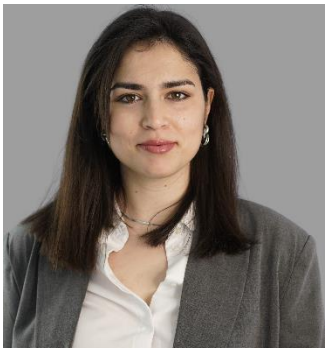
ROKAS

Articles for Lexology

ROKAS

Date: March 2025

TOPIC:
DORA overview: Legal provisions for financial entities and ICT third-party providers



Authors: **Maria Katsioti, Associate**
Andreas Papastathis, Junior Partner

The integration of new technologies in the banking, investment and insurance sectors has digitalized various business processes, including payments, lending and funding operations, claims management and digital insurance underwriting. This digital transformation has interconnected financial entities and their ICT third-party service and infrastructure providers, facilitating the transmission of cyber vulnerabilities and potentially disrupting the financial stability of the EU.

To ensure the operational resilience of these entities, the European Union adopted Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, known as the Digital Operational Resilience Act (DORA), in November 2022. As of January 17, 2025, DORA is in effect and entities within its scope are required to comply with a set of obligations regarding ICT risk management, ICT third-party risk management, digital operational resilience testing and information sharing. The Greek supplementary implementing law to DORA has not yet been issued.

Entities under the scope of DORA

The Digital Operational Resilience Act (DORA) applies to entities in the banking, investment and insurance sectors. This includes, among others specified in the Regulation, credit institutions, payment institutions, electronic money institutions, investment firms, trade and securitisation repositories, crypto-asset service providers within the scope of the Markets in Crypto-Assets (MiCA) Regulation, credit rating

agencies, institutions for occupational retirement provision and insurance intermediaries (hereinafter referred to as financial entities). However, the Regulation sets forth some exemptions from its application for some of the above entities with specific characteristics, such as insurance intermediaries which are small or medium-sized enterprises or entities subject to a very light regulatory framework under relevant sector-specific Union law.

In addition to financial entities, DORA also applies to ICT third-party service providers. These are undertakings that provide digital and data services via Information and Communication Technologies (ICT) and on whom financial entities depend for their ICT functions. Such providers include those offering cloud computing services, software, data analytics services, data center services, operating payment infrastructures and financial entities providing ICT services to other financial entities. The European Supervisory Authorities (ESAs) are expected to finalize the designation of critical ICT third-party providers by the end of 2025, which, as a result, will impose additional compliance responsibilities on them.

Obligations for financial entities with a focus on ICT Risk Management

To achieve the goal of resilient financial entities and ensure the financial stability of the EU, DORA prescribes the following obligations, categorized into five pillars, for financial entities within its scope: ICT risk management, ICT incident management and reporting, digital operational resilience testing, ICT third-party risk management and information-sharing arrangements. It is important to note that financial entities must implement these obligations *"in accordance with the principle of proportionality, taking into account the size, overall risk profile, and the nature, scale, and complexity of their services, activities, and operations"*.

Regarding ICT risk management, DORA requires entities to establish an internal governance, control and risk management framework. This framework should include policies, strategies, protocols and tools to ensure high standards of data availability, authenticity, integrity and confidentiality, as well as the security of ICT assets such as software, hardware, servers and data centers. ICT systems must be appropriate, reliable, technologically resilient and have sufficient capacity.

Additionally, the Entities should map, classify and adequately document all ICT-supported business functions, roles and responsibilities and review risk scenarios regularly. Continuous monitoring of the security and operation of ICT systems and tools is essential to minimize the impact of any ICT risk. Prompt detection of anomalies and identification of potential failure points are crucial. Financial entities must also establish a comprehensive ICT business continuity policy with appropriate plans, procedures and mechanisms and develop and document backup policies and restoration and recovery procedures.

Furthermore, staff should be trained and generally resources should be used to identify vulnerabilities and cyber threats, handle ICT incidents like cyberattacks and assess their impact on the entity's digital resilience. Finally, crisis communication plans should be created to inform clients, counterparts and the public about major ICT incidents or vulnerabilities. It is imperative to note that the management body of the Entities is

responsible for defining, approving, overseeing and ensuring all relevant policies, procedures and arrangements of the ICT risk management framework are in place.

