MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

M
L

LEGAL ALERT

NEW RULES FOR DIGITAL OPERATIONAL RESILIENCE IN THE FINANCIAL SECTOR

DIGITAL OPERATIONAL RESILIENCE ACT – REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, OF 14 DECEMBER 2022

On January 16th, 2023, the Digital Operational Resilience Act – Regulation (EU) 2022/2554 of the European Parliament and of the Council, of 14 December 2022, published in the Official Journal of the European Union on December 27th, 2022 ("DORA Regulation") – came into force.

Nowadays, the risk associated with cyberattacks and data breaches knows no quantifiable limits and can have unpredictable and irreparable reputational, and other, consequences. This is true for companies operating across the financial sector, whether they are traditional incumbents (*e.g.*, banks), fintechs or technology service providers.

The DORA Regulation establishes uniform requirements and rules, regarding the security of network and information systems supporting the operational processes of financial entities, related to information and communications technology ("ICT") matters, in order to achieve a higher level of security in cyberspace, in particular digital operational resilience in the financial sector.
The regulation will be directly applicable as of January 17th, 2025, date on which the entities subject to it will have to ensure compliance with the regulatory obligations regarding digital operational resilience.

Thus, one of the major projects to be developed by financial entities and technology suppliers to the financial sector will be the reformulation of the entire governance model of technological areas and security systems and technological risk management.

Purpose of the DORA Regulation

With the aim of harmonizing the rules around operational resilience and cybersecurity regulation in the European Union (EU), the DORA Regulation sets uniform requirements for the security of network and information systems of companies operating in the financial sector, as well as third parties providing critical ICT related services.

The DORA Regulation creates a regulatory framework on digital operational resilience through which all entities need to assure that they can **withstand, respond to, and recover from all types of ICT-related disruptions** (ICT is defined broadly to include digital and data services delivered through ICT systems to one or more internal systems or external users on a continuous basis).

Scope – who is covered?

Financial Entities, such as:

- Credit Institutions;
- Payment Institutions;
- Electronic Money Institutions;
- Investment Companies;
- Management Companies of Undertakings for Collective Investment in Transferable Securities and Alternative Investment Undertakings;
- Insurance and reinsurance companies and insurance intermediaries;
- Crowdfunding service providers;
- VASP – Virtual Asset Service Providers/CASP – Crypto Asset Service Provider and issuers of asset-backed tokens (stablecoins), authorized under the MiCA Regulation.

Technology companies, providing ICT services to Financial Entities.

The application of the rules set out in the diploma should take into account the size and risk profile of each entity covered, particularly in relation to its nature, scale and complexity of services, activities and operations.

Main Obligations – Financial Entities

The obligations applicable to Financial Entities are divided into the following:

Governance
Financial Entities must implement a governance and internal control framework to quickly detect, mitigate and respond to ICT related risks in order to comply with the provisions of the DORA Regulation.

Risk Management

The management board of the Financial Entity should be responsible for defining, approving, and overseeing and be continuously responsible for managing ICT risk within the entity's overall risk management framework.

To this extent, we list the main duties and obligations that arise from this:

- Members of the management board should develop and maintain knowledge regarding ICT risks;
- Implementation of an internationally recognized information security management system;
- Maintenance of risk management programs and assessments;
- Identifying the entity's tolerance for ICT risk and maintaining a comprehensive framework for managing that risk;
- Constant monitoring and control of security, systems operation, and ICT tools.

Incident Reporting

The DORA Regulation aims to institute an incident reporting mechanism, including a management process for detecting, managing and reporting ICT-related incidents.

Incidents considered "serious" must be reported to the competent authorities within strict time limits.

Resilience tests

As part of the ICT risk management framework, the law requires Financial Entities to adopt a robust testing system that covers ICT tools, systems and processes.

The critical tools, systems, and processes must be tested annually, with certain entities required to perform "penetration tests" every three years.

Information Sharing

The DORA Regulation contains provisions facilitating the sharing, between Financial Entities, of information regarding cyber threats, including indicators of compromise, tactics, techniques and procedures, cybersecurity alerts, *inter alia*, in order to strengthen their digital operational resilience, provided it is done in compliance with applicable law (*e.g.*, data protection, competition law).

Risks and Contractual Obligations –Technology Companies

Within the scope of risk concerning Technology Companies, the most relevant matters in the DORA Regulation concern procurement and outsourcing.

The law regulates, specifically and among other things, the requirements for the termination of contracts and the imposition of several mandatory contractual provisions that must be included in contracts with ICT service providers.

Where critical ICT services are concerned, the contractual impositions and duties of the service provider are more demanding, of which we highlight:

- The definition of quantitative and qualitative performance targets for the agreed service levels;
- The adoption of corrective measures;

- The execution and testing of operational contingency plans;
- The obligation to notify Financial Entities regarding services that may have a material impact on their activities;
- The security measures, tools and policies in the ICT domain that ensure security in service delivery;
- The monitoring permission to its activity and facilities by the Financial Entities;
- The definition of exit strategies and their transition to another service provider.

Moving Forward...

Although the Regulation will only be applicable in two years, we expect it to be a disruption to the current landscape, as it **imposes new obligations**, in addition to absorbing some of the rules already contained in the EBA Guidelines on outsourcing (among other similar guidelines, such as those of ESMA), thus **being important to anticipate changes in a timely manner**.

David Silva Ramalho [+info]
Nicole Fortunato [+info]
Ashick Remetula [+info]