EXPLORING DORA: EU TIGHTENS IT SECURITY RULES FOR THE FINANCIAL SECTOR, TARGETING "CRITICAL" THIRD-PARTY PROVIDERS

Date: 13 January 2023

EU Data Protection, Privacy, and Security Alert

By: Dr. Ulrike Elteste, Dr. Thomas Nietsch

In mid-December the European Union (EU) enacted new legislation aiming at harmonizing, and tightening, information technology (IT) security rules in the financial sector: Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (Digital Operational Resilience Act, or DORA). Coming into full force on 17 January 2025, DORA lays down uniform requirements concerning information and communication technology (ICT) supporting the business processes of most regulated entities in the financial sector. It also extends the powers of the financial services supervisory authorities to ICT service providers deemed to be "critical" by the authorities.

Due to the complexity of the requirements and processes involved, companies in - or serving - the financial sector should already start preparing for the impending changes. This applies in particular to potentially "critical" service providers, as deadlines for comments and compliance during the designation procedure are short.

SUBJECT MATTER OF DORA

DORA harmonizes the rules on ICT risk management, incident notification, digital operational resilience testing, and related supervisory activities, notably as it pertains to the management of third-party ICT service providers.

Furthermore, DORA clarifies that "Financial Entities" may share information with other Financial Entities with the aim of protecting themselves against ICT security risks, provided they notify the authorities of the corresponding arrangements and comply with privacy and competition laws. This appears to be similar in some respects to IT security related information sharing arrangements adopted in the United States, which the U.S. Department of Justice has opined can be implemented in principle without triggering competition concerns.

SCOPE OF APPLICABILITY OF DORA

"Financial Entities"

DORA applies to a wide range of financial sector undertakings, under the common umbrella designation of "Financial Entities," which includes:

- Credit institutions;
- Payment institutions, electronic money institutions, and account information service providers;
- Investment firms, managers of alternative investment funds, and management companies of undertakings for collective investment in transferable securities;

- Crypto-asset service providers authorized under the forthcoming MiCA Regulation (see our previous alert here) and issuers of asset-referenced tokens;
- Central securities depositories, central counterparties, trading venues, trade repositories, and securitization repositories;
- Data reporting service providers within the meaning of Regulation (EU) 600/2014;
- Insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, and institutions for occupational retirement provision;
- Credit rating agencies;
- Administrators of critical benchmarks designated by the EU Commission pursuant to Regulation (EU) 2016/1011; and
- Crowdfunding service providers.

"IT and Communications Services Providers"

In addition to the Financial Entities themselves, DORA also applies to companies providing Financial Entities with ICT Services ("ICT Third-Party Service Providers"), defined as digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis. This expressly includes also the provision of hardware as a service (such as data center services) and hardware services that include the provision of technical support via software or firmware updates by the hardware provider. It also covers "over the top" and other electronic communication services, not however traditional analogue telephone services.

Out of Scope

Companies exempt from certain regulatory requirements for their respective sector due to their limited size or significance are mostly also exempt from DORA or subject only to simplified risk management requirements.

Payment systems (i.e., funds transfer systems with formal and standardized arrangements and common rules for the processing, clearing, or settlement of payment transactions) remain subject to a distinct framework and oversight by central banks.

Providers of purely technical services for payment processing (including those processing messages between equipment used for and players involved in card payments and online payments) are not directly regulated as Financial Entities but may qualify as ICT Third-Party Service Providers.

USE OF THIRD-PARTY ICT SERVICES BY FINANCIAL ENTITIES

Chapter V (Articles 28–44) DORA sets out principles for how Financial Entities must manage the risks of using ICT Third-Party Service Providers. While most "Financial Entities" are already subject to extensive risk management, documentation, and outsourcing-related obligations, DORA takes these to a new level. The requirements include (among others) the following:

- Financial Entities must conduct and document internal assessments, in particular, develop a strategy on ICT third-party risk and conduct due diligence to assess the suitability of each provider.

- Financial Entities must inform the supervisory authorities of ICT Services supporting critical or important functions that they use.
- Contracts with ICT Third-Party Service Providers must be “in one written document” available either on paper or in “downloadable, durable and accessible format.”
- Article 30 DORA lists topics that must be covered in service agreements with ICT Third-Party Service Providers, including audit rights, termination rights, and service level agreements.

DORA does not distinguish between outsourcing and other forms of using service providers, but there is an operational differentiation based on the nature of the services performed: Third-party providers supporting “critical or important functions” will be placed under higher regulatory scrutiny. Article 30 DORA even contemplates the possibility of supervisory authorities developing standard contractual clauses and detailed conditions for providing “certain” (read: cloud computing) services. These provisions suggest that legislators are concerned that IT security in the financial sector is not adequate for the current threat environment. Under DORA, any Financial Entity may only enter into contractual arrangements with ICT providers that comply with “appropriate” information security standards, and for providers supporting critical or important functions, Financial Entities should “consider” requiring the application of “the most up-to-date and highest quality information security standards."

