The Digital Operational Resilience Act – An Overview

May 2024

ROPES & GRAY

Agenda

1. Introduction to DORA

2. Four Core Obligations

3. Countdown to 2025

1. Introduction to DORA

ROPES & GRAY

The EU Cyber Landscape: A Reminder

- The European Union has become the most heavily regulated jurisdiction in the world for cybersecurity – as well as one of the most attractive for criminals and bad actors, from solo hackers to nation states.

- In 2024 alone, Orange, Mandiant and the Swiss Air Force suffered large hacks – and those are **only a fraction** of the hundreds (if not thousands) of incidents that go unreported or undetected.

- In addition to the existing laws – EU GDPR and UK GDPR; NIS Directive (EU) and NIS Regulations (UK); and ePrivacy Directive (EU) and ePrivacy Regulations (UK) – there is a raft of soon-to-be-finalised legislation which aims at regulating and strengthening cybersecurity in a range of key sectors.

- The Directive on minimum cybersecurity standards to be implemented across the EU ("NIS2") and the Digital Operational Resilience Act ("DORA") are the most important of these laws – DORA will take effect in **January 2025**.

- **And the UK?** The Product Security and Telecommunications Infrastructure Act 2022 and Regulations 2023 took effect last month – and more is to come.

DORA: The View From 30,000 Feet

- DORA is a European Union regulation designed to strengthen the financial sector's IT security posture.

- It sets requirements for the security of network and information systems of organisations in the financial sector – **as well as** critical third parties that provide information communication technologies ("ICT) to them (e.g., cloud platforms and data analytics services).

- In practice, this means harmonising and strengthening existing obligations around ICT **governance**, **risk management** and **incident reporting** – with responsibility for compliance going to the board level.

- DORA is part of a wider European legislative drive – the Digital Finance Package – that aims to foster technological development and ensure financial stability and includes proposals on (1) markets in crypto assets ("MiCA") and distributed ledger technology ("DLT").

- **TAKEAWAY**: DORA must be implemented in the same way across the EU (subject to some national derogations). Member States have until **17 January 2025** to do this, at which point DORA will apply…

Scope of Application

- DORA applies to a **wide range** of financial and financial-adjacent institutions and entities, including:
  - Credit Institutions and Investment Firms; Payment and Electronic Money Institutions
  - Central Counterparties / Trade Repositories; Alternative Investment Managers
  - (Re)Insurance Undertakings and Intermediaries
  - Crypto-Asset Services Providers / Issuers; Crowdfunding Service Providers

- Although most of these organisations are already subject to some form of cybersecurity regulation in the EU, DORA (1) significantly expands the scope of these laws, and (2) will apply to most of your business activities in the EU – **including on an extra-territorial basis…**

- DORA also applies to ICT third-party providers that are considered to be "critical" by the **European Banking Authority**, the **European Securities and Markets Authority** and the **European Insurance and Occupational Pensions Authority**, acting through their Joint Committee.

- Providers will be designated as critical based on several factors, including: (1) the potential **systematic impact** on the provision of financial services in the event of a **large-scale failure**; (2) the type and importance of entities that rely on the provider; and (3) how easily the provider **can be replaced**.

DORA Enforcement

- **Overview**: EU Member States are required to introduce rules that provide for "appropriate, effective and proportionate" penalties and other measures for breaches of DORA.

- This can include **criminal penalties** – an approach that aligns with wider trends in EU tech regulation.

- Penalties for ICT third-party service providers can be up to 1% of their daily average worldwide turnover and applied on a daily basis (for a maximum of six months) until compliance is met.
  - Providers are therefore likely to impose strict indemnification obligations on your entities to ensure that they bear the liability for acts or omissions that result in non-compliance by the provider.

- DORA gives supervisory authorities (i.e., national regulators) wide investigational powers, including on-site audits, document requests and orders to remedy non-compliance (likely within a short period).
  - The last of these is increasingly being used under the GDPR – and in practice is worse than a fine.

2. Four Core Obligations

ROPES & GRAY

Core Obligation #1: Governance and Controls

- **Overview**: Management must approve and oversee the implementation of an IT risk management compliance programme that aligns with and reflects the entity's risk profile and tolerance.

- In other words, the board must **maintain an active role** in understanding and directing the company's approach to ICT risk – including through regular training to keep their knowledge up to date.
  - Given the speed at which the cybersecurity world is developing, this won't always be an easy task.

