Luxembourg Newsflash - 16 January 2023

DORA in force from 16 January 2023 – check your digital operational resilience readiness

DORA enters into force on 16 January 2023. Given the ever-increasing risk of cyberattacks, the EU has decided to strengthen the requirements surrounding the IT security of financial entities.

The Digital Operational Resilience Act ("**DORA**") is part of the Digital finance package adopted in 2020 by the EU Commission to further enable and support the potential of digital finance in terms of innovation and competition, while mitigating the risks arising from it.

DORA enters into force on 16 January 2023. The designated European Supervisory Authorities are currently developing technical standards with which financial entities must comply, whilst national competent authorities will oversee compliance and enforce the regime as required. The new rules will apply from 17 January 2025.

Broad scope of application

To ensure consistency concerning the ICT risk management requirements applicable to the financial sector, DORA applies to a range of financial entities regulated at EU level. This includes most credit institutions, payment institutions, electronic money institutions, investment firms, most managers of alternative investment funds and management companies, as well as most insurance and reinsurance undertakings and intermediaries. Specific provisions are anticipated for microenterprises, which are also within scope of DORA.

DORA also applies to ICT third-party service providers providing digital and data services, including providers of cloud computing services, software, data analytics services and data centres.

Main requirements

Governance and ICT Risk Management

For affected companies, DORA significantly expands existing requirements relating to ICT risk management with the obligation to ensure effective and prudent management of all ICT risks, based on the management body's accountability and final responsibility for managing the company's ICT risks. Companies are required to use, document in writing, and maintain, the appropriate systems, protocols and tools needed to provide sufficient reliability, capacity and resilience.

ICT-related incident management, classification and reporting

In particular, financial entities must comply with requirements for an ICT-related incident management process which enables monitoring and logging of ICT-related incidents, followed by an obligation to classify them based on specific criteria. When ICT-related incidents are deemed major, they must be reported to the national competent authorities and, when relevant, to the client, following a harmonised procedure.

Digital operational resilience testing

Financial entities must also establish and maintain a sound and comprehensive digital operational resilience testing programme in order to assess their preparedness for handling ICT-related incidents, identifying weaknesses, deficiencies and gaps in digital operational resilience, and promptly implementing corrective measures.

ICT third-party risk management

The management of ICT third-party risk is considered a full component of ICT risk. The ICT third-party risk and ICT third-party risk strategy must be documented and regularly reviewed. For technically complex ICT services, internal and external auditors must possess appropriate skills and knowledge. In addition, the contracts that govern the relationship between ICT service providers and financial entities will need to contain certain new, specific contractual provisions.

DORA also introduces an oversight framework for critical ICT third-party providers, to be designated by the European Supervisory Authorities. Any such providers which are located in third countries and provide critical services, will be required to establish a subsidiary within the EU to be used by financial entities. This is so that oversight can be properly implemented.

How to prepare

Given the wide range of operational resilience topics covered by DORA, it is strongly recommended that companies start assessing now the impact of DORA on their operations and their contractual arrangements for use of ICT services, by conducting a thorough gap analysis provision by provision. Using this gap analysis, companies should be able to organise themselves to best prepare for the entry into application of DORA in January 2025.

How can we help?

Contact our experts **Bénédicte d'Allard**, **Astrid Wagner** and **Marc Mouton** for further assistance in understanding how DORA could potentially impact your activities.

your contacts

BENEDICTE D'ALLARD
Senior Manager
Regulatory Consulting

Learn more_

ASTRID WAGNER
Partner
IP, Communication & Technology

Learn more_

MARC MOUTON
Partner
Banking & Financial Services

Learn more_

Arendt & Medernach SA
Registered with the Luxembourg Bar
RCS Luxembourg B 186371

arendt.com

41A avenue JF Kennedy
L-2082 Luxembourg
T +352 40 78 78 1