ACCADEMIA EUROPEA

CORSO DI FORMAZIONE
ONLINE

ATTACCHI INFORMATICI E DATA BREACH: ADEMPIMENTI INDEROGABILI, RISCHI E RESPONSABILITÀ CIVILI E PENALI

NIS2 e GDPR alla luce delle novità normative e giurisprudenziali: obblighi di formazione, misure di sicurezza e gestione degli incidenti. Compiti di organi apicali, dirigenti e responsabili e ruolo di DPO e referenti CSIRT.

Venerdì 15 Gennaio 2027
dalle ore 9,00 alle ore 13,00

CODICE MEPA: DFG24GI

PRESENTAZIONE

La prevenzione degli attacchi informatici e la gestione delle violazioni dei dati personali richiedono misure di sicurezza adeguate, una chiara attribuzione dei compiti e personale preparato a riconoscere i rischi e ad attivare tempestivamente le procedure previste. Le decisioni degli organi apicali, l'organizzazione delle attività, la formazione e il coordinamento tra le diverse funzioni assumono un ruolo centrale anche nella valutazione delle responsabilità conseguenti a un incidente.
Il corso esamina gli adempimenti inderogabili in materia di cybersicurezza e protezione dei dati personali, attraverso una lettura coordinata della disciplina NIS2, recepita dal D.Lgs. 138/2024, e del GDPR, con attenzione alle determinazioni dell'Agenzia per la cybersicurezza nazionale, agli adempimenti rilevanti per il 2027 e agli aggiornamenti normativi e

giurisprudenziali. Gli obblighi saranno analizzati in relazione al tipo di organizzazione, ai trattamenti effettuati e alle funzioni concretamente esercitate dai diversi soggetti.
Particolare attenzione sarà dedicata all'obbligo di formazione in materia di sicurezza informatica degli organi di amministrazione e direttivi dei soggetti NIS, alla promozione della formazione periodica dei dipendenti e alle istruzioni e ai comportamenti richiesti al personale che tratta dati personali. Saranno approfonditi i compiti di amministratori, dirigenti e responsabili, il ruolo di consulenza e sorveglianza del DPO e le funzioni del punto di contatto NIS e del referente CSIRT.
Il percorso affronta inoltre i rischi e i presupposti delle responsabilità civili e penali, il risarcimento dei danni e le conseguenze sanzionatorie delle violazioni. L'esame della giurisprudenza e di situazioni applicative consentirà di collegare gli obblighi di prevenzione alle procedure da attivare in caso di ransomware, compromissione delle credenziali, indisponibilità dei sistemi e sottrazione di dati.
Responsabile scientifico del corso: Avv. Prof. Andrea R. Sirotti Gaudenzi.

PRIMO MODULO
Dalle ore 9,00 alle ore 11,00 - Docente: Avv. Prof. Andrea Sirotti Gaudenzi
GDPR, sicurezza dei dati e data breach: obblighi, rischi e responsabilità civili e penali

1. Protezione dei dati personali e ripartizione dei compiti
Principi del GDPR e responsabilizzazione dell'organizzazione. Compiti del titolare, del responsabile del trattamento e del personale autorizzato. Funzioni degli organi apicali e dei dirigenti. Autonomia, consulenza e sorveglianza del DPO.

2. Gli obblighi di sicurezza ai sensi dell'art. 32 GDPR
Valutazione dei rischi e individuazione delle misure tecniche e organizzative adeguate. Criteri di proporzionalità, verifica dell'efficacia delle misure e aggiornamento delle procedure. Documentazione delle scelte e delle attività svolte.

3. Misure di protezione e sicurezza nel lavoro quotidiano
Riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi. Cifratura, controllo degli accessi, gestione delle credenziali, copie di sicurezza e ripristino. Utilizzo della posta elettronica, dei servizi cloud e degli strumenti di condivisione dei documenti.

4. Formazione, istruzioni e comportamenti del personale
Istruzioni al personale autorizzato, obblighi di riservatezza e sensibilizzazione rispetto ai rischi del trattamento. Riconoscimento delle comunicazioni sospette e segnalazione delle anomalie. Rilevanza delle procedure interne e delle condotte del personale nella prevenzione degli incidenti.

