



Resilienza operativa e gestione dei cyber-risks in ambito bancario, finanziario e assicurativo alla luce del Regolamento DORA

Presidi organizzativi contro i cyber risks
Gestione degli incidenti
Rimedi e sanzioni

Giovedì 20 giugno 2024



Evento disponibile in videoconferenza
La qualità degli eventi Paradigma fruibile da qualsiasi luogo, direttamente su PC o tablet

PARADIGMA Srl

Tel. 011.538686
Corso Vittorio Emanuele II, 68 - 10121 Torino

P.IVA 06222110014
www.paradigma.it
info@paradigma.it



Relatore

Prof. Avv. Alessandro del Ninno

Docente di Informatica Giuridica Presso la **LUISS Guido Carli di Roma**.

Docente di Intelligenza Artificiale, Machine Learning e Diritto presso il medesimo Ateneo.

Avvocato esperto di ICT, AI, Data Protection, Partner di **FIVELEX Studio Legale e Tributario**.

Presidente del Comitato Scientifico dell'**Associazione Nazionale per la Protezione dei Dati Personali**.

Membro del Comitato Scientifico dell'**Istituto Italiano Privacy**.

Appointed member del Pool of Experts europei di supporto e consulenza al **Comitato Europeo per la Protezione dei Dati Personali**.

Relatore nell'ambito dei più importanti convegni nazionali e internazionali ove viene frequentemente invitato in qualità di esperto su tematiche legate all'Information & Communication Technology, all'IP e alla Data Protection.

Nelle stesse materie è autore di oltre 150 tra libri, trattati, monografie, saggi e articoli. Per Key Editore è Direttore delle due collane editoriali "GDPR: casi pratici risolti" e "Le Leggi del Decennio Digitale 2020-2030 della UE - I commentari pratici".

Il docente, nel corso dell'evento formativo, risponderà alle **domande** e alle **richieste di chiarimenti** formulate dai partecipanti. Eventuali quesiti potranno essere anticipati inviando una email all'indirizzo info@paradigma.it.

Agevolazioni e formazione finanziata



EARLY BOOKING -20%

Inviando il modulo di iscrizione **entro il 30 maggio 2024** si avrà diritto a una **riduzione del 20%** sulla quota di partecipazione



PROGETTO GIOVANI ECCELLENZE -50%

Iscrivi una seconda risorsa **che non abbia compiuto il 30° anno di età** con una **riduzione del 50%** sulla quota di partecipazione



FORMAZIONE FINANZIATA

Finanzia la tua formazione utilizzando i **Fondi Paritetici Inter-professionali**. Paradigma offre la **completa e gratuita gestione** dei necessari adempimenti



EVENTO ACQUISTABILE SUL MEPA

Paradigma opera sul MePA e sui principali mercati elettronici di soggetti aggregatori e centrali di committenza

Modulo di iscrizione Mod. 3.4 rev. 3

L'iscrizione si perfeziona al momento del ricevimento del presente modulo da inviare via mail all'indirizzo info@paradigma.it integralmente compilato e sottoscritto per accettazione. La Segreteria Organizzativa provvederà a inviare conferma dell'avvenuta iscrizione.



Dati relativi all'evento

Resilienza operativa e gestione dei cyber-risk in ambito bancario, finanziario e assicurativo alla luce del Regolamento DORA

Giovedì 20 giugno 2024

Dati relativi al partecipante

Nome _____ Cognome _____

Azienda/Studio/Ente _____

Funzione aziendale/Professione _____

E mail _____

Telefono _____

Dati per eventuale partecipante under 30

Nome _____ Cognome _____

E mail _____

Dati per la fatturazione elettronica

Intestatario fattura _____

Indirizzo _____

Città _____ CAP _____ Provincia _____

P. Iva/C. F. _____

Codice destinatario o PEC (Privati) _____

Codice univoco uff. (PA) _____

Codice CIG (PA) _____

Split Payment SI NO

OdA _____ Data OdA _____

Altri riferimenti _____

Per informazioni contattare

Referente _____

Telefono _____

E mail _____

Data e Firma

Ai sensi dell'art. 1341 c.c. si approvano espressamente le condizioni di partecipazione riportate sul sito www.paradigma.it con particolare riferimento alle modalità di disdetta e alle variazioni di programma.

