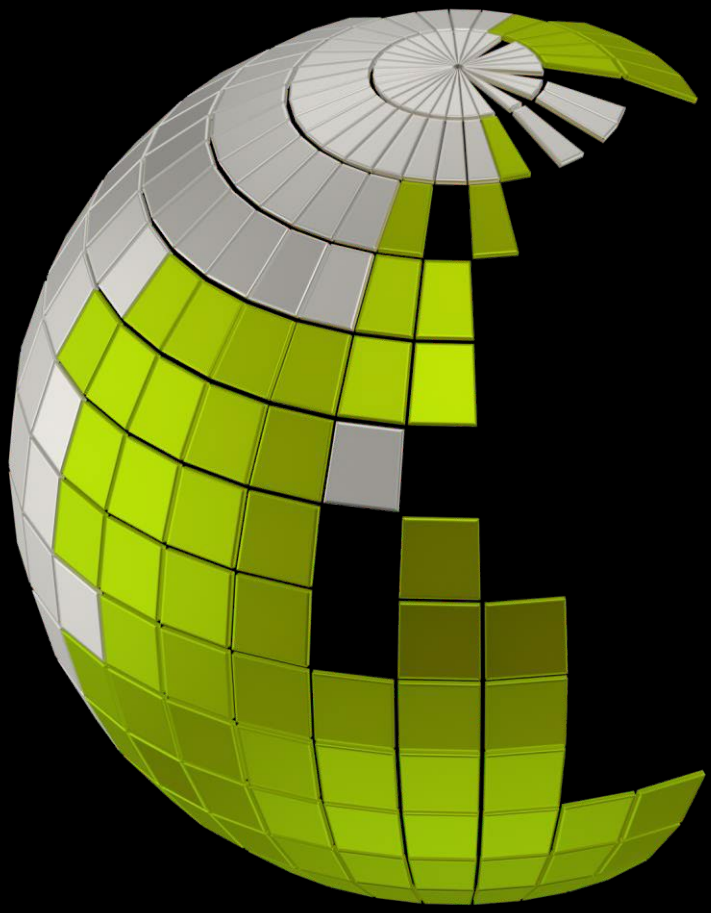
Deloitte.
Legal



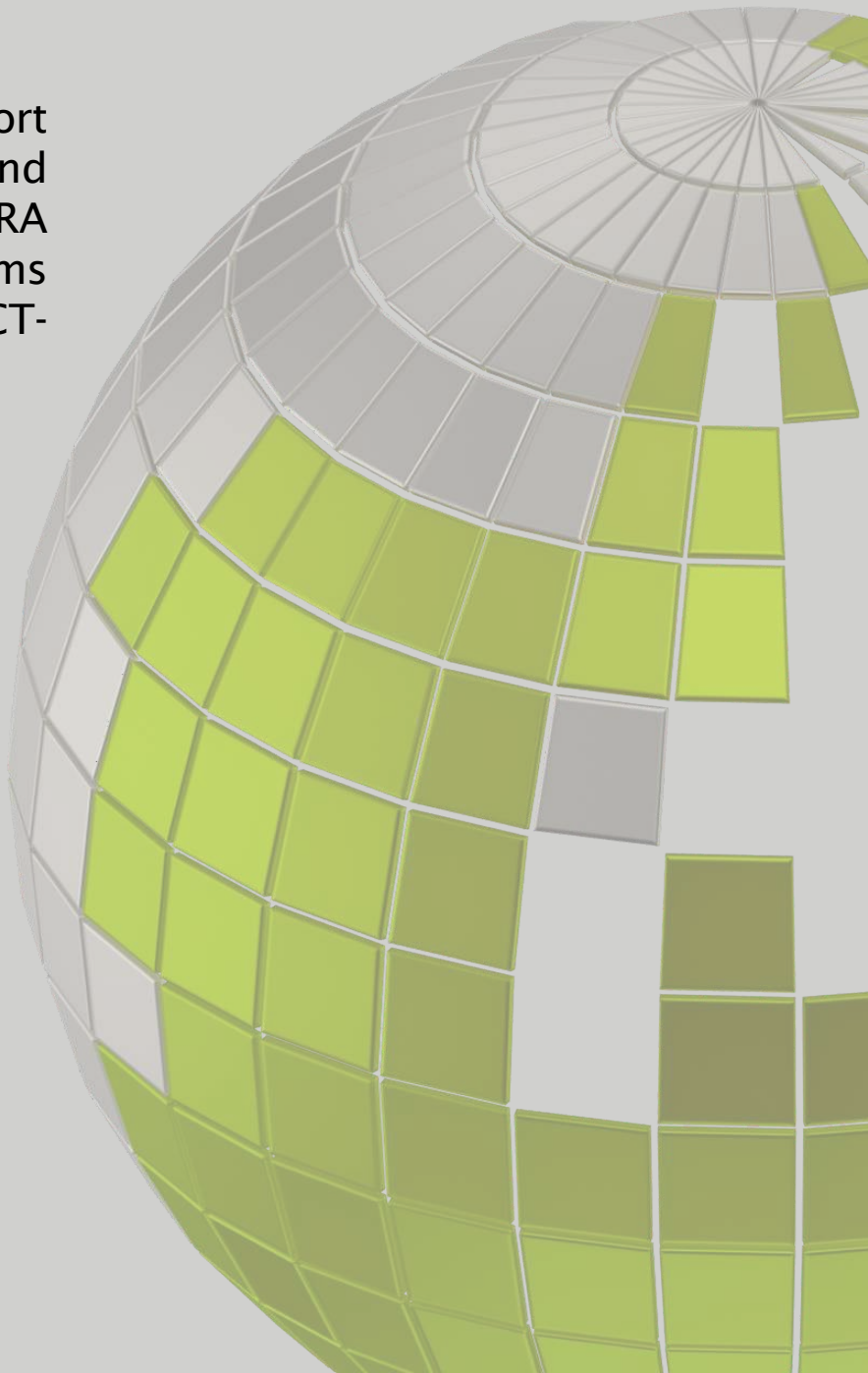
DORA

Getting your contracts ready

July 2024

After adoption of the European Union's Digital Operational Resilience Act ("DORA") on 20 November 2022, the Council of the European Union and the European Supervisory Authorities have begun the process of developing the relevant underlying technical standards, companies that operate in the financial services sector in the EU will be looking to understand how DORA could impact them.

This article provides a short overview of the scope and contractual implications DORA has for financial services firms and third parties offering ICT-related services.



Background

DORA is a wide-ranging piece of legislation, aimed at increasing the resilience of the EU's financial services sector by ensuring firms are able to withstand, respond to, and recover from, all types of information and communications technology ("ICT") related disruptions and threats.

It was initially proposed in September 2020, as part of a broader package of measures which also address digital finance, markets in crypto-assets and proposals regarding uses of distributed ledger technology.

A key part of DORA is the requirement for specific contractual terms to be included in each agreement with an ICT supplier. The requirements will be familiar to those working within the financial services sector, as similar requirements exist in relation to outsourcings by EU regulated firms, as set out in various guidance and regulation including:

- the European Banking Authority 'Guidelines on outsourcing arrangements' ("*EBA Outsourcing Guidelines*"), which require credit institutions, investment firms, payment institutions and e-money institutions to comply with;
- European Securities and Markets Authority 'Guidelines on outsourcing to cloud service providers', which apply to AIFM and AIFs, UCITS, management companies and depositaries of UCITS, central counterparties, central securities depositories, credit rating agencies, etc.
- the National Bank of Belgium's circular 2019/19 of 19 July 2019 regarding the EBA Outsourcing Guidelines, which applies to Belgian credit institutions, stockbroking firms, payment institutions, e-money institutions and Belgian branches of non-EEA credit institutions and investment firms.

