PLMJ

JAN. 25

INFORMATIVE NOTE

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

The DORA Regulation – final countdown: contracting third parties

The DORA Regulation

As of 17 January 2025, Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 *on digital operational resilience for the financial sector* ("**DORA Regulation**") will apply as a special law which, in cases of conflict, overrides Directive (EU) 2022/2555 of 14 December 2022 *on measures for a high common level of cybersecurity across the Union*. Entities covered by this Directive will continue to be subject to the resulting obligations.

This law covers a wide range of financial institutions[1] operating in the European Union (e.g. credit institutions, payment institutions, electronic money institutions) as well as third party ICT[2] service providers (e.g. cloud service providers). It has been in force since 16 January 2023 and is now mandatory.

The DORA Regulation aims to harmonise security rules and digital operational resilience in the financial sector. It is a response to the growing reliance on digital solutions, which, while improving efficiency and innovation, also increase vulnerability to risks such as cyber-attacks or technical failures. To address these threats, the Regulation lays down common security rules for financial institutions operating in the European Union. It takes into account the impact that a single attack could have on the Union's financial system and its stability, given the interconnectedness of information systems, and the urgency of establishing a common framework to combat these risks[3].

The Regulation aims to harmonise security rules and digital operational resilience in the financial sector. It is a response to the growing reliance on digital solutions.

Pedro Lomba
Marta Salgado Areias
Technology, Media and Telecommunications team

1 Article 2.

2 Article 3(21) provides that "ICT services" are "digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services".

3 As highlighted by the European Systemic Risk Board ("ESRB"), in its February 2020 document on "Systemic Cyber Risk", which identified vulnerabilities in the financial system related to digitalisation and cyber risks.

The Regulation requires the implementation of rigorous management mechanisms. These include third party assessments, ongoing monitoring and the definition of exit strategies to ensure business continuity.

To this end, it provides for applicable requirements in the field of ICT risk management, incident reporting, data and information sharing, digital operational resilience testing, third party ICT-related risk management measures and cooperation with public authorities. It also sets out requirements for contractual arrangements with ICT service providers and the establishment and implementation of the oversight framework for these third parties.

Managing of ICT third-party risk

Specifically, with regard to third party outsourcing and related risk management - one of the pillars of the DORA Regulation - financial organisations need to integrate third party ICT risk into their ICT management framework. In doing so, they must apply the principle of proportionality and take into account the nature, size, complexity and relevance of the dependencies created by the services in question. The risks associated with contracts with service providers are managed taking into account the criticality or importance of the service, process or function and the potential impact on the continuity and availability of financial activities, both individually and as a group.

To mitigate these risks, the Regulation requires the implementation of rigorous management mechanisms. These include third party assessments, ongoing monitoring and the definition of exit strategies to ensure business continuity. They also include the definition of contractual provisions to be included in contracts to be signed with third party ICT service providers.

Contractual provisions and ongoing monitoring

There is also a requirement to maintain an up-to-date register of all contractual arrangements for ICT services, identifying those involving critical or important functions. This register must be made available to the competent authorities upon request. Financial institutions must report annually to the competent authorities on the number of new agreements, including the number of contracts concluded, the categories of third parties involved, the types of agreements and services provided, and the functions covered. In addition to this obligation, financial entities must inform the competent authorities of their intention to enter into a contract for ICT services supporting critical or important functions, as well as when a function becomes critical or important.

Before entering into a contractual arrangement for the use of ICT services, financial entities must assess whether the service supports critical or important functions, review the prudential conditions for subcontracting, identify and assess relevant risks, including ICT concentration risk, conduct due diligence on potential providers to ensure their suitability, and analyse potential conflicts of interest arising from the arrangement.

PL
MJ

ICT concentration risk refers to excessive reliance on a limited number of providers due to the vulnerability of financial institutions in the event of failure, interruption or difficulties of these providers, which could jeopardise the continuity and resilience of their critical operations. According to the Regulation, the assessment of ICT concentration risk must take into account criteria such as the number of critical or important services provided by the same third party, the potential impact of disruptions to these services and the ability of the market to provide adequate alternatives.

Contracts must be in writing and clearly set out the rights and obligations of each party. The DORA Regulation sets out a minimum content for these contracts, i.e. they must contain a clear description of the functions and services to be provided. They must also specify the conditions for subcontracting critical functions, the locations of service provision and data processing, provisions for data protection and recovery in the event of failure. Contracts must also include descriptions of service levels, incident response obligations, cooperation with competent authorities, termination rights and conditions for participation in digital resilience training and awareness programmes. Contractual arrangements for ICT services supporting critical or important functions must also include *(i)* detailed descriptions of service levels with strict performance targets, *(ii)* notification periods and obligations for material impacts, *(iii)* requirements for contingency planning and ICT security, *(iv)* participation in operational resilience testing, *(v)* rights to ongoing monitoring, including audits and inspections, *(vi)* exit strategies with transition periods to avoid disruption, and *(vii)* guarantees for migration to other providers or in-house solutions, ensuring compliance with regulatory frameworks.

Responsibilities and actions required

Financial institutions need to identify all ICT service providers, especially those providing critical services.

In short, the DORA Regulation establishes a legal framework to mitigate the growing risks associated with the digitalisation of the financial sector, in order to ensure greater stability, trust and resilience.

Financial institutions need to identify all ICT service providers, especially those providing critical services, and ensure that contracts comply with the DORA Regulation. They must also implement due diligence policies, ongoing monitoring and audits of suppliers, conduct detailed risk analyses, including concentration risks, and establish clear contingency plans. Institutions must also seek to diversify ICT service providers to reduce exposure to concentration risk and ensure that contracts include appropriate measures to ensure business continuity and exit strategies.

The responsibility for complying with this regulatory framework rests with financial institutions, which face the challenge of ensuring compliance with the requirements of the Regulation, even when dealing with large suppliers and having limited bargaining power.

For their part, ICT service providers will need to implement appropriate security measures to ensure compliance with the DORA Regulation and be able to negotiate contracts in the light of these new rules ■