area legale, Responsabile del Trattamento, Amministratore di Sistema;
- Liberi Professionisti che svolgono attività di consulenza in materia privacy o che intendono diventare DPO di aziende pubbliche o private quali Avvocati, Commercialisti, Consulenti del Lavoro, Consulenti della Privacy, Consulenti Informatici, Risk Manager.

METODOLOGIA E STRUTTURA DEL CORSO

Tutti gli argomenti del Corso sono affrontati con taglio operativo e con una metodologia didattica interattiva, affiancando all'analisi dei singoli argomenti case history ed esercitazioni pratiche.
Il Corso rilascia un attestato di frequenza per un totale di **80 ore** di formazione suddivise in tre macroaree:

Modulo I – 5 giornate in presenza (35 ore)
Il Regolamento Europeo n.679/2016: coordinamento e differenze con l'attuale Codice Privacy

Modulo II – 2 giornate in presenza (14 ore)
La data security alla luce del nuovo Regolamento europeo: quali accorgimenti?

Modulo III – 1 giornata (7 ore)
Il trattamento dei dati negli archivi e nei cloud

Modulo IV in modalità e-learning (24 ore di formazione)
Laboratori verticalizzati su:

- eHealth
- Pubblica Amministrazione e pubblicazione online
- Videosorveglianza e controllo dei lavoratori
- Privacy e social banking

ESAME FINALE E ATTESTATI

A chiusura del Corso - e previa frequenza dell'80% delle ore formative - si è ammessi all'esame finale valido ai fini dell'iscrizione all'elenco dei Professionisti della privacy di ANORC Professioni per ottenere l'attestato di qualità dei servizi professionali.
In caso di mancato superamento dell'esame finale si riceverà l'**Attestato di partecipazione al Corso di Data Protection Officer.**
L'esame consisterà in un colloquio orale che si svolgerà in modalità telematica tramite la piattaforma BitMeeting (https://www.bitmeeting.it/) sulle materie affrontate durante il percorso. L'esame si terrà durante la seconda settimana di aprile 2018 sulla base del numero delle iscrizioni pervenute.

CALENDARIO, FACULTY E CREDITI FORMATIVI

Orario, Sedi e Data

Le lezioni si terranno dalle 09.30 alle 13.00 e dalle 14.00 alle 17.30

BOLOGNA ZanHotel			***MILANO*** Hotel Michelangelo			***PADOVA*** Best Western Hotel Biri			***ROMA*** C.C. Cavour		
17	gennaio	2018	18	gennaio	2018	22	novembre	2017	16	novembre	2017
24	gennaio	2018	25	gennaio	2018	29	novembre	2017	23	novembre	2017
07	febbraio	2018	08	febbraio	2018	13	dicembre	2017	14	dicembre	2017
21	febbraio	2018	22	febbraio	2018	17	gennaio	2018	18	gennaio	2018
28	febbraio	2018	01	marzo	2018	24	gennaio	2018	25	gennaio	2018
14	marzo	2018	15	marzo	2018	07	febbraio	2018	08	febbraio	2018
21	marzo	2018	22	marzo	2018	21	febbraio	2018	22	febbraio	2018
28	marzo	2018	29	marzo	2018	07	marzo	2018	08	marzo	2018

Coordinatore Scientifico

Andrea Lisi
Avvocato, Coordinatore del Digital&Law Department dello Studio Legale Lisi, Presidente ANORC Professioni

Corpo Docente

Luca Bolognini
Avvocato, Presidente Istituto Italiano per la Privacy

Andrea Caccia
Ingegnere, esperto sicurezza informatica

Carola Caputo
Avvocato, consulente del D&L Department dello Studio Legale Lisi, esperta privacy e conservazione

Franco Cardin
Consiglio Direttivo di ANORC, esperto privacy in ambito sanitario

Claudio Di Cocco
Avvocato, Professore a contratto in Diritto dell'Informatica dell'Università di Bologna

Lino Fornaro*
Coordinamento ANORC Privacy, esperto sicurezza informatica

Alessandro Frillici*
Avvocato, Coordinatore Osservatorio Privacy e Sicurezza delle Informazioni di AIP - ICTS (Associazione Informatica Professionisti)

