Ensuring Contractual Compliance with the Digital Resilience Operational Act

By Michael Pelosi, Senior Legal Counsel and Emilios Charalambous, Associate at Elias Neocleous & Co. LLC

With the rapid technological progress that is taking place, EU legislators have been actively trying to keep up and enhance the regulatory provisions in the fields of cybersecurity. Near the top of the headlines is the Digital Operational Resilience Act (DORA) under Regulation (EU) 2022/2554, which has been entered into force on 16 January 2023 and will apply as of 17 January 2025.

DORA was created with the intention of addressing resilience and security requirements for financial entities and their ICT systems, with two key objectives:

- To comprehensively address ICT risk management in the financial services sector and;
- To harmonise the ICT risk management regulations that already exist in individual member states

While DORA has different pillars, including principles and requirements on ICT risk management frameworks, basic and advanced testing, and reporting of major ICT-related incidents to competent authorities, it also places a focus on key contractual provisions – the considerations that should be taken into account before entering into a contract on the use of ICT services, the circumstances that they should be able to be terminated under, the exit strategies that should be put in place and the overall provisions that should be included.

Who does it apply to?

DORA applies to all financial institutions within the EU, including traditional entities like banks, investment firms, and credit institutions, as well as non-traditional entities such as crypto-asset service providers and crowdfunding platforms.

Importantly, DORA also extends to certain entities that are usually outside the scope of financial regulations. For instance, third-party service providers that offer ICT systems and services to financial firms—such as cloud service providers and data centers—must adhere to DORA requirements. Additionally, DORA covers firms that provide critical third-party information services, including credit rating agencies and data analytics providers.

Why should one pay attention?

Unlike many legislations that request firms to take action without counteractions, DORA has prioritized penalties in order to ensure compliance with its provisions.

Companies that violate the requirements could face financial penalties of up to 2% of their total annual global turnover or, for individuals, a maximum fine of EUR 1,000,000. The exact fine will be determined based on the severity of the violation and the level of cooperation from the financial entity with authorities.

Likewise, financial entities that do not report major ICT-related incidents or significant cyber threats as mandated by DORA could be subject to fines. Third-party ICT service providers classified as "critical" by the European Supervisory Authorities (ESAs) may incur penalties of up to EUR 5,000,000, or in thE case of individuals, a maximum fine of EUR 500,000 for failing to comply with the Regulation's requirements. The ESAs will have the power to enforce these fines.

Considerations before entering into contracts on the use of ICT services:

As per Article 28(4) of DORA, financial entities should:

a. Consider whether the ICT services would support a critical or important function;
b. Evaluate whether supervisory conditions for contracting would be met;
c. Identify and assess all relevant risks in relation to the contractual arrangement;
d. Undertake all due diligence on prospective ICT third-party providers and ensure that they are suitable;
e. Identity and assess potential conflicts of interest.

The intention of course is to ensure that companies are aware of who they are entering into a contractual relationship with and what the associated risks are – as with every proper contract, technological or not.

Ending and getting out of contracts:

Under Article 28(7) of DORA, financial entities should have in place provisions that would allow them to terminate their ICT services contracts in cases that:

a. There has been a significant breach of applicable laws, regulations or contractual terms by the ICT third party providers
b. They have identified circumstances that are deemed capable of altering the performance of the functions provided through the contractual arrangement
c. The ICT third party provider has evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and confidentiality of data
d. The competent authority can no longer effectively supervise the financial entities as a result of the respective contractual arrangement

While, under Article 28(8), financial entities are encouraged to put exit strategies in place, which should take into account the risks that may emerge from the failure, deterioration of services or any other disruptions to the third-party provider. Such exit strategies should allow the financial entities to exit their contractual arrangements without disrupting their business activities or limiting their regulatory compliance and without any detriment to the continuity and quality of their services.

Provisions to include:

As per Article 30 of DORA, the contractual arrangements should include different aspects considering whether the use of ICT services support critical or important functions. As a brief overview, some of the key provisions to include are:

- A clear and complete description of all functions and ICT services to be provided by the ICT third-party provider
- The locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed
- Provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in case the ICT third party provider stops operating for one reason or another
- Termination rights and related minimum notice periods for the termination of the contractual arrangements
- Exit strategies, with a focus on the establishment of a mandatory adequate transition period.
-

Overall, when negotiating contractual arrangements, financial entities and ICT third-party service providers shall consider the use of standard contractual clauses developed by public authorities for specific services.

As DORA is one of many cybersecurity regulations within the European Union, financial firms should try to stay up to date with the recent updates and compliant with the latest provisions in order to ensure smooth and long-term operations alongside the regulatory technological landscape.

If you would like further information or support in evaluating your contracts in relation to DORA, please contact Michael Pelosi or Emilios Charalambous.

ELIAS NEOCLEOUS & Co LLC