NEW OVERSIGHT FRAMEWORK FOR “CRITICAL” ICT THIRD-PARTY SERVICE PROVIDERS

The most significant change introduced by DORA is that supervisory authorities for the financial sector will directly supervise ICT Third-Party Service Providers that are themselves not engaged in regulated activities but deemed to be “critical” to Financial Entities.

In the current pre-DORA era, the use of IT and communications services by regulated entities from the financial services sector is only subject to the outsourcing and risk management rules that apply to the regulated entities. These requirements are primarily and directly bearing on the regulated entities themselves and only affect ICT Third-Party Service Providers indirectly through contractual requirements passed on by the regulated entities to the providers.

Designation of “Critical” ICT Third-Party Service Providers

Under DORA, the main EU financial services regulators such as theEuropean Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority will designate ICT Third-Party Service Providers that are critical for Financial Entities and then directly supervise those providers.

To determine which providers should have the status of “critical” providers, the authorities will conduct an assessment, which will take into account the number and importance of the ICT Third-Party Service Provider's customers in the financial sector, including constellations where the provider serves only as a subcontractor of the immediate contract partners of the Financial Entities. The EU Commission may adopt a supplementing legal instrument further detailing the criteria for the “criticality” assessment by 17 July 2024.

As mentioned, DORA starts to apply only on 17 January 2025, but once applicable, the process for designating “critical” providers will be subject to tight deadlines:

- The lead authority will notify the provider of the outcome of the criticality assessment;
- The provider will be able to submit a statement within six weeks of receiving the notification;
- The lead authority will respond to this within 30 days and may request additional information; and
- The authorities, through a Joint Committee, will notify the provider that it has been designated as a critical ICT provider for the financial sector and the starting date as from which it is subject to oversight activities, which will be no later than one month after the notification.

All in all, between the first notification by the authority to the actual implementation, companies which would not already be ready for DORA may need to expedite their compliance implementation within a very tight four-to-eight-month window.

Option to Apply for "Critical" Status

Considering it will be possible for ICT Third-Party Service Providers to apply to be given "critical" status on a voluntary basis, some companies may consider stepping forward to acquire not only regulatory foreseeability and predictability but also gain a non-negligible competitive advantage by being "DORA-Ready."

Extraterritorial Scope

In line with recent EU developments, DORA also has an extraterritorial component: Once designated as "Critical," ICT Third-Party Service Providers not already established within the EU territory will need to set up a subsidiary in the EU within 12 months of the designation. While there will not be a requirement to also process data only locally in the EU, DORA envisages that the supervisory authorities will conduct inspections also in third countries outside the European Economic Area.

RELATIONSHIP WITH OTHER LAWS

General Data Protection Regulation (GDPR)

Privacy law requirements for companies regulated under DORA remain unaffected. IT service providers should note that DORA presents challenges which are separate and distinct from those of GDPR. Privacy law requirements partly overlap with requirements under financial services supervisory law: If personal data is processed as part of the services provided, it must be protected by adequate technical and organizational means under GDPR. While the most obvious overlap targets the need for data processing agreements underArticle 28(3) GDPR and personal data security requirements under Article 32 GDPR, the supervision and enforcement of each DORA and GDPR will be performed by different authorities, whose interpretations may vary (but, hopefully, will not contradict each other).

Consequently, breaches of European privacy laws may also constitute a violation of financial services supervisory laws and expose companies to cumulative procedures.

General IT Security Laws

Directive (EU) 2022/2557 on the resilience of critical entities does not apply if DORA is applicable.

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the union (NIS2) applies in addition to DORA to the extent the NIS2 directive covers certain credit institutions, trading venues, and central

counterparties. However, DORA is more specific (lex specialis), thus taking prevalence in the event of any contradictions. (See our alert here.)

Other Financial Services Sector Laws:

Most of the Financial Entities to which DORA applies are already subject to IT security requirements, but they derive from a patchwork of EU directives, each targeting specific players, as well as implementing laws, guidelines, and standards on both the EU and national levels, with a varying degree of harmonization between them.

DORA replaces the provisions of the existing directives that deal with ICT risks and related supervisory powers, as set out in the accompanying Directive (EU) 2022/2556. Because DORA, as a regulation, is directly applicable in EU member states, it will be more efficient from the perspective of the EU Commission and the supervisory authorities.

The security of payment systems and payment processing service providers remains a cause of concern, as evidenced by the DORA recitals. The EU Commission will assess the need for additional cyber resilience measures in the context of its forthcoming review of the Second Payment Services Directive (EU) 2015/2366, which is due in July 2023 and may result in stricter requirements for those actors, be it under DORA or other laws.

Our Global Data Protection and Cybersecurity Team remains available to assist you in global and local cybersecurity matters from our offices in the Americas, Europe, Middle East, Asia and Australia.

KEY CONTACTS

DR. ULRIKE ELTESTE
COUNSEL

FRANKFURT
+49.69.945.196.416
ULRIKE.ELTESTE@KLGATES.COM

DR. THOMAS NIETSCH
PARTNER

BERLIN
+49.30.220.029.408
THOMAS.NIETSCH@KLGATES.COM

