INTELLIGENCE UPDATE

DORA update: what the EU act means for data centers

 Douglas Donnellan  Seb Shehadi

17 Apr 2025

The EU's Digital Operational Resilience Act (DORA), which took effect in January 2025, establishes strict digital resiliency and security requirements for financial entities (FEs). These include banks, insurance companies, investment firms and, for the first time, the data centers and third-party digital service providers they rely on.

EU-based data centers that host financial workloads, including those operated by colocation and cloud providers, can be subject to DORA's requirements. In-house data centers are regulated as part of the FE that owns and operates them. For the first time, regulators will also now directly oversee certain FE’s third-party service providers if they are designated as critical third-party providers (CTPPs).

CTPP designation is based on factors such as size, importance to the FE's operations, and the potential impact of disruptions to the EU financial sector. It is likely that each EU member state will designate five or fewer providers as CTPPs — only a few large companies will meet the criteria.

For example, a colocation provider hosting critical workloads for a single financial services client may not pose sector-wide risks in the event of a failure and could therefore avoid CTPP designation. In contrast, cloud and colocation providers hosting critical workloads for multiple FEs are more likely to be designated as CTTPs and become subject to direct regulatory oversight.

This designation process is currently underway. National financial regulators (i.e., Competent Authorities) in the EU must collect information from FEs about their relevant third-party providers, such as cloud, colocation, payment technology and managed service providers. Competent Authorities must submit these details to the European Supervisory Authorities (ESAs) by April 30, 2025, who will then determine which providers qualify as CTPPs by July 2025.

If they have not already done so, FEs will begin requesting resiliency details from their data center providers to ensure compliance with DORA. Third parties not designated as CTPPs will not face direct regulatory oversight but their financial clients may still require them to demonstrate

compliance with regulatory conditions. Those unable to do so risk being replaced.

Some service level agreements (SLAs) or other contracts may need to be amended. For example, if an FE determines that a third-party provider is "important" or "significant" to its operations, the contracts must include specific obligations outlined by DORA — such as availability guarantees, audit rights, and requirements for ongoing monitoring and incident reporting (see *Financial resiliency: how Europe plans to regulate service providers*). Since DORA requires FEs to manage risks from their third-party providers even if they are not designated as CTPPs, they may also impose stricter security measures alongside contract amendments.

DORA aligns with the Network and Information Security 2 (NIS 2) Directive, which specifies security obligations for essential digital infrastructure providers and came into effect in late 2024 (see *Are data centers on top of NIS 2 cyber compliance?*). However, unlike NIS 2, DORA mandates more extensive risk assessments and introduces direct regulatory oversight of third-party providers. This oversight can include inspections and requests for operational documents and details by ESA representatives.

Non-compliant entities may face daily periodic payments of up to 1% of their average daily global turnover in the preceding year, for up to six months, along with additional corrective actions mandated by regulators (see *Digital resiliency in finance: a regulatory review*).

Next steps for operators

Uptime Intelligence's research and conversations with industry practitioners suggest that many FEs have formed DORA-specific compliance teams and are working with their third-party providers to:

- Test cyber incident response systems and perform red team exercises.
- Consolidate contingency and exit plans, including procedures for data migration to alternative providers if a CTPP becomes non-compliant or insecure.
- Expand distributed resiliency strategies, including hybrid and multi-cloud approaches for hosting sensitive data.
- Further assess geopolitical risks in light of increased cyber threats from state-sponsored actors.
- Automate compliance processes through software.

DORA is more comprehensive than existing rules in the UK or US, featuring enforceable requirements and direct oversight of CTPPs. The UK relies on resiliency frameworks developed by the Financial Conduct Authority and Prudential Regulation Authority, while the US approach is more fragmented, with guidance spread across multiple regulators. However, growing operational risks may prompt the UK, US, and other countries to adopt approaches like DORA.

Data center operators and services companies that fall under DORA's scope can benefit from taking a proactive approach to compliance. This may include reviewing existing contracts with financial clients, strengthening backup and recovery systems through threat penetration testing, and reinforcing risk management frameworks.

DORA marks a shift in EU cybersecurity regulation by elevating a business-critical issue to one of national resiliency — systemic and concentration risks, for example, have become a major concern. This legislative approach highlights the growing dependence of national critical infrastructure sectors on digital services and the importance of mitigating a widening array of risks.

DORA recap: impact on financial services companies

- Strengthens and unifies regulations relating to digital infrastructure availability and resiliency across all EU member states.
- Makes third-party risk central to its regulatory approach.
- Covers all infrastructure servicing financial institutions, including data centers (design, operations and security).
- Requires comprehensive supply chain disclosure and risk management, audit and intervention rights, and frequent, in-depth testing.
- Regulatory oversight of certain data centers designated as CTPPs.
- Non-compliance can result in daily periodic payments of up to 1% of average daily global turnover.

Note: The regulatory analysis provided in this Update is the opinion of Uptime Intelligence. Data center operators should validate the interpretations with their legal staff and any relevant regulatory authorities.

ABOUT THE AUTHORS

Douglas Donnellan

Douglas is a Research Associate at Uptime Institute covering sustainability in data centers. His background includes environmental research and communications, with a strong focus on education.

ddonnellan@uptimeinstitute.com

Seb Shehadi

Sebastian Shehadi is Uptime Institute's Research Analyst for regulation, policy and legislation across the data center industry. Mr Shehadi has a decade's experience as a business journalist covering international investment and geopolitics, with a focus on the EMEA region. He has written for the Financial Times, BBC, New Statesman, Investment Monitor and many other publications.

sshehadi@uptimeinstitute.com

About Uptime Institute

Uptime Institute is the Global Digital Infrastructure Authority. Its Tier Standard is the IT industry's most trusted and adopted global standard for the proper design, construction, and operation of data centers – the backbone of the digital economy. For over 25 years, the company has served as the standard for data center reliability, sustainability, and efficiency, providing customers assurance that their digital infrastructure can perform at a level that is consistent with their business needs across a wide array of operating conditions.

With its data center Tier Standard & Certifications, Management & Operations reviews, broad range of related risk and performance assessments, and accredited educational curriculum completed by over 10,000 data center professionals, Uptime Institute has helped thousands of companies, in over 100 countries to optimize critical IT assets while managing costs, resources, and efficiency.