5. Data breach: valutazione e adempimenti
Violazioni della riservatezza, dell'integrità e della disponibilità dei dati personali. Valutazione del rischio per le persone interessate. Presupposti e termini della notifica al Garante e della comunicazione agli interessati ai sensi degli artt. 33 e 34 GDPR. Documentazione delle violazioni e motivazione delle decisioni adottate.

6. Responsabilità civile e risarcimento del danno
Violazione degli obblighi di protezione, danni materiali e immateriali, nesso causale e criteri di imputazione ai sensi dell'art. 82 GDPR. Responsabilità del titolare e del responsabile del trattamento. Orientamenti della giurisprudenza europea e italiana sull'adeguatezza delle misure di sicurezza, sulla prova e sulle conseguenze degli attacchi informatici.

7. Profili penali degli attacchi informatici e dei trattamenti illeciti
Accesso abusivo ai sistemi, danneggiamento informatico, frodi ed estorsioni mediante strumenti informatici. Condotte degli autori degli attacchi e possibili responsabilità individuali all'interno dell'organizzazione: presupposti e limiti. Rapporti tra responsabilità penale, risarcimento del danno e sanzioni amministrative. Aggiornamenti normativi e giurisprudenziali pertinenti.

SECONDO MODULO
Dalle ore 11,00 alle ore 13,00 - Docente: Avv. Gualtiero Roveda
NIS2, obblighi di formazione e gestione degli incidenti: organizzazione, misure di sicurezza e ruolo del referente CSIRT

1. NIS2 e GDPR: ambiti di applicazione e obblighi dell'organizzazione
Il D.Lgs. 138/2024 e l'individuazione dei soggetti essenziali e importanti. Applicazione della disciplina a enti e imprese. Rapporti con fornitori e prestatori di servizi. Coordinamento tra obblighi di cybersicurezza e protezione dei dati personali.

2. Compiti degli organi apicali, dei dirigenti e dei responsabili
Approvazione delle modalità di attuazione delle misure di gestione del rischio e supervisione della loro implementazione. Ripartizione dei compiti, deleghe e flussi informativi verso la direzione. Documentazione delle decisioni, delle verifiche e delle azioni correttive.

3. L'obbligo di formazione in materia di sicurezza informatica
Formazione degli organi di amministrazione e direttivi ai sensi dell'art. 23 del D.Lgs. 138/2024 e promozione dell'offerta periodica di formazione ai dipendenti. Individuazione dei

destinatari e dei contenuti in funzione dei ruoli. Sensibilizzazione su phishing, ransomware, credenziali compromesse e richieste fraudolente di pagamento.

4. Misure di sicurezza e aggiornamenti ACN
Specifiche e determinazioni ACN applicabili. Gestione degli accessi, autenticazione a più fattori, aggiornamento dei sistemi, copie di sicurezza, continuità operativa e ripristino. Evidenze documentali dell'attuazione delle misure. Decorrenze degli obblighi e adempimenti per il 2027 in relazione all'anno di inserimento nell'elenco NIS.

5. La gestione dell'incidente informatico
Rilevazione dell'evento e segnalazione interna. Valutazione dell'impatto e attivazione delle funzioni competenti. Contenimento, conservazione delle evidenze e ripristino dei servizi. Distinzione tra incidente significativo ai fini NIS e violazione di dati personali ai fini GDPR.

6. Punto di contatto NIS, referente CSIRT e notifiche
Ruoli, designazioni, sostituzioni e organizzazione dei flussi informativi. Pre-notifica, notifica dell'incidente e successive comunicazioni al CSIRT Italia. Termini, contenuti e aggiornamenti delle informazioni. Coordinamento con direzione, personale informatico e fornitori.

7. Coordinamento con il DPO e gestione degli adempimenti privacy
Coinvolgimento tempestivo del DPO nella sua funzione di consulenza e sorveglianza. Raccolta delle informazioni necessarie alle decisioni del titolare del trattamento. Coordinamento tra notifiche NIS, notifica al Garante e comunicazione agli interessati, nel rispetto dei rispettivi presupposti e termini.

8. Caso applicativo: attacco ransomware e possibile sottrazione di dati
Analisi di uno scenario con indisponibilità dei sistemi e possibile accesso illecito ai dati. Individuazione dei soggetti da coinvolgere, delle priorità e delle decisioni da documentare. Valutazione delle notifiche, rapporti con i fornitori e verifica delle misure correttive. Confronto conclusivo sui quesiti dei partecipanti.

