McCann FitzGerald

The EU Digital Operational Resilience Act: are you in scope of the new requirements?

16 September 2024

The Digital Operational Resilience Act[1] ("**DORA**") will apply on an EU-wide basis from **17 January 2025**. It will introduce comprehensive rules on digital operational resilience for in-scope financial entities. In preparation for DORA's entry into application, entities will need to assess whether they fall within the scope of the new requirements and, if they do, what steps are required.

This briefing will help entities determine if they may be within scope of DORA's requirements.

What are the core requirements under DORA?

At a high-level, DORA introduces uniform requirements concerning:

- ICT risk management;
- reporting of major ICT–related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities;
- digital operational resilience testing;
- information and intelligence sharing in relation to cyber threats and vulnerabilities;
- measures for the sound management of ICT third–party risk;
- requirements in relation to the contractual arrangements concluded between ICT third–party service providers and financial entities; and
- rules for the establishment and conduct of the oversight framework for critical ICT third–party service providers.

For a more detailed overview of the requirements under DORA, see our earlier briefings here and here.

What entities are in scope of DORA?

DORA applies to "financial entities", as defined under Article 2(1) of the DORA Regulation. They comprise the following entities:

- credit institutions;
- payment institutions, including payment institutions exempted pursuant to the Payment Services Directive ("**PSD2**")[2];
- account information service providers;
- electronic money institutions, including electronic money institutions exempted pursuant to the E-Money Directive[3];
- investment firms;

- crypto-asset service providers as authorised under the Markets in Crypto-Assets Regulation ("**MiCA**")[4] and issuers of asset-referenced tokens ("**ARTs**");
- 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; and
- securitisation repositories.

ICT third-party service providers will also be subject to DORA.

It should be noted that DORA will apply in a proportionate manner, taking into account a financial entity's size and overall risk profile, and the nature, scale and complexity of its services, activities and operations.

The following entities have been exempted from the scope of DORA, pursuant to Article 2(3) of the DORA Regulation:

- managers of alternative investment funds that qualify for the exemption under Article 3(2) of the Alternative Investment Fund Managers Directive[5] ("**AIFMD**");
- insurance and reinsurance undertakings that qualify for the exemption under Article 4 of the Solvency II Directive[6];
- institutions for occupational retirement provision ("IORPs") which operate pension schemes which together do not have more than 15 members in total;
- natural or legal persons exempted pursuant to Articles 2 and 3 of the Markets in Financial Instruments Directive[7] ("**MiFID II**");
- insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises or small or medium-sized enterprises; and
- post office giro institutions as referred to in Article 2(5), point (3), of the Capital Requirements Directive[8] ("**CRD IV**").

What steps should be taken by entities to ensure compliance with DORA by 17 January 2025?

Given the scale of the new requirements, and the impending application of DORA, preparations by in-scope financial entities should be well underway, to ensure full compliance by 17 January 2025.

Steps that entities may have already taken, or may consider taking, include:

- establishing a DORA implementation team which benefits from management support and buy-in;
- conducting a gap analysis of existing ICT risk management frameworks against DORA requirements;

- reviewing ICT contractual arrangements, assessing ICT third-party risk (for more information on this point, see our briefing here);
- commencing engagement with ICT third-party service providers, as required; and
- commencing the process of conducting a thorough cyber hygiene review.

How can we help?

McCann FitzGerald LLP is a premier law firm in Ireland and stands ready to assist in-scope entities, as they prepare for full compliance with DORA by the deadline of 17 January 2025. For assistance, please get in touch with one of the below key contacts, or your usual contact at the firm.

Also contributed to by David O'Keeffe Ioiart, Isobel Murphy and Eunice Collins

---

1. Comprising Regulation (EU) 2022/2554 (here) and Directive (EU) 2022/2556 (here).
2. Directive (EU) 2015/2366.
3. Directive 2009/110/EC.
4. Regulation (EU) 2023/1114.
5. Directive 2011/61/EU.
6. Directive 2009/138/EC.
7. Directive 2014/65/EU.
8. Directive 2013/36/EU.