GOODWIN

ALERT · 28 OCTOBER 2024

EU Commission Regulations on Digital Operational Resilience: A Reminder That DORA is Less Than Three Months Away and Will Apply to US and UK CTPPs

BY Andrew Henderson Gretchen Scott Curtis McCluskey Céline Moille James Taylor Matthew Dixon-Ward

The European Commission's adoption on 23 October 2024 of the two regulations (Regulations) supplementing the [the Regulation on digital operational resilience for the financial sector Publications Office (europa.eu)] (DORA) is a further reminder that the need for DORA compliance is now less than three months away.

DORA came into force on 16 January 2023 and will apply starting on **17 January 2025**.

The Regulations comprise:

- a delegated regulation Register of Commission Documents - C(2024)6901 (europa.eu) which addresses content and time limits for notifications of and reports on major ICT-related incidents, and the content of the voluntary notification for significant cyber threats; and
- an implementing regulation Implementing Regulation Register of Commission Documents - C(2024)7277 (europa.eu) lays contains the standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threats.

The Regulations will take effect when DORA starts to apply.

DORA Revisited

We have discussed DORA in previous alerts, ESA Publications on Digital Operational Resilience: A Reminder That DORA is Less Than Six Months Away and Will Apply to US and UK CTPPs | Insights & Resources | Goodwin (goodwinlaw.com), Digital Markets Act: Mandatory Compliance for Big Tech Companies | Insights & Resources | Goodwin (goodwinlaw.com), What DORA Means for Fund Managers | Insights & Resources | Goodwin (goodwinlaw.com) and Too Important To Fail? Further Light on When EU and Non-EU Technology Providers Will Become Subject To DORA. We have also set up a microsite to address DORA and the similar regime in the UK: Financial Regulations for Critical Third-Party Technology Providers in the EU and UK.

DORA seeks to address potential systemic and concentration risks posed by the financial sectors' reliance on a small number of critical third-party providers (CTPPs), and introduces an oversight framework for CTPs located in the EU whom the three EU supervisory authorities (ESAs) deem to be "critical to the stability and integrity of the [EU] financial system" and designate as critical TPPs.

Main Obligations for EU Financial Entities

DORA's main requirements for EU financial entities, such as banks, broker-dealers, and insurers, are summarised below:

Risk Management: Implement policies and procedures to identify and manage risks associated with ICT.

Incident Management: Develop processes for identifying, reporting, responding to, and recovering from ICT-related incidents.

Resilience Testing: conduct regular testing of systems and processes, including threat led penetration testing, at least every three years.

Third-party ICT Risk Management: Maintain a register of third-party ICT service providers, focusing on critical suppliers, to ensure compliance with contractual obligations.

Information Sharing: Engage in information-sharing arrangements on cyber threats with other financial entities.

Application Outside The EU: US and UK Third Party ICT Providers Beware

In addition to the provisions of DORA that apply to EU financial entities, DORA will also apply to CTTPs that provide services such as information and communication technology to EU financial entities. As we have noted before, DORA **can apply to non-EU** CTPPs, including those in the US and UK, that provide services to EU financial entities.

The Commission Regulations

As an EU regulation and unlike an EU directive, DORA will bind EU business directly without the need for the individual Member States themselves to implement laws to give DORA effect. DORA does require the Commission and European Supervisory Authorities to make further measure to expand DORA's provisions: the Regulations are part of this.

These materials consist of four final draft regulatory technical standards (RTS), one set of Implementing Technical Standards (ITS) and two guidelines.

Next Steps for Financial Entities and Third-Party Providers

Ahead of the 17 January 2025 deadlines, EU financial institutions will need to have begun the following:

- **Assess current ICT frameworks** including identifying existing policies, procedures, and controls, and conducting GAP analyses to consider essential changes with robust governance measures and ultimate board responsibility.
- **Identify responsibilities and roles of current management and other staff**, including consideration of roles that can be delegated internally and roles that require additional expertise across all relevant departments, such as ICT, legal, compliance, client/investor relations, and general operations.
- **Recognize key external contacts and service providers** to ensure procedures, communications and reporting are well established and contractual arrangements are reviewed and renegotiated, as necessary.
- **Implement regular testing for digital operational resilience as well as the mandatory penetration tests.**
- **Consider internal and external communications practices** to ensure open and transparent communication for warning, disclosing and reporting, including local regulator contact.

- **Finalise your Digital Resilience Strategy** which should cover all the above, including: risk assessments, incident response plans and reporting, management of external service providers, internal procedures, monitoring, and compliance with updates.

How Can Goodwin Help?

We can assist you with:

1. Analysis of whether and how DORA applies to your business;
2. Setting up an EU subsidiary in order to comply with DORA;
3. Conducting a review of your key procedures and contracts to ensure DORA compliance;
4. Drafting and negotiating addenda to your contracts that satisfy the requirements of DORA; and
5. Helping you prepare and implement internal processes and procedures and draft or amend policies and manuals for DORA compliance.

To discuss the contents of this alert, please contact the authors or your usual Goodwin contact.

CONTACTS

Andrew Henderson
Partner

andrewhenderson@goodwinlaw.com
London | +44 (0)20 7667 3628

Gretchen Scott
Partner

gscott@goodwinlaw.com
London | +44 (0)20 7447 4292

Curtis McCluskey
Partner

cmccluskey@goodwinlaw.com
London | +44 (0)20 7447 4279

Céline Moille
Counsel

cmoille@goodwinlaw.com
Luxembourg | +352 27 86 67 58
Paris | +33 1 85 65 71 71

James Taylor
Counsel

jamestaylor@goodwinlaw.com
London | +44 (0)20 7447 4825

Matthew Dixon-Ward
Associate

mdixonward@goodwinlaw.com
London | +44 (0)20 7667 3086