DESTINATARI DELL'OFFERTA FORMATIVA

Il corso è rivolto a: Amministratori, componenti degli organi di amministrazione e direttivi, dirigenti e responsabili di pubbliche amministrazioni, società pubbliche e imprese private.
Responsabili della sicurezza informatica, dei sistemi informativi e delle funzioni organizzative coinvolte nella prevenzione e nella gestione degli incidenti. Responsabili della protezione dei dati personali, DPO e consulenti privacy.
Punti di contatto NIS, referenti CSIRT e relativi sostituti. Responsabili delle risorse umane, della formazione, della compliance e dei controlli interni.

Avvocati e professionisti che assistono enti e imprese in materia di cybersicurezza, protezione dei dati e responsabilità.

I DOCENTI

Avv. Gualtiero Roveda

Avvocato cassazionista e giornalista pubblicista, esercita l'avvocatura nel settore del diritto d'impresa e del lavoro. Cura da oltre vent'anni le relazioni industriali per un'Associazione nazionale di categoria ed è il responsabile tecnico della Commissione che stipula il Contratto Collettivo Nazionale di Lavoro per il comparto di riferimento della stessa. È, altresì, componente della Commissione paritetica nazionale istituita dallo stesso contratto.
È il responsabile innanzi alla Direzione Provinciale del Lavoro *ex* art 12, L. 11 gennaio 1979 dell'organizzazione di uffici di gestione degli adempimenti in materia di lavoro.
È stato componente del Comitato Scientifico della Scuola Forense di Forlì-Cesena. Svolge attività di formatore in materia di Sicurezza sul lavoro, Legislazione alimentare, D. Lgs. 231/01 e Privacy.
È Organo di vigilanza *ex* D. Lgs. 231/01 di imprese in ambito privato e pubblico. Ha pubblicato vari testi, tra cui «La fattura commerciale e la gestione del credito» (2003) e il «Manuale operativo del recupero crediti. Profili di diritto civile, processuale, internazionale e fiscale per la gestione le gale ed il recupero del credito» (2008). Di recente ha coordinato un volume in materia di cybersicurezza.
Collabora stabilmente con testate giornalistiche con articoli di carattere giuridico. Ha conseguito le seguenti certificazioni: IDCERT – DIGITAL COMPETENCE: Level specialised; DPO/RPD: Level specialised; IT SECURITY: Level specialised; PRIVACY SPECIALIST: Level specialised.

Avv. Prof. Andrea R. Sirotti Gaudenzi

Avvocato abilitato all'esercizio della professione dinanzi alle Magistrature superiori, è docente universitario e arbitro internazionale. Svolge attività di docenza in Italia e all'estero. Ha patrocinato davanti alla Corte europea dei diritti dell'Uomo e alla Corte di giustizia dell'Unione europea. Responsabile scientifico e formatore accreditato dal Ministero della Giustizia ai sensi del D.M. n. 180/2010 presso vari enti, è presente nell'Albo dei Docenti della Scuola Superiore della Magistratura. Dirige il Master in diritto, arte e nuove tecnologie organizzato da Wolters Kluwer ed è docente nel Master in informatica giuridica presso l'Università La Sapienza di Roma. È stato docente e membro dei comitati ordinatori del Master in *Diritto della Rete* e del Master in *International Litigation* dell'Università di Padova. È titolare degli insegnamenti di *International Criminal Law* e di *Cybercrime* nel corso PhD in Law & Criminology di Ego - Malta. È membro del Comitato scientifico del Dipartimento interuniversitario di criminologia clinica,