Other obligations for financial entities and ICT third-party service providers

Regarding ICT incident management and reporting obligations under DORA, financial entities are required to establish robust measures for detecting, managing, recording and notifying ICT-related incidents. For specific financial entities that fall within the scope of both DORA and Directive (EU) 2015/2366 (PSD2), such as credit institutions, e-money institutions and payment institutions, the incident reporting requirements for all operational or security payment-related incidents under PSD2 should be replaced by those of DORA.

The classification of the incidents must be based on their impact, considering factors such as the number of clients and counterparts affected, the duration of the incident, its geographical spread and any data losses incurred. For more details on the classification criteria for ICT-related incidents and cyber threats, refer to the Commission Delegated Regulation 2024/1772.

Major ICT-related incidents must be reported to the designated by national law competent authority, which will then forward the information to higher bodies such as the European Central Bank or the European Banking Authority. Relating to the reporting timeframe of major ICT-related incidents, the Commission Delegated Regulation 2025/301 sets the content and time limits for the initial notification (*24h from the moment the entity has become aware)*, intermediate *(within 72 hours from the submission of the initial notification)* and final report on major ICT-related incidents (*no later than one month after the submission of the intermediate report)* as well as the content of the voluntary notification for significant cyber threats. The aforementioned timeframe resembles the incident reporting timeframe under NIS II Directive. This structured approach ensures that incidents are effectively managed and communicated, thereby enhancing the overall digital operational resilience of financial entities.

As for digital operational resilience testing, DORA mandates financial entities to test their ICT systems in order to detect potential ICT vulnerabilities and augment the effectiveness of their preventive, response and recovery capabilities, using tools such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing or end-to-end testing. For some financial entities *(other than entities referred to in Article 16(1), first subparagraph and other than microenterprises),* DORA requires more advanced testing every three years based on threat-led penetration testing *(TLPT)*.

In relation to ICT third-party risk management, financial entities should integrate third-party risk management within their broader ICT risk management framework. To comply with this obligation under DORA and other relevant laws, they need to establish contractual agreements with the ICT service providers. These agreements should clearly define each party's rights, duties under DORA and generally the service terms, taking into account the nature, scale, complexity and importance of ICT dependencies and associated risks. Within the context of third party risk management duty, other relevant

law is the GDPR, as ICT service providers (e.g. providers of data analytics or cloud computing services) often act as data processors under GDPR for the processing of personal data of clients or employees of financial entities on their behalf. Therefore, it is important for financial entities under the scope of DORA, as data controllers, to conclude *(additionally and supplementary to the aforementioned contractual agreement under DORA)* a Data Processing Agreement (DPA) with their ICT service providers, who act as data processors.

Finaly, financial entities may exchange cyber threat information among themselves to strengthen their digital operational resilience. This information-sharing must occur within their trusted communities, protect business confidentiality and personal data as well as respect competition policy rules.

Role of competent authorities under DORA

Competent Authorities *(as set out in article 46 of DORA)* possess all the necessary supervisory, investigatory and sanctioning powers to fulfill their duties under DORA, including imposing and publishing administrative penalties and remedial measures as determined by national law. For the smooth and effective implementation of DORA, the Competent authorities work along with European Supervisory Authorities (ESAs) which are responsible for drafting guidelines and regulatory technical standards for ICT risk management tools, the classification and reporting of ICT-related incidents and the conduct of oversight activities. Finally, the European Commission has the authority to adopt delegated acts and is required to submit a review of the regulation to the European Parliament and the Council by January 17, 2028, after consulting the ESAs and the European Systemic Risk Board.

DORA and NIS II

The NIS II Directive on measures for a high common level of cybersecurity across the Union is relevant to DORA Regulation, as the former sets out similar rules to the latter aiming to enhance the level of cybersecurity of critical entities, including among other sectors of energy, digital infrastructure, transport, space, health, banking and financial markets infrastructure. For financial entities that fall within the scope of both legislations, such as credit institutions, DORA is considered sector-specific union act under the article 4 of NIS II. Consequently, the provisions of DORA regarding reporting obligations, cybersecurity risk management and its supervision and enforcement are applied instead of those of NIS II Directive. As a final note, both DORA and NIS II, along with the GDPR provisions on the security of personal data and other relevant regulations, constitute part of the EU's strategy and regulatory framework to enhance the cybersecurity and resilience of services, products, information systems and data (personal or not) in critical, financial and other sectors across the EU.