ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy ADVISORY ■

NOVEMBER 21, 2023

What You Should Know About the EU Digital Operational Resilience Act

by *Alice Portnoy* and *Wim Nauwelaerts*

On September 24, 2020, the European Union (EU) adopted its digital finance package to foster a European approach to technological development that encourages financial stability and consumer protection. The package includes various legislative initiatives, with a view to stimulating European innovation and competition while addressing and mitigating the risks that can result from the use of digital tools by the financial sector.

As part of this package, the EU institutions approved the Digital Operational Resilience Act (DORA) at the end of 2022. DORA, which goes into effect on January 17, 2025, is intended to strengthen the IT security of financial entities (FEs) such as banks, insurance companies, and investment firms. It introduces uniform requirements—homogenous across all EU Member States—for the security of network and information systems of companies and organizations operating in the financial sector, as well as third parties that provide information and communication technology (ICT)-related services to those companies and organizations, such as cloud platform and data analytics services.

DORA will supplement and interact with other EU laws such as the Payment Services Directive, the General Data Protection Regulation (GDPR), and the Data Governance Act (DGA). Companies and organizations subject to the DORA may therefore have to consider their obligations under these other EU laws as well.

DORA's Main Requirements in a Nutshell

DORA imposes new obligations on FEs for ICT risk management; reporting and notifying cyber incidents; performing resilience testing; sharing information and intelligence relating to cyber threats with other businesses; and reviewing contracts with ICT service providers (ICTSPs). It also provides new requirements for ICTSPs that support FEs and establishes a new oversight framework for critical ICTSPs. DORA will be supervised and enforced by EU and Member State authorities.

Financial Entities Subject to DORA

DORA applies to a wide range of FEs, including:

Credit institutions	Payment institutions, including those exempted pursuant to Directive (EU) 2015/2366	Account information service providers	Electronic money institutions, including those exempted pursuant to Directive 2009/110/EC
Investment firms	Crypto-asset service providers as authorized under the regulation on markets in crypto-assets and issuers of asset-referenced tokens	Central securities depositories	Central counterparties
Trading venues	Trade repositories	Managers of alternative investment funds	Management companies
Data reporting service providers	Insurance and reinsurance undertakings	Insurance intermediaries, reinsurance intermediaries, and ancillary insurance intermediaries	Institutions for occupational retirement provision
Credit rating agencies	Administrators of critical benchmarks	Crowdfunding service providers	Securitization repositories

Depending on their size and overall risk profile, as well as the nature, scale, and complexity of their activities, FEs will have to comply with different requirements ranging from ICT risk management and governance to incident response, resilience testing, and third-party risk management. For instance, DORA requires FEs to implement internal governance and control frameworks to ensure that they can properly manage ICT risks (i.e., by drafting policies that set high data protection standards and allocate clear roles and responsibilities to internal teams). Also, FEs subject to DORA will have to put in place robust mechanisms that can detect irregularities, respond to ICT-related incidents, and gather information on vulnerabilities and cyber threats to analyze the impact of these incidents.

Regarding ICT-related incidents, DORA requires FEs to record all incidents and implement extensive incident management procedures. This includes establishing detailed processes to classify incidents and assess their impact based on specific factors, such as the criticality of the services of the FEs, the geographical impact of the incident, and the types of data affected. Major ICT-related incidents will have to be reported by FEs to their relevant authorities in accordance with standards that will be established at the EU level by July 2024 (and which will determine the content of reports and notifications and the reporting deadlines). In some cases, FEs may also have to inform their clients and the media about serious ICT-related incidents.

ICT Service Providers Subject to DORA

FEs increasingly depend on ICT services, software solutions, and data-related services offered by third parties. Providers of cloud computing services, software, data analytics services, data center services, or payment-processing activities, as well as operators of payment infrastructures, have crucial roles in the delivery of financial services. Operational disruptions and cyber incidents affecting ICTSPs can endanger the financial stability of FEs and, ultimately, the integrity of the EU market.

DORA includes new rules for FEs to monitor the (additional) risks and threats that can arise from the involvement of ICTSPs. For instance, FEs are required to rely on ICTSPs that have implemented appropriate information security standards, and to that end, FEs will be expected to conduct and document due diligence on potential ICTSPs. FEs will also have to maintain a record of all their contracts with ICTSPs, documenting the functions supported by the ICTSPs, and FEs should report to their competent authorities about their ICTSPs at least once a year.