vittimologia e psicopatologia forense del Consorzio universitario Humanitas di Roma. Insegna diritto delle esecuzioni in corsi di UniMarconi. Collabora con le testate del gruppo «Il Sole 24 Ore».
Nel 2021 ha coordinato il primo Trattato in lingua italiana sul diritto della rete. Con Renato Borruso e Glauco Riem ha scritto il «Glossario di diritto delle nuove tecnologie e dell'e-government» (Giuffrè, 2007). Ha diretto vari Trattati giuridici, tra cui il «Trattato in materia di proprietà intellettuale e concorrenza» edito da Utet e il «Trattato operativo dei contratti commerciali» edito da Maggioli. Ha diretto il Trattato «La disciplina dell'IA e degli algoritmi avanzati in Italia e in Europa» (Zanichelli, 2026) ed è autore di decine di manuali, tra cui «Proprietà intellettuale e diritto industriale» (Il Sole 24 Ore, II edizione, 2022), «I ricorsi alla Corte europea dei diritti dell'uomo» (VII edizione, Maggioli, 2025), «Il nuovo diritto d'autore» (XIII edizione, Maggioli, 2026). Ha scritto assieme a Vincenzo Franceschelli il volume «La legge italiana sull'intelligenza artificiale» (II edizione, Maggioli, 2026). Coordina varie collane edite da diverse case editrici. Siede nel comitato scientifico di varie riviste scientifiche, tra cui Rivista di Diritto Industriale (Giuffrè), Il Diritto d'Autore (SIAE) e Le Controversie Bancarie (CAB). È responsabile scientifico dell'Istituto nazionale per la formazione continua di Roma.

QUOTA SINGOLA DI PARTECIPAZIONE
ISCRIZIONE AL CORSO ONLINE
EURO 399,00 + IVA (SE DOVUTA)

Il pagamento della quota deve avvenire all'atto di iscrizione per soggetti privati (associazioni, cooperative, fondazioni, enti privati, libero professionista), mediante bonifico bancario utilizzando le seguenti coordinale:

> Conto corrente bancario IBAN: IT74R0899524207000000092212 intestato ad Accademia Europea Formazione S.r.l. c/o Riviera Banca Credito Cooperativo di Rimini e Gradara, filiale di Rimini Città (RN).

Il pagamento della quota di iscrizione per gli enti pubblici avverrà di norma a 30 giorni data fattura (modalità applicabile per Enti Pubblici e Aziende a partecipazione pubblica) che sarà emessa a seguito svolgimento del corso.

Se la fattura è intestata ad Ente Pubblico, la quota è esente IVA, ai sensi dell'art. 10, D.P.R. n. 633/72 (e successive modificazioni). Nelle fatture emesse in esenzione IVA verrà addebitato il costo del bollo virtuale pari a € 2,00.

Non è necessaria l'acquisizione del codice SMART/CIG trattandosi di partecipazione di un dipendente/consigliere ad un seminario o convegno (cfr. Linee Guida tracciabilità dei flussi ANAC).

Società abilitata al Mercato elettronico delle PA – Acquistinretepa.

Il pagamento della quota dovrà essere effettuato entro 30 giorni dalla data delle fattura nel conto dedicato.

Le adesioni si intenderanno perfezionate con la completa compilazione della domanda di iscrizione al webinar (uno o più moduli), cui seguirà la trasmissione del link di collegamento all'evento ed l'emissione della fattura elettronica.

È necessario procedere alla compilazione della domanda di iscrizione per ogni partecipante (in caso di più iscritti appartenenti ad uno stesso ente o azienda occorre indicare un indirizzo e-mail diverso per ogni partecipante).

Il contratto si intenderà concluso e quindi efficace e vincolante tra le parti nel momento in cui il cliente avrà inoltrato telematicamente il modulo di iscrizione seguendo l'apposita procedura online.

Si potrà seguire il webinar in diretta tramite la piattaforma Zoom. I corsi saranno interamente registrati, e resi disponibili per la visione in differita, pertanto la mancata partecipazione al webinar non sarà rimborsata.

Al termine del percorso verrà rilasciato l'attestato individuale di frequenza previo superamento di un test a risposta multipla. **Si precisa che il corso è valido ai fini della Direttiva "Zangrillo" in materia di formazione dei dipendenti pubblici.**

Sarà attivo un servizio di segreteria organizzativa dalle ore 9,00 alle 13,00 al numero 0541/448562 e al cellulare 333/2430327.

MODALITÀ DI PARTECIPAZIONE

PER ISCRIVERSI:
CLICCA QUI

Procedendo all'iscrizione, verrà perfezionata l'adesione al webinar (uno o più moduli) con impegno a procedere al pagamento per l'erogazione della formazione richiesta.

Prima dell'inizio del corso sarà inviata all'indirizzo e-mail indicato il link di collegamento al webinar e si procederà all'emissione della fattura elettronica.