

IL REGOLAMENTO "DORA" DAL PUNTO DI VISTA DEI FORNITORI ICT

(corso dedicato ai fornitori ICT diretti o appartenenti alla catena di fornitura ICT, a qualunque livello, di banche e altre entità finanziarie)

1

20 e 29 novembre 2024

Contesto

Il Regolamento DORA (Digital Operational Resilience Act) impone alle entità finanziarie l'obbligo di garantire la resilienza operativa digitale non solo all'interno delle proprie strutture, ma anche **lungo l'intera catena di fornitura ICT**. Questo significa che le **AZIENDE ICT**, anche quelle che non annoverano tra i propri clienti entità finanziarie, potrebbero essere chiamate a adeguarsi agli stringenti requisiti del Regolamento. In particolare, DORA richiede che le misure di sicurezza informatica, la gestione dei rischi e la continuità operativa vengano implementate lungo tutta la filiera di fornitura. Pertanto, un'azienda ICT potrebbe dover adottare le misure previste da DORA qualora sia parte della catena di fornitura di un cliente che, a sua volta, opera in ambito finanziario.

Nel caso in cui l'azienda non accetti di conformarsi a tali requisiti, il cliente potrebbe essere obbligato a terminare il contratto con il fornitore, per evitare di incorrere in sanzioni o violazioni del regolamento. Questo rende l'adesione ai requisiti DORA un fattore critico per mantenere i rapporti commerciali con le entità finanziarie o con i loro fornitori diretti.

Una delle novità più rilevanti del regolamento è la possibilità, conferita alle entità finanziarie, di condurre ispezioni e audit direttamente sui fornitori ICT, anche in assenza di un rapporto contrattuale diretto. Questo implica che un'azienda ICT, pur non avendo un legame diretto con un'entità finanziaria, possa essere soggetta a verifiche da parte di queste ultime, qualora faccia parte della loro catena di fornitura.

Obiettivi

Per offrire un quadro chiaro sui requisiti e le opportunità che DORA rappresenta per le aziende del settore ICT, INFORMA Istituto Nazionale di Formazione propone due corsi dedicati (modalità a distanza tramite "microsoft teams") ognuno della durata di 4 ore. Il programma è focalizzato sugli obblighi normativi, le best practice di adeguamento, gli aspetti contrattuali ed i vantaggi competitivi che possono derivare dall'adeguamento al regolamento DORA.

I corsi sono pensati per fornire alle aziende ICT tutte le informazioni necessarie per affrontare con successo questa nuova sfida normativa, le relative opportunità commerciali e per garantire la continuità dei rapporti con i clienti del settore finanziario.

- Corso 1: **"DORA dal punto di vista dei fornitori ICT: gli adempimenti"**
- Corso 2: **"DORA dal punto di vista dei fornitori ICT: gli aspetti contrattuali"**

[PROGRAMMA DEL PRIMO CORSO]

IL REGOLAMENTO "DORA" DAL PUNTO DI VISTA DEI FORNITORI ICT:

GLI ADEMPIMENTI

2

20 novembre 2024

Ore 8.45 collegamento – ore 9.00 apertura dei lavori

Regolamento DORA, RTS, ITS, Regolamenti delegati e loro impatto su FORNITORI e OUTSOURCER

- Il perimetro normativo in ambito di fornitura ed outsourcer
- Il Regolamento DORA, RTS, ITS, Regolamenti delegati in materia di rischi di terze parti
- Il perimetro di applicazione di DORA

Il punto di vista delle Entità Finanziarie

- Verifiche preliminari
- Aspetti contrattuali
- Monitoraggio e audit

Il punto di vista dei fornitori ICT

- Vincoli ed obblighi
- Opportunità commerciali

Approfondimenti

- Exit strategy ed exit plan
- Strumenti per la valutazione dei fornitori

I fornitori critici

- Criteri di individuazione
- Il quadro di sorveglianza
- Adempimenti e sanzioni

Il cloud

- Peculiarità dell'ambiente cloud
- Checklist di valutazione e qualificazione di ambienti cloud
- Marketplace
- Certificazione del personale per verifiche in ambito cloud

