Platis - Anastassiadis & Associates

The associate law firm of EY Greece

December 2022

Law Alert

Greece: DORA – New Rules for Digital Operational Resilience in the Financial Sector

The DORA lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities with the aim to achieve a high common level of digital operational resilience of the financial sector throughout the European Union.

On 17 November 2022, EU Institutions adopted the Regulation on Digital Operational Resilience for the Financial Sector ("DORA" or "Act"). The Act, which was proposed by the Commission on 24 September 2020 as part of the 2020 EC Digital Finance Package, constitutes the most solid initiative of the European Union ("EU") to ensure security and resilience of the European financial sector in conditions of rapid digital transformation.

The expansive scope of the Act includes, among others, credit and financial institutions, crypto-asset service providers, trading venues and repositories, investment firms, managers of alternative investment funds, management companies, credit rating agencies, data reporting service providers, crowdfunding service providers and, also, ICT third-party service providers.

In respect of the foregoing entities, the DORA provides for obligations related to (i) ICT risk management; (ii) ICT incident reporting; (iii) digital operational resilience testing; (iv) information and intelligence sharing in relation to cyber threats and vulnerabilities; and (v) ICT third party risk management.

In order to promote innovation, the Act also allows for a more proportionate set of obligations for financial entities which are qualified as micro enterprises vis-à-vis larger financial institutions, which are required to establish more complex governance arrangements.

In addition, the Act explicitly establishes the proportionality principle in both the supervision and compliance with its provisions, according to which financial entities are generally expected to implement the requirements of the Act in accordance with the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.

The DORA will be set into application at the end of a 24-month implementation period, commencing twenty (20) days following publication in the Official Journal of the European Union.

1. **ICT Risk Management Requirements**
   The Act establishes the general obligation of financial entities to have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk under the supervision and responsibility of their management bodies.

   In addition, financial entities are required under the Act to have a sound, comprehensive and well-documented ICT risk management framework, which includes a digital operational resilience strategy and appropriate, reliable, sufficient and technologically resilient policies, procedures, ICT protocols and tools, along with an independent control function within their organization.

   According to this framework, financial entities will be required, on the one hand, to classify ICT supported business functions, roles, responsibilities and assets and their roles and dependencies in relation to ICT risk. On the other hand, they will be needed to identify, on a continuous basis, all sources of ICT risk, assess cyber threats and ICT vulnerabilities and perform a risk assessment upon each major change in their infrastructures, processes and assets.

   Furthermore, they will be obliged to deploy appropriate ICT security tools, policies and procedures, including an information security policy and policies for strong authentication, change management, patches and updates. In addition, they shall have in place (i) detection mechanisms for anomalous activities, (ii) a business continuity policy and ICT response and recovery plans, (iii) backup policies and procedures, restoration and recovery procedures and methods, and (iv) procedures for post ICT-related incident reviews.

   A novelty introduced by the Act is the requirement for obligated entities to conduct business impact analyses ("BIAs") of their exposures to severe business disruptions as means to develop methods of managing risk scenarios.

   Finally, as part of their ICT risk management framework, financial entities shall have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate.

2. **ICT Incident Reporting Requirements**
   In respect of incident reporting, the DORA imposes the following obligations to financial entities:

   - The establishment and implementation of an ICT-related incident management process;
   - The maintenance of a record for ICT-related incidents and cyber threats;
   - The consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to ensure that root causes are addressed;
   - The classification of ICT-related incidents on the basis of the criticality of the services at risk and the determination of their impact;

   Under the Act, financial entities shall report major ICT-related incidents to competent supervisory authorities, which may provide feedback and guidance on the handling of such incidents. Incidents inflicted upon credit institutions classified as significant shall be reported by national authorities to the ECB.

   Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, give relevant notice to their clients and also inform them about mitigation measures.

3. **Digital Operational Resilience Testing Requirements**
   Financial entities, other than microenterprises, are also required to establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework.

