ARTICLE

FINANCE & TECH: ADOPTION OF THE "DORA" REGULATION ON DIGITAL OPERATIONAL RESILIENCE IN THE FINANCIAL SECTOR NECESSARY ADJUSTMENTS TO PROCESSES AND CONTRACTS

IT and Data Protection | 21/11/22 | Mahasti Razavi

On November 10, 2022, the European Parliament adopted the Digital Operational Resilience Act (DORA).

This regulation aims to harmonize and strengthen the rules for managing the IT-related risks faced by financial entities in the European Union.

It will enter into force on 17th January 2025, leaving a very short period of time for the companies concerned to adjust their internal processes and contractual relations, including existing contracts.

DORA has a significant impact for all financial entities, and their technology partners, as the DORA regulation requires them to:

- *strengthen the financial sector governance mechanisms (art. 5);*
- *implement and maintain IT risk management procedures (art. 6 to 16);*
- *notify security incidents (art. 17 to 23);*
- *perform operational resilience tests (art. 24 to 27);*
- *manage the risks associated with third-party IT service providers in their contractual arrangements (art. 28 to 44); and*
- *implement information sharing mechanisms (art. 45).*

The DORA regulation thus provides for minimum mandatory contractual provisions regardless of the criticality of the services - notably in terms of description of service levels, audit rights or termination - as well as additional provisions for contractual arrangements supporting critical or important functions.

Finally, the regulation also requires an oversight framework of critical IT service provider, which will be subject to increased risk management processes.

General overview

The DORA regulation has a very broad scope and covers almost the entire financial sector. It applies to twenty-one categories of entities, including credit institutions, payment institutions, electronic money institutions, insurance undertakings and management companies. It also applies directly to third-party IT service providers.

DORA aims in general to improve the IT operational resilience of financial entities, in particular by:

- the adoption of internal governance and control frameworks that ensure effective and prudent management of all types of IT risks;
- the implementation and maintenance of IT risk management policies designed to duly protect all the information and IT assets of financial entities;
- obligations to notify the competent authorities (and in certain circumstances end clients) of major IT-related incidents, according to harmonized reporting content and templates;
- the performance of resilience testing aimed at assessing preparedness for IT incidents, identifying any weaknesses, and taking prompt corrective measures;
- mechanisms for the exchange of information on cyber threats between financial entities;
- contractual requirements to manage the risks associated with IT service providers, as detailed below.

These obligations necessarily lead to internal transformations for the financial entities concerned but also have a major impact on their technological partners.

Focus sur l'encadrement des risques liés aux prestataires de services informatiques tiers

The DORA regulation addresses the risks associated with IT providers in two ways:

- by setting out principles and provisions to be included in contracts entered into by financial entities, and
- by establishing an oversight framework of critical IT service providers.

- *Provisions to be included in contracts entered into by financial entities*

According to Article 28 of the Regulation, general principles must be respected by financial entities in their relations with third party IT service providers, resulting in particular in:

- ensuring that their providers comply with appropriate information security standards;
- including in their contracts of termination rights in certain circumstances;
- being able to exercise their rights of access, inspection and audit;
- arranging for the reversibility of services supporting critical or important functions.

More specifically, Article 30 of the Regulation also provides a list of elements that shall at least be included in all contracts between a financial entity and an IT provider, including:

- the locations where the services are to be provided and where data is to be processed;
- des dispositions sur la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, notamment à caractère personnel,
- provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;
- service level descriptions;
- the obligation of the IT service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined ex–ante, in case of IT incident;
- the obligation of the IT service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity;
- termination rights and related minimum notice periods; and
- the conditions for the participation of IT service providers in the financial entities' IT security awareness programmes and digital operational resilience training.

For IT services supporting critical or important functions other obligations apply, including those relating to:

- service levels and applicable corrective measures;
- notice periods and reporting obligations by the IT service provider regarding its ability to effectively provide the IT services supporting critical or important functions under certain conditions;
- the obligation for the IT service provider to implement and test business contingency plans;
- the obligation for the IT service provider to implement complementary security measures, tools and policies;
- the obligation for the IT service provider to participate and fully cooperate in the financial entity's threat-led penetration testing;
- the right to monitor, on an ongoing basis, the IT service provider's performance; and
- exit strategies for contracts with mandatory adequate transition periods.

The regulation also encourages the development of standard contractual clauses to be developed for particular services by the European Supervisory Authorities (ESAs) and adopted by the European Commission.

- *Establishing an oversight framework of critical IT service providers*

The Regulation establishes an oversight framework of critical IT service providers, which will be designated by the ESAs based on various criteria: systemic impact on the stability, continuity or quality of the provision of financial services, reliance of financial entities, degree of substitutability, etc.

Oversight of critical IT service providers consists of an assessment of the rules, procedures, mechanisms and arrangements to manage the IT risks they may pose to financial entities. Within this framework, the overseers have broad powers, including the power to request all relevant information and documents, to conduct general investigations and inspections or to issue recommendations.

This body of rules will have an impact on all parties, both in terms of processes and contractual relationships, and will have to be implemented within a timeframe that is ultimately very short given the scope of the work to be carried out in order to comply with the regulation on the date it enters into force.