Ore 13.00 chiusura dei lavori

[PROGRAMMA DEL SECONDO CORSO]

IL REGOLAMENTO "DORA" DAL PUNTO DI VISTA DEI FORNITORI ICT: GLI ASPETTI CONTRATTUALI

3

29 novembre 2024

Ore 8.45 collegamento – ore 9.00 apertura dei lavori

La valutazione preliminare dei fornitori

Certificazioni ed audit di terze parti quale strumento di valutazione

Le informazioni da fornire alle entità finanziarie

La tecnica legislativa

- Il coordinamento tra le fonti
- Espressione dei contenuti degli obblighi degli Enti Finanziari
- Generalità delle norme
- Possibili declinazioni contrattuali

Centralità del contratto

- Gli obblighi espliciti di normazione interna (policy / procedure)
- Gli obblighi espliciti di normazione esterna (con fornitori TIC)
- Il coordinamento: conseguenze sulle clausole contrattuali
- Gli obblighi contrattuali attesi
- Le clausole contrattuali a tutela del fornitore TIC

Le opportunità commerciali offerte da DORA

- I nuovi adempimenti contrattuali
- I nuovi servizi richiesti da DORA

Ore 13.00 chiusura dei lavori

RELATORI:

Giancarlo BUTTI

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Membro del Comitato Scientifico del CLUSIT (referente ESG ed Inclusion). Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore con oltre 170 corsi, seminari e master universitari presso ISACA, CLUSIT, ITER, CETIF, IKN, AIIA, UNIVERSITA DI MILANO, POLITECNICO DI MILANO, UNIVERSITÀ DEGLI STUDI SUOR ORSOLA BENINCASA NAPOLI, UNIVERSITA' CA FOSCARI VENEZIA, CEFRIEL, UNISEF,... Ha all'attivo oltre 800 articoli e collaborazioni con oltre 30 testate, 26 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha inoltre partecipato alla redazione di 28 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT... Socio e già proboviro di ISACA/AIEA è socio del CLUSIT, di DFA (Digital Forensics Alumni) e del BCI (Business Continuity Institute), partecipa a numerosi gruppi di lavoro. Ha inoltre acquisito le certificazioni/qualificazioni: (LA BS 7799), (LA ISO IEC 27001:2005/2013/2022), (LA ISO IEC 42001:2023), CRISC, CDPSE, ISM, DPO, DPO UNI 11697:2017, CBCI, AMBCI

Maria Roberta PERUGINI

Avvocato, si occupa sin dal 1995 di protezione dei dati personali e data governance – compresi gli aspetti tecnici e organizzativi – e svolge attività di consulenza alle imprese fornendo un supporto completo dei connessi profili contrattuali e in generale civilistici, e assistenza nei contenziosi. Svolge la funzione di DPO. Membro del Support Pool of Experts dello European Data Protection Board (EDPB) con riferimento ai settori "Technical expertise in new technologies and information security" e "Legal expertise in new technologies". Relatrice e docente a convegni, master e corsi di specializzazione in materia di protezione dei dati personali e data governance di numerosi enti, associazioni, Università e istituzioni private e pubbliche. Socia CLUSIT, contribuisce alla Clusit Community for Security. Autrice di monografie e articoli su problematiche attuali di governance dei dati su riviste divulgative e scientifiche e attraverso il blog istituzionale www.mrperugini.it. E' co-fondatrice di IUSINTECH, team di professioniste con specializzazioni multidisciplinari nel campo dell'innovazione, trasformazione digitale e sviluppo tecnologico.

Quote di partecipazione (comprensiva di materiale didattico su formato elettronico):

Corso 1: **"DORA dal punto di vista dei fornitori ICT: gli adempimenti"** 20/11/2024

- Euro 300 + 22% Iva a partecipante

Corso 2: **"DORA dal punto di vista dei fornitori ICT: gli aspetti contrattuali"** 29/11/2024

- Euro 300 + 22% Iva a partecipante

Corso 1 + Corso 2: Euro 500 + 22% Iva a partecipante

Per iscrizioni e ulteriori informazioni Tel. 02.36577120; e-mail: informa@informabanca.it