Data e Firma

Informativa Privacy
I dati forniti a **Paradigma Srl** sono raccolti e trattati, con modalità anche informatiche, esclusivamente per evadere la Sua richiesta di partecipazione all'intervento formativo e svolgere le attività a ciò connesse. I dati potranno essere trattati, per conto di **Paradigma Srl**, da dipendenti e collaboratori incaricati di svolgere specifici servizi necessari all'esecuzione delle Sue richieste. Il conferimento dei suoi dati, pur essendo facoltativo, si rende necessario per l'esecuzione del servizio richiesto.

Solo in caso di Sua autorizzazione i dati saranno inoltre conservati e trattati da **Paradigma Srl** per effettuare l'invio di materiale informativo relativo a prossime iniziative di **Paradigma Srl**. Lei potrà esercitare i diritti sanciti agli artt. 15 - 22 del Regolamento (UE) 2016/679 inviando una richiesta scritta a **Paradigma Srl** con sede in Torino, C.so Vittorio Emanuele II, 68, tel. 011.538686. Letta l'informativa, acconsente all'utilizzo dei dati inseriti nel presente modulo per l'invio del materiale informativo?

SI NO

Data e Firma

Programma dei lavori

Giovedì 20 giugno 2024

I PRESIDI OBBLIGATORI DI SICUREZZA INFORMATICA E CIBERNETICA PREVISTI DAL REGOLAMENTO DORA E DA ALTRE NORMATIVE PERTINENTI

Il Digital Operational Resilience Act (DORA) quale normativa settoriale di riferimento per la cybersicurezza nel settore bancario, finanziario e assicurativo

Il DORA quale parte del c.d. "Cyber-security & Cyber-resilience Package della UE"
Ragioni giustificanti l'adozione di una regolamentazione specifica in materia di cybersicurezza e resilienza informatica
Destinatari degli obblighi previsti dal DORA e soggetti esclusi
Le tempistiche previste per l'adeguamento
Ulteriori normative da considerare nel definire strategie e processi interni per la gestione dei rischi informatici e della resilienza operativa digitale
I concetti fondamentali alla base del DORA

I livelli di responsabilità aziendale coinvolti nell'applicazione del DORA e la definizione di assetti di governance adeguati

L'obbligo di adottare assetti di governance e organizzativi idonei a realizzare un controllo efficace dei rischi ICT
Il principio della "piena e principale responsabilità dell'organo di gestione per la gestione dei rischi informatici dell'entità finanziaria, bancaria o assicurativa"
I compiti e le responsabilità operative dell'organo di gestione nell'attuazione degli obblighi del Regolamento DORA

L'obbligo di dotarsi di un "quadro per la gestione dei rischi informatici"

In cosa consiste il "quadro per la gestione dei rischi informatici" previsto dal Regolamento DORA e quali adempimenti organizzativi, tecnici e pratici esso comporta
Gli standard tecnici o documentali cui poter fare riferimento nello strutturare le politiche e delle strategie di cui al "quadro di gestione dei rischi informatici"
L'esternalizzazione del controllo di conformità del quadro di gestione dei rischi informatici

Gli incidenti rilevanti ai fini del DORA e gli adeguamenti richiesti

Individuazione degli incidenti informatici rientranti nel campo di applicazione del Regolamento DORA
La messa a punto di procedure e processi di prevenzione, monitoraggio e gestione degli incidenti, nonché di un efficiente sistema di notifica degli stessi alle Autorità competenti
Il processo di classificazione degli incidenti occorsi connessi alle TIC: indicazioni operative
Distinzione tra incidenti e minacce informatiche
Sussiste un obbligo di classificare anche le minacce informatiche?
Le prescrizioni del DORA rispetto agli obblighi di segnalazione alle Autorità competenti di incidenti e minacce informatiche
Informazioni alla clientela circa gli incidenti e le minacce informatiche: sono dovute?