- **NEXT STEPS**: The board bears responsibility for its entity's ICT risks and compliance, so you should:
  - Make management aware **now** about the DORA assessment process and their role going forward.
  - Help them understand what's needed: roadmaps / gap assessments; institutional backing; investments.
  - Roll out training **before** DORA takes effect (ideally starting in mid-2024).

Core Obligation #2: ICT Risk Management

- **Overview**: Entities must have in place an appropriate and documented IT risk management framework that helps them address risks quickly and comprehensively. As a minimum it will include:
  - Implementing policies, procedures and tools, including reporting lines.
  - Adopting robust security systems and advanced resilience testing at least once every three years.
  - Helpfully, these measures can be applied on a **proportionate** and **risk-based basis…**

- … However, DORA takes a prescriptive approach to certain of its obligations, such as making entities:
  - Conduct business impact analyses of their exposure to severe business disruptions.
  - Establish a crisis management function for handling internal and external communications.

- **NEXT STEPS**: Although most of these organisations are already subject to some form of cybersecurity regulation in the EU (e.g., the GDPR, NIS1), DORA (1) significantly expands the scope of these laws, and (2) will apply to at least some – if not most – of an entity's business activities in the EU.

Core Obligation #3: Incident Reporting

- **Overview**: Entities must have processes in place to identify, manage and notify ICT security incidents.

- Reporting timelines are among the most involved in the EU:
  - **Initial Notification**: Major incidents must be notified to the competent authority without undue delay.
  - **Secondary Notification**: This time period is to be determined by regulatory authorities in due course.
  - **Ongoing Notification(s)**: Whenever there is a relevant update or if requested by the authority.
  - **Final Report**: This time period is to be determined by regulatory authorities in due course.

- Entities may need to report to affected clients – in addition to their obligations under GDPR/NIS2 – and senior ICT staff must provide reports and recommendations to management on a yearly basis.

- **NEXT STEPS**: Existing reporting procedures are unlikely to be sufficient, meaning that you should: (1) assign roles and responsibilities for DORA breach reporting; (2) establish incident response procedures (these can be folded into a wider framework); and (3) train relevant staff.

Core Obligation #4: Third Parties

- **Overview**: Financial entities must ensure that their (new and existing) contractual arrangements with third-party ICT service providers meet the prescriptive requirements set out in DORA.

- These requirements are similar to the EBA's guidelines on outsourcing arrangements; the GDPR mandatory provisions will also be required if the services involve personal data (which is likely…).

- Contracts must include provisions on (among other things):
  - A description of the services being provided and any conditions on sub-contracting.
  - Assistance with incident management (at no additional cost).
  - Vendors taking part in the entity's security awareness programmes and operational resilience training.

- Entities must maintain information registers covering their contractual arrangements and report information to competent authorities **every three years** – and more often when engaging vendors for critical functions.

- **NEXT STEPS**: You should (1) put a process in place to review the provisions in its existing contracts with ICT vendors and identify those that need updating, and (2) ensure that new and updated contracts entered into from mid-2024 contain provisions that meet the DORA requirements.

Countdown to 2025

ROPES & GRAY

Mapping the Next 9 Months

- Although the requirements are different, you should leverage your GDPR compliance programme – and the experience gained through putting that in place – to inform your DORA strategy.

- **Given the impact DORA will have on you, it should be treated as seriously as the GDPR.**

- As a first step, we recommend taking the following actions :
  - Assess which business lines will be impacted and identify key stakeholders (internal and external).
  - Determine the extent to which current processes and procedures can be leveraged or updated.
  - Identify compliance gaps – both organisational and technical – and agree on remediation priorities.
  - Ensure that management is involved from the outset so it can help to play an active role in the journey.

- **TAKEAWAY**: Avoid burying your head in the sand. One year feels like a long time but our experience with the GDPR is that too many organisations left it too late – and some are still playing catch up…

How We Can Help

- Ropes & Gray has significant expertise designing and helping hundreds of asset management firms implement their privacy, data protection and security compliance programmes in the EU and UK.

- We also have deep experience in assisting our clients' investee companies with ongoing monitoring and remediation of their privacy, data protection and information security compliance programmes.

- In addition to ongoing GDPR and NIS1 work, we are already working with U.S. and EU asset managers to identify and plan for the measures that they need to take for DORA compliance.

- Several of these firms have a monthly "hotline" in place with Ropes & Gray for data privacy and security advice that they are now also using for scoping and assisting with DORA implementation.

Contacts

Rohan Massey
Partner
Rohan.massey@ropesgray.com
+44 20 3201 1636

Edward Machin
Counsel
Edward.machin@ropesgray.com
+44 20 3847 9094