Following the adoption of DORA in November 2022, entities which provide financial services within the EU now have until 17 January 2025 to ensure they meet the latest contractual requirements.

Scope

DORA targets businesses and organisations that operate in the financial sector as well as (critical) third parties that offer information and communication technology (ICT)-related services to financial entities.

1. **Financial entities:** all financial market participants, including but not limited to credit institutions, payment providers, investment firms, securitization repositories, intermediaries, etc.

2. **Third-party ICT service providers:** providers of digital and data services through ICT systems to financial entities, including software, hardware services, technical support; firmware updates, …

   Examples of such ICT providers are providers of SAAS, outsourcing, fraud management, collaborative tools, data storage solutions, CRM, etc.

Dora has an **extra-territorial component**, meaning that entities outside of the EU providing ICT services to financial entities within the EU will be required to comply with its provisions.

Outside outsourcing

A key difference between the requirements DORA imposes on contracts and the position set out in the EBA Outsourcing Guidelines is that DORA applies to contracts for all “ICT services”, not only to outsourcings. ICT services is defined very broadly in DORA, as:

> *digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services*

Whereas outsourcings are defined in the EBA Outsourcing Guidelines as "*activities that would be undertaken by the relevant financial institution if it was not procuring the service from a supplier*", ICT services under DORA has no such limitation.

As such, EU institutions are likely to need to revise contracts which have previously been considered to fall outside the regulatory requirements applicable, because they do not qualify as “outsourcing”.

Critical and important functions

As with the EBA Outsourcing Guidelines, there are two levels of contractual requirements under DORA. One applies to all contracts for ICT services, and the other to **contracts for ICT services which are "critical or important functions"**. This is defined in DORA as:

> *"a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law."*

Whilst very similar to the definition of "critical or important functions" in the EBA Outsourcing Guidelines, the terms are not identical.