L'attività di testing obbligatoria

L'obbligo di istituire e condurre test di resilienza operativa digitale
Le caratteristiche dei test avanzati di tipo TLPT (Threat-Led Penetration Testing)
Entità bancarie, finanziarie e assicurative tenute a condurre i test avanzati di tipo TLPT
La periodicità prevista per i test TLPT
I soggetti che concretamente svolgono i test TLPT

I rischi informatici derivanti da terzi e la relativa gestione

Nozione di rischi informatici derivanti da terzi
La messa a punto e l'attuazione di una strategia per fronteggiare i rischi informatici derivanti da terzi
L'impatto degli obblighi concernenti i rischi informatici derivanti da terzi sui processi di selezione dei fornitori ICT e sulle attività precontrattuali
Le cautele da adottare in sede di redazione e stipula dei contratti di fornitura dei servizi TIC
Le peculiarità caratterizzanti i contratti di fornitura dei servizi TIC a supporto delle funzioni essenziali o importarti e gli specifici obblighi di cooperazione per i fornitori coinvolti in tali contratti
I "piani di uscita" da prevedere specificatamente nei contratti di fornitura dei servizi TIC a supporto delle funzioni essenziali o importarti
Gli obblighi documentali relativi ai contratti per servizi TIC
Gli obblighi di comunicazione alle Autorità competenti che le entità bancarie, finanziarie e assicurative devono osservare ai fini di consentire la sorveglianza sui contratti stipulati per servizi TIC con i fornitori terzi
Individuazione della categoria dei "fornitori terzi critici di servizi TIC" e regole apposite previste dal Regolamento DORA

Valutazione di ulteriori impatti sui procedimenti e le strutture dei soggetti tenuti all'applicazione del DORA

Il Regolamento DORA istituisce nuovi registri/inventari specifici da redigere, mantenere e aggiornare da parte delle entità bancarie, finanziarie e assicurative?
Il Regolamento DORA istituisce nuovi ruoli specifici e/o assegna compiti specifici a funzioni esistenti nell'ambito degli organigrammi delle entità bancarie, finanziarie e assicurative?
È obbligatorio per le entità bancarie, finanziarie e assicurative organizzare e svolgere iniziative di formazione e sensibilizzazione sulla resilienza operativa digitale, i rischi informatici e sull'impianto complessivo del Regolamento DORA?

L'apparato sanzionatorio

Sanzioni civili e misure di riparazione
Sanzioni penali

I presidi di riservatezza delle informazioni scambiate ai sensi del DORA

Il segreto professionale previsto dall'art. 55
Ambito soggettivo e oggettivo del segreto

Le Autorità Europee di Vigilanza (AEV) investite di poteri regolatori, di vigilanza e sanzionatori in ordine all'applicazione del DORA

La messa a punto delle norme tecniche di regolamentazione comuni: roadmap dei termini previsti
Individuazione e compiti dell'Autorità di sorveglianza capofila

Rapporto tra Regolamento DORA e misure di gestione dei rischi informatici e risk control previsti per le banche dalla Circolare della Banca d'Italia n. 285 del 17 Dicembre 2013

Note organizzative e condizioni

Data dell'evento

Giovedì 20 giugno 2024

Orario dei lavori

Accesso alla piattaforma alle 09.00 - 9.30
9.30 – 13.30 14.30 – 17.30

Quota di partecipazione

€ 1.100 + Iva
(Early booking): € 880 + Iva

Quota di partecipazione in videoconferenza

La quota di partecipazione in aula virtuale (diretta streaming) include l'invio del materiale didattico in formato elettronico e la possibilità di sottoporre ai relatori quesiti di specifico interesse. E altresì possibile anticipare domande e richieste di approfondimento inviando una email a info@paradigma.it entro il giorno antecedente l'evento. In caso di **videoconferenza con accessi multipli** è necessario contattare la Segreteria organizzativa per un preventivo personalizzato.

