Legal Flash

January, 2025

Regulation DORA (Regulation (EU) 2022/2554): Establishing an enhanced framework for Digital Operational Resilience in the EU.

Regulation DORA (Digital Operational Resilience Act) is a modern legislative framework of the European Union aimed at strengthening the digital resilience of financial institutions, considering the increasing challenges in the digital sector and the urgent need to protect banks from cyberattacks.

This Regulation is part of the broader strategy of European digital reform, with the goal of ensuring the uninterrupted operation of digital systems, even in cases of significant disruptions. Despite the enactment of Regulation DORA in January 2023, its implementation commenced on January 17, 2025.

Scope of the Regulation	The Regulation aims to: • Enhance the cybersecurity of financial institutions by imposing stringent rules on the resilience of their systems and the management of risks related to Information and Communication Technology (ICT). • Establish a unified framework that will be applied across all member states of the European Union, reducing complexity in risk management through common requirements and obligations. • Protect consumers and the market from financial losses and disruptions that may arise from cyberattacks or technical malfunctions.
Businesses to which the Regulation applies	The DORA Regulation applies to: • Financial institutions, such as large banks and multinational insurance companies, as well as small and medium-sized enterprises in the financial sector.

	• Third-party IT service providers, such as multinational cloud service providers and small and medium-sized software providers. • Startups and fintech companies, regardless of size. • Third-party providers of financial market infrastructures, such as investment firms and providers of cryptographic asset services.
Basic obligations introduced by the DORA Regulation	The DORA Regulation establishes specific obligations for the involved entities to enhance their operational resilience. These include: **Supervision and Management of Digital Risks** • Development of a comprehensive ICT risk management framework. • Implementation of rapid response mechanisms to cyber-attack incidents. • Regular risk assessments. **Incident Recording and Reporting Obligations** • Reporting of cybersecurity incidents within strict timeframes. • Details on the nature of the incident, its impacts, and the mitigation measures taken. **Conducting Digital Operational Resilience Testing** • Rules for the continuous operation of critical infrastructures. • Regular resilience checks and alternative plans for data and operations recovery. **Supervision of Third-Party Providers** • Compliance checks of third-party service providers with DORA requirements. • Contracts only with providers that meet security and resilience standards.

Information exchange provisions	Financial entities have the capability to exchange data and information regarding cyber threats among themselves, with the aim of enhancing their digital operational resilience. This exchange takes place within trusted communities and ensures the protection of business confidentiality and personal data, while simultaneously respecting competition policy rules.
Financial penalties for non-compliance	Supervisory authorities may impose sanctions in the event of violations: • **For financial enterprises**: Fines of up to 2% of annual global revenues. • **For individual executive officers:** Fines of up to 1 million euros. • **For technology service providers:** Fines of up to 1% of the average daily global revenues of the previous financial year. • **Continuous fines for enterprises**: Daily fines for a period of up to 6 months until compliance is achieved. • **For critical third-party ICT providers**: Fines of up to 5 million euros. • **For individual executives of critical third-party providers:** Fines of up to 500,000 euros

Let's talk

For a more detailed discussion of the issues regulated by the DORA Regulation, please contact:

Sophia Grigoriadou
Partner | Legal Services & Legal Specialties
+306936644900
sophia.grigoriadou@pwc.com

Kalliopi Vlachopoulou
Senior Manager | Legal Services & Legal Specialties
+306948757337
kalliopi.vlachopoulou@pwc.com