Diego Fulco
Avvocato, Direttore Scientifico dell'Istituto Italiano per la Privacy

Patrizia Ghini
Of Counsel D&L Department dello Studio Legale Lisi, Commercialista, Revisore dei conti e Giornalista pubblicista

Corrado Giustozzi*
Comitato dei Saggi di ANORC, esperto sicurezza informatica

Fabio Guasconi
Esperto e Consulente per la Sicurezza delle Informazioni

Michele Iaselli
Avvocato, esperto privacy, Presidente Associazione Nazionale per la Difesa della Privacy (ANDIP)

Giovanni Manca
Presidente ANORC, esperto sulle tematiche di dematerializzazione e sicurezza ICT

Enrico Pelino
Avvocato, esperto privacy

Alessio L.R. Pennasilico
Presidente AIP - ITCS (Associazione Informatici Professionisti), Esperto Sicurezza Informatica

Lucio Scudiero
Avvocato, esperto privacy

Sarah Ungaro
Avvocato, consulente del D&L Department dello Studio Legale Lisi, esperta privacy e conservazione

Giovanni Ziccardi
Professore Associato di Informatica Giuridica presso la Facoltà di Giurisprudenza dell'Università degli Studi di Milano

* Docenti invitati e in attesa di conferma.

Crediti formativi

Ai fini della formazione professionale continua è stata inoltrata richiesta di accreditamento a:

Consiglio Nazionale Forense

Consiglio Nazionale Ingegneri

Consiglio Nazionale Consulenti del Lavoro

(gli aggiornamenti sull'avvenuto accreditamento su www.euroconference.it)

Materiale Didattico

A supporto dell'attività di studio saranno disponibili tutte le slide e i testi normativi utilizzati durante il percorso formativo.

PROGRAMMA

I MODULO

IL REGOLAMENTO EUROPEO N.679/2016: COORDINAMENTO E DIFFERENZE CON L'ATTUALE CODICE IN MATERIA DI PROTEZIONE DEI DATI PROFESSIONALI, REDISTRIBUZIONE DEI RUOLI E NUOVE PROFESSIONALITÀ

I giornata

- **Principi generali**
- **Diritti dell'interessato e strumenti di tutela**

Le tematiche di approfondimento saranno inerenti all'ambito di applicazione del Regolamento Europeo Privacy; l'analisi dei principi generali del trattamento e principio di responsabilità (accountability); condizioni di liceità del trattamento, legittimo interesse del titolare o di terzi; i diritti dell'interessato e strumenti di tutela; le novità in tema di informativa, consenso e richiesta di accesso ai dati; i diritti conoscitivi e di controllo dell'interessato (diritto all'informativa, diritto di accesso, diritto alla comunicazione di una violazione dei dati, diritto alla limitazione del trattamento, diritto di opposizione, diritto alla portabilità dei dati personali, diritto di rettifica e integrazione, diritto alla cancellazione e oblio); dati comuni, sensibili e le nuove "categorie particolari" di dati personali del GDPR.

II giornata

- **Il responsabile della protezione dei dati DPO**
- **Le attività e adempimenti del DPO**

Nello specifico, si approfondirà la figura del DPO come prevista dal Regolamento Europeo Privacy, la sua designazione e formalizzazione dell'incarico, i requisiti necessari, i suoi compiti e profili operativi e organizzativi, i doveri connessi alla violazione dei dati personali, le sue responsabilità; i soggetti del trattamento (titolare, contitolare, responsabile, sub- responsabile, rappresentante del titolare e del responsabile, incaricati.

III giornata

- **Trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali**
- **Violazioni e sanzioni**

Gli argomenti di approfondimento concerneranno: il diritto all'oblio e la portabilità dei dati nel nuovo Regolamento Europeo; autorità di controllo, Comitato europeo per la protezione dei dati e Commissione; le violazioni ricorrenti; il sistema disciplinare/sanzionatorio; la circolazione dei dati infra gruppo e nelle holding.

