

# Digital Operational Resilience Act

*Concerns and necessary measures for compliance with the EU-wide cybersecurity regulation for the financial sector*

The Digital Operational Resilience Act (DORA) establishes a uniform European legal framework for cybersecurity requirements in the financial sector. The aim is to ensure the operational resilience of financial companies. The DORA has already entered into force and will apply from 17 January 2025.

## Who is affected?

The DORA is primarily aimed at financial companies from over 20 different industries, including credit institutions, payment and account information service providers, investment firms, insurance and reinsurance companies, and institutions for occupational retirement provision. ICT third-party service providers that support financial companies with ICT services are additionally covered.

## What needs to be implemented?

The requirements of the DORA can be divided into four main areas. The first area concerns ICT risk management. Financial firms need to establish an internal governance and control framework to effectively identify and respond to ICT risks. The responsibility for monitoring and implementation lies with the company's management. The second area covers the treatment and reporting of ICT-related incidents. Companies are required to implement incident management, which includes monitoring, root cause identification, classification and documentation of ICT-related incidents. The third area concerns resilience testing. ICT resilience must be ensured regularly through comprehensive testing procedures such as vulnerability assessments, penetration tests and network security assessments. Finally, the

fourth area regulates the management of third-party risks. Even in the case of outsourcing to ICT third-party service providers, the responsibility remains with the concerned company. Risk analyses must be carried out, an information register must be maintained and contractual agreements with specified minimum content must be concluded. For small companies, there are some exceptions and facilitations in the implementation of individual requirements.

## What are the consequences of violations?

Supervisory authorities such as BaFin or the ECB can impose penalty payments, issue instructions and make violations public. Criminal sanctions are also possible.

## Our support

We support you in implementing the requirements of the DORA with the following services, among others:

- Legal review of the impact on your company
- Derivation of the concrete requirements for your company
- Legal support for implementation and documentation
- Introduction of cybersecurity compliance management

## Next step: Contact us

We would be happy to explain our detailed approach to you in a personal meeting. Contact us now without obligation!

**T** +49 30 / 2332 895 0

**E** [info@reuschlaw.de](mailto:info@reuschlaw.de)