If FEs delegate critical or important functions to specific ICTSPs (i.e., ICTSPs that are considered, by EU regulators, to be essential for FEs to perform financial activities), more stringent requirements will apply. For example, DORA requires FEs relying on critical ICTSPs to set up strong exit strategies to make sure they can secure the continuity and quality of their financial services. Critical ICTSPs will have to comply with strict notice periods and reporting obligations and will be subject to more scrutiny by both FEs and regulators.

The EU legislators wanted to ensure appropriate oversight of critical ICTSPs, especially because these companies also provide, in some cases, their services to FEs within the same group, which may lead to potential conflicts of interest and concentration risks. To address this issue, DORA establishes a new oversight framework whereby one of the major EU financial authorities (e.g., the European Banking Authority or the European Securities and Markets Authority) is designated as a lead overseer (LO) to monitor the activities of critical ICTSPs. LOs will have the power to conduct investigations (i.e., on-site and offsite inspections) and oppose contractual arrangements ultimately affecting the stability of an FE or the financial system.

While DORA does not prohibit FEs from using non-European ICTSPs, the law requires ICTSPs that support FEs subject to DORA and are considered critical or important to establish a subsidiary in the EU. This means that non-EU ICTSPs that support EU FEs subject to DORA will have to assess whether they can be considered, under EU law, critical ICTSPs and are compelled to set up a place of business in the EU.

In any case, FEs will have to reinforce their contracts with ICTSPs and make sure that an extensive set of contractual safeguards are included (e.g., on the authenticity and confidentiality of protected data, on the locations where ICT services are provided, and where data is to be processed).

Enforcement

DORA compliance will be overseen by a combination of supervisory authorities designated by the EU Member States. For instance, activities of credit institutions subject to DORA will be supervised by their home authority, while insurance companies will be monitored by the sector-specific authority of the EU Member State where they are established. FEs and ICTSPs subject to DORA will therefore have to determine, on a case-by-case basis, which EU Member State authority or authorities will be competent to monitor their compliance.

To harmonize the supervision of ICT risks in the financial sector, DORA also brings together EU financial authorities—such as the European Banking Authority and the European Securities and Markets Authority, collectively referred to as the European Supervisory Authorities—to support the myriad designated EU Member State authorities monitoring DORA compliance.

DORA allows EU Member State authorities competent to monitor the activities of FEs and ICTSPs to impose administrative fines (including in collaboration with other authorities, such as data protection authorities). For example, DORA leaves it to the discretion of these authorities to examine whether a DORA violation was intentional or resulted from an FE's or ICTSP's negligence in determining the amounts of fines to be imposed.

Interplay Among DORA, GDPR, and DGA

DORA also establishes a framework for promoting voluntary business-to-business data sharing in the financial sector. This aims to help FEs boost their cyber resilience and raise awareness of cyber threats in the financial industry. To encourage these initiatives, DORA will allow FEs to exchange information and intelligence (such as indicators of compromise, tactics, and procedures) with other FEs, provided the sharing can be secured via arrangements that comply with other EU data-related laws, such as the GDPR or the DGA.

Moreover, DORA will impose new incident reporting and notification requirements on FEs and ICTSPs that may apply in parallel to personal data breach notification requirements under the GDPR. FEs and ICTSPs will have to make sure that their DORA procedures are aligned with data protection responsibilities and should design effective protocols to handle ICT-related incidents that involve personal data.

How DORA Can Impact Companies and Organizations Outside the EU

The financial sector often uses cross-border ICT services. DORA is therefore expected to affect non-EU companies that qualify as FEs or that provide ICT-related services to FEs in the EU. Companies active in the financial sector should therefore assess whether their activities as an FE, an ICTSP, or even a critical ICTSP bring them under DORA's scope.

DORA also has extra-territorial enforcement scope. When oversight objectives cannot be attained by interacting with a subsidiary in the EU or by exercising oversight activities on premises located in the EU, the LO may exercise its investigatory powers on any premises located in a non-EU country that is owned or used in any way by a critical ICTSP to provide services to FEs in the EU.

You can subscribe to future ***Privacy, Cyber & Data Strategy*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or a member of our **Privacy, Cyber & Data Strategy Team**.

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: Vantage South End ■ 1120 South Tryon Street ■ Suite 300 ■ Charlotte, North Carolina, USA 28203-6818 ■ +1 704 444 1000 ■ Fax: +1 704 444 1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: City Center Fort Worth ■ Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ +1 214 922 3400 ■ Fax: +1 214 922 3899
LONDON: LDN:W ■ 6th Floor ■ 3 Noble Street ■ London ■ EC2V 7DE ■ +44 20 8161 4000
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 755 Page Mill Road ■ Building C - Suite 200 ■ Palo Alto, California, USA 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333