IV giornata

- **Obblighi e adempimenti per PA e aziende Titolari e Responsabili del trattamento - Come adeguarsi in concreto al nuovo approccio basato sul rischio**

Gli argomenti approfonditi riguarderanno, nello specifico, gli obblighi di compliance (accountability e obbligo di rendicontazione degli adempimenti); data breach; "privacy by design" e "privacy by default"; misure di sicurezza; valutazione d'impatto sulla protezione dei dati e consultazione preventiva; codici di condotta e certificazioni; tempistiche di adeguamento e impatto sui provvedimenti del Garante: come gestire la fase di transizione dal d.lgs. 196/2003 al Regolamento 679/2016.

V giornata

- **Casi particolari di trattamento**

Gli argomenti di interesse concerneranno il trattamento di dati personali per finalità di profilazione e marketing; il trattamento nell'ambito dei rapporti di lavoro; il trattamento dati personali nell'esercizio di controlli difensivi, nell'implementazione dei modelli 231 e nel whistleblowing; Big Data e IoT; la tutela dei dati personali nelle attività on line.

II MODULO

DATA SECURITY ALLA LUCE DEL NUOVO REGOLAMENTO EUROPEO: QUALI ACCORGIMENTI?

VI giornata

- **Gestione del rischio privacy e impatto sull'organizzazione aziendale**

Nello specifico, si affronteranno le tematiche legate al Data Protection by design e by default; definizione e implicazioni alla luce del nuovo Regolamento europeo in materia di protezione dei dati personali; Privacy Impact Assessment.

VII giornata

- **Le misure di sicurezza per la protezione dei dati personali**

Si approfondirà l'importanza dell'analisi del rischio per la determinazione delle misure di sicurezza da adottare; gli standard di sicurezza nella gestione delle informazioni; la sicurezza dei dati e dei sistemi; standard sui sistemi di sicurezza della gestione dell'informazione ISO 27001, ISO 27002.
Dopo l'approfondimento teorico, si proseguirà con un'esercitazione pratica dedicata all'analisi di un Data Breach.

III MODULO

VIII giornata

- **Il trattamento dei dati negli archivi e nel cloud**

Le tematiche riguarderanno il trattamento dei dati personali per fini di archiviazione; l'archivio dei dati personali e il contemperamento di interessi; la conservazione dei dati in archivi cartacei o su supporto magnetico/ottico; la protezione dei dati archiviati su supporti magnetici; l'archiviazione di documenti contenenti dati sensibili e/o giudiziari; il cloud computing e protezione dei dati.

IV MODULO

LABORATORI VERTICALIZZATI (in modalità e-learning)

eHealth: la gestione documentale e il trattamento dei dati in ambito sanitario

Saranno approfonditi gli aspetti su: documento informatico in sanità; trattamento dei dati personali in ambito sanitario; Fascicolo Sanitario Elettronico e Dossier sanitario; Linee guida del Garante in materia di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute; cartella clinica elettronica; ePrescription – ricetta medica elettronica.

Pubblica Amministrazione: protezione dei dati, codice degli appalti, pubblicazione on line e diritto di accesso

Le tematiche di discussione riguarderanno, nello specifico, le ultime novità normative introdotte dal decreto correttivo del Codice dei contratti pubblici (d.lgs. correttivo n. 56/2017), adottato dal Governo in attuazione della facoltà di emendamento prevista dalla Legge delega n. 11/2016; la corretta gestione degli adempimenti derivanti dalle ultime novità previste in tema di pubblicazione e accesso ai dati; le novità sul FOIA e la nuova trasparenza introdotte dal d.lgs. 25 maggio 2016, n. 97; il nuovo accesso civico; la pubblicazione di dati tramite link alle banche dati pubbliche e su Open Data.

Videosorveglianza e controllo dei lavoratori

Si discuterà di privacy e gestione delle risorse umane; valutazioni e diritto di accesso alla pratica personale; comunicazioni di dati a terzi; controllo sulle attività lavorative.

Privacy e Social Banking

Le tematiche approfondiranno gli aspetti legati alle implicazioni privacy nell'utilizzo di strumenti di web marketing; web marketing e trattamento dei dati; i rischi di illecito trattamento dei dati personali e la responsabilità amministrativa della banca per reato commesso dal dipendente; telemarketing; la disciplina sull'utilizzo dei cookie di profilazione e nell'ambito dei servizi di mobile remote payment.