Modalità di funzionamento della videoconferenza

È possibile accedere all'aula virtuale da qualsiasi luogo, utilizzando il proprio PC o tablet con una connessione a Internet. La piattaforma informatica utilizzata da Paradigma (Adobe Connect) non necessita di requisiti tecnici particolari. Nei giorni antecedenti l'evento il partecipante riceverà per posta elettronica le credenziali e le istruzioni di accesso. Il giorno dell'evento sarà sufficiente selezionare il link che troverà nella mail e inserire le credenziali per accedere all'aula virtuale. Durante gli interventi, oltre a vedere e sentire i docenti, è possibile consultare simultaneamente la documentazione predisposta dal relatore. Ogni utente collegato potrà porre domande sulle tematiche affrontate, alle quali il docente risponderà nel corso dell'intervento.

Modalità di iscrizione

L'iscrizione si perfeziona al momento del ricevimento del modulo di registrazione, da inviare via email all'indirizzo info@paradigma.it, integralmente compilato. Il numero dei collegamenti disponibili è limitato e la priorità d'iscrizione è determinata dalla data di ricezione del modulo di registrazione. Si consiglia pertanto di effettuare una preiscrizione telefonica.

Modalità di pagamento

La quota di partecipazione deve essere versata all'atto della presentazione della richiesta di iscrizione e, in ogni caso, prima dell'effettuazione dell'intervento formativo, tramite bonifico bancario intestato a:
Paradigma Srl - Corso Vittorio Emanuele II, 68 - 10121 Torino
c/o Banco BPM Spa
IBAN IT 14 V 05034 01017 000000002530

Formazione finanziata

La quota di partecipazione può essere completamente rimborsata tramite voucher promossi dai Fondi Paritetici Interprofessionali. Paradigma offre la completa e gratuita gestione delle spese di progettazione, monitoraggio e rendicontazione. La possibilità di accedere alla formazione finanziata con partecipazione mediante videoconferenza può variare a seconda dell'Ente erogante.

Attestato di frequenza

L'attestato di partecipazione nominativo sarà rilasciato al termine dell'intervento formativo ai partecipanti che hanno regolarmente preso parte ai lavori.

Diritto di recesso e modalità di disdetta

È attribuita ai partecipanti la facoltà di recedere ai sensi dell'art. 1373 c.c. Il recesso dovrà essere comunicato in forma scritta almeno sette giorni prima della data di inizio dell'evento formativo (escluso il sabato e la domenica). Qualora la disdetta pervenga oltre tale termine o si verifichi di fatto con il mancato collegamento alla videoconferenza, la quota di partecipazione sarà addebitata per intero e sarà inviato al partecipante il materiale didattico. In qualunque momento l'azienda o lo studio potranno comunque sostituire il partecipante, comunicando il nuovo nominativo alla nostra Segreteria organizzativa.

Variazioni di programma

Paradigma, per ragioni eccezionali e imprevedibili, si riserva di annullare o modificare la data dell'evento formativo, dandone comunicazione agli interessati entro tre giorni dalla data di inizio prevista. In tali casi le quote di partecipazione pervenute verranno rimborsate, con esclusione di qualsivoglia onere o obbligo a carico di Paradigma. Paradigma si riserva inoltre, per ragioni sopravvenute e per cause di forza maggiore, di modificare l'articolazione del programma e di sostituire i docenti previsti con altri docenti di pari livello professionale. Per ulteriori informazioni è possibile contattare la Segreteria organizzativa al numero 011.538686 o all'indirizzo email info@paradigma.it