The relevant tests, 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, end-to-end testing and penetration testing, shall be undertaken by independent parties, whether internal or external.

At least every three (3) years financial entities shall also be obliged to conduct advanced testing by means of TLPT on several or all critical or important functions, performed on live production systems. At the end of the testing, the financial entity and, where applicable, the external testers shall provide to the competent authority a summary of the findings of the TLPT and the authority shall provide an attestation that the test has been performed in accordance with the requirements.

4. **Information and Intelligence Sharing in relation to Cyber Threats and Vulnerabilities**
Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing takes places within trusted communities of financial entities through information-sharing arrangements that protect the potentially sensitive nature of the information shared.

5. **ICT Third Party Risk Management**
According to the provisions of the DORA, financial entities are obliged to manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework, among others, in accordance with the following conditions:

   - The establishment of a strategy on ICT third-party risk, taking into account multi-vendor strategy. The strategy on ICT third-party risk shall include a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers.
   - The maintenance of a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.
   - The annual reporting to the competent authority of new contractual arrangements with ICT third-party service providers and the ICT services and functions which are being provided.
   - The assessment of outsourced ICT services, the concentration of risks and the undertaking of due diligence on prospective ICT third-party service providers prior to entering into contractual arrangements.
   - The inclusion of a minimum set of elements in the contractual arrangements ICT third-party service providers laid down under the Act and an advanced set of requirements, if the support of critical or important functions is involved. When negotiating contractual arrangements, financial entities and ICT third-party service providers shall consider the use of standard contractual clauses developed by public authorities.

6. **Oversight Framework & Supervisory Powers**
The DORA grants new wide-ranging powers to national and European supervisory authorities for the oversight of critical ICT third-party service providers. In particular, the ESAs shall have the power to designate the ICT third-party service providers that are critical for financial entities. Competent authorities shall also have the power to hold inspections on individual critical ICT third-party service providers and issue recommendations.

   In terms of supervision, competent authorities are granted with all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under the Act, including the execution of on-site inspections, the ordering of corrective and remedial measures, the imposition of effective, proportionate and dissuasive administrative penalties.

7. **Secondary Regulation**
A key aspect of the DORA is its delegation to European Supervisory Authorities ("ESAs"), i.e. the EBA, ESMA and EIOPA, to enact the secondary rules which will render possible the operationalization of the security framework of the Act. Hence, within 24 months from the entry into force of the Act ESAs shall jointly issue Regulatory Technical Standards ("RTS") and Implementing Technical Standards ("ITS") about the implementation of its obligations, which will be compulsory for financial institutions. In addition, the European Commission will also adopt two Delegated Acts for the establishment of the critical supplier supervision framework.

The DORA is available **here**.

About Platis – Anastassiadis & Associates

Platis - Anastassiadis & Associates is part of the EY Law network operating in 90 countries globally and is comprised of 3,500+ people.

We are an independent law office with a core team of 39 lawyers. Our office provides high quality legal services across the full range of commercial and financial transactions.

Especially in our geographical area, we have established an ongoing cooperation with the respective law firms which are associated with EY, in order to offer seamless and consistent regional services to our clients that have cross country operations.

Our experience allows us to better understand our clients' needs and offer them integrated multidisciplinary solutions in the fields of accounting, tax and financial advisory services. Platis – Anastassiadis & Associates law office is solution focused. We work closely with our clients to seek innovative and practical ways of dealing with their issues. Our priority is to help our clients meet their business objectives. Our expertise, commitment and enthusiasm has resulted in the build up of a client base which includes local and international listed, state and private sector companies and financial institutions.

For more information on digital law issues, please contact:

Eirinikos Platis
Partner
eirinikos.platis@gr.ey.com

Antonios Broumas
Senior Manager
antonios.broumas@gr.ey.com

at the
Platis - Anastassiadis & Associates Law Partnership
Tel.: +30 210 2886 512
Email: platisanastassiadis@gr.ey.com

ey.com