Firms will need to verify whether their existing categorisations capture all of the ICT contracts which are for critical or important functions under DORA, to ensure that the correct contractual terms are included.

Mandatory contractual terms

As with the EBA Outsourcing Guidelines, DORA does not set out full form clauses to be copied into all contracts, but instead sets out elements the contract must address.

Whilst some of these are terms which would typically be included in any properly drafted ICT contract, such as requiring a full description of the services, or identifying whether sub-contracting is permitted, others may not be in supplier's standard terms or in regulated firm's templates. These include:

- requirements that the ICT service provider deliver assistance at no cost, or a cost which is determined or estimated in advance (DORA uses the Latin phrase "ex ante", leaving the exact requirement open to interpretation), when an ICT incident related to the ICT service occurs;
- conditions for the supplier to participate in the relevant firm's ICT security awareness programmes and digital operational resilience training; and
- for critical and important functions, requirements that the service provider participate and fully cooperate in the financial entity's threat-led penetration testing, which is a mandatory DORA requirement.

Whilst many of the topics covered by DORA's requirements will be familiar to organisations which have been through the exercise of updating their contracts in relation to the EBA Outsourcing Guidelines and/or the PRA Requirements in the past few years, DORA's requirements are sufficiently different that all ICT contracts will need to be reviewed to ensure compliance with DORA.

Other terms necessary for compliance

Whilst the mandatory contractual terms imposed in the EBA Outsourcing Guidelines and now DORA are the primary focus of most contractual remediation exercises, some organisations miss that other requirements of DORA may be best addressed contractually.

One example is "exit". Separately from requiring mandatory clauses relating to exit strategies in contracts for critical and important functions, DORA requires that firms must be able to exit all contracts without:

- disruption to their business activities;
- limiting compliance with regulatory requirements; and
- detriment to the continuity and quality of services provided to clients,

and exit plans must be comprehensive, documented and sufficiently tested and reviewed periodically. Many firms may need the support of their suppliers to meet this requirement and would be well served by including an additional contractual obligation to this effect.

Firms should ensure they understand the full implications of DORA for their ICT contracts before starting the amendment and negotiation process.

Stepping towards DORA compliance

There are clear steps that firms impacted by the DORA contractual requirements should now take:

1. Identify all contracts for ICT services.

2. Analyse those contracts and separate them into two categories: (1) ICT contracts for critical or important functions; and (2) all other contracts for ICT services.

3. Identify amendments required to align each contract with the applicable mandatory DORA requirements and any additional changes needed to allow the firm's compliance with other aspects of DORA.

4. Engage with suppliers to seek to agree necessary variations.

5. Where suppliers are not willing or able to agree to mandatory provisions, arrange for alternative services.

6. Update templates and playbooks to ensure all future contracts entered into comply with the relevant DORA requirements.

Contacts

Deloitte Legal's experience in advising on the contractual implications of regulatory changes, combined with our legal managed services capabilities, allows us to provide efficient solutions to contractual re-papering exercises, which take advantage of the latest technologies to drive speed, efficiency and accuracy of outcome. If you would like to discuss, please get in touch with us.

Els Van Poucke
Partner Commercial Contracts and Litigation
Brussels, Belgium
+ 32 2 800 71 54
evanpoucke@deloitte.com

Jan Roggen
Director Legal Operate
Brussels, Belgium
+32 2 800 70 41
jroggen@deloitte.com

Laurent Godts
Senior Director Banking & Finance
Brussels, Belgium
+32 2 800 70 63
lgodts@deloitte.com

Deloitte.
Legal

As a top legal practice in Belgium, Deloitte Legal - *Lawyers* is a full service business law firm, highly recommended by the most authoritative legal guides. Deloitte Legal - *Lawyers* is based in Zaventem, Watermael-Boitsfort, Antwerp, Ghent and Kortrijk. It consists of close to 150 highly qualified Bar-admitted lawyers. Deloitte Legal - *Lawyers* offers expert advice in the fields of banking & finance, commercial, corporate/M&A, employment, IT/IP, public/administrative, insolvency and reorganisations, real estate, EU law, tax law, tax & legal services for high-net-worth families & individuals (Greenille Private Client) and dispute resolution. Whenever required to ensure a seamless and comprehensive high-quality service, Deloitte Legal - *Lawyers* collaborates closely with other professions (e.g. tax, financial advisory, accountancy, consulting), and with a select group of law firms all over the world.
Deloitte Legal - *Lawyers* provides thorough and practical solutions tailored to the needs of clients ranging from multinational companies, national large and medium-sized enterprises, financial institutions, government bodies to private clients.
More information: **www.deloittelegal.be**