DORA's legal aspects: a practical guide for legal counsel

1. Introduction and purpose

The Digital Operational Resilience Act ("DORA") tightens the requirements for regulated firms in the financial sector concerning cybersecurity and operational resilience, and affects the ICT sector either indirectly or, for providers that are designated as critical, directly. As the full name of DORA itself suggests, some of the main challenges of the new regime will be of an operational nature. For a more fulsome treatment of the operational ramifications, we refer you to KPMG's dedicated DORA-portal.[1]

In this publication, after some introductory remarks, we will focus on those aspects of DORA that we believe benefit from an early involvement of either in-house or external counsel, along with some practical steps the legal function can take to ensure a smooth implementation. In our experience, the success of any regulatory implementation project – even in a highly technical area such as this – is greatly enhanced by a proactive involvement of legal counsel, especially during the initial stages of the project to sharpen gap or impact analyses and the drafting of business requirements. Strong legal interpretation and drafting skills are key during these important stages of your project. Additionally, DORA includes contract management and content requirements that we expect will need to be translated into a dedicated contract/repapering workstream on which legal counsel should take the lead, as well as training and various notification and consent requirements towards the regulator in which legal counsel also has an important role to play.

This publication is relevant both for financial entities as well as the ICT third-party service providers on whom they rely.

2. Background

DORA is part of the so-called digital finance package that also includes the EU digital finance strategy and three regulations including DORA, the Regulation on Markets in Crypto-Assets ("MiCA") and a sandbox regime for DLT-based market infrastructure. DORA's ambition is to create a holistic monitoring and control framework covering ICT risk management, incident reporting, continuity management and outsourcing/ contracting with ICT third-party service providers.

3. Scope

DORA applies to the financial sector as a whole (including banking, investment services, asset management, payments, insurance, financial market infrastructures and various other actors in the financial ecosystem), with limited exceptions, and impacts their ICT third-party service providers. As an indication of the scale of the impact on the latter, a joint high-level analysis conducted by the European Supervisory Authorities ("ESAs") together with the Competent Authorities ("CAs") identified around 15,000 ICT third-party service providers directly serving financial entities.[2]

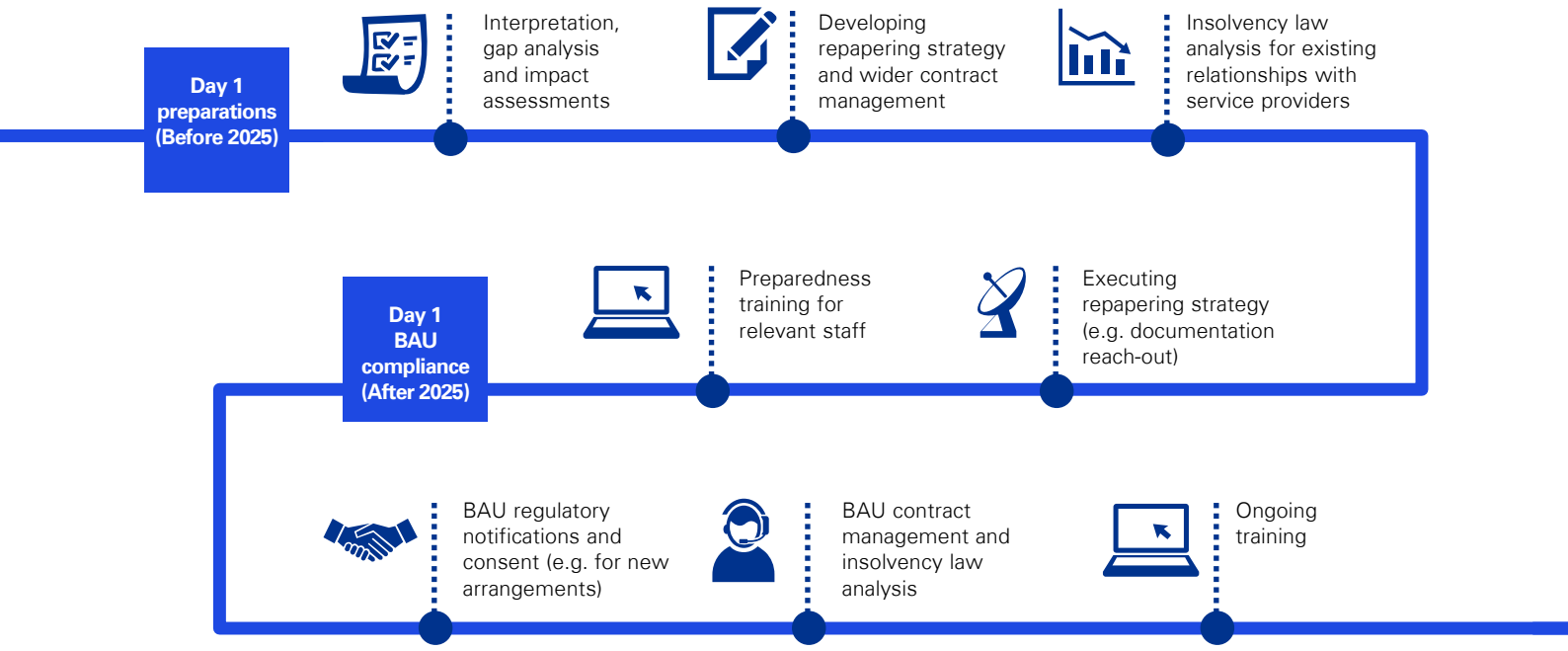
DORA stands to become a centerpiece in the current patchwork of EU rules on operational resilience for the financial sector. Most of the existing operational requirements at an EU-level are limited in either their personal or material scope, whereas DORA applies on a sector-wide basis and regulates the management of ICT risk, both internally and externally (with respect to third-party providers), comprehensively. For example, while PSD2 contains requirements relating to operational resilience (such as incident reporting measures, annual operational and security risk reporting and outsourcing requirements for operational functions), its application is limited to firms that provide payment services. Similarly, MiFID II contains detailed outsourcing requirements the aim of which is

1 See Prepare for DORA secure digital operational resilience - KPMG Belgium.
2 See ESA 2023 22 - ESAs report on the landscape of ICT TPPs.pdf (europa.eu).

to mitigate the operational and legal risks arising from a reliance on third party service providers, particularly where such reliance affects critical or important functions. As is the case with PSD2, however, MiFID II affects only a limited proportion of the financial sector, its application being limited to those firms that provide investment services (i.e. banks and investment firms).

The General Data Protection Regulation ("GDPR"), on the one hand, and the Network and Information and Security Directive 2 ("NIS2"), on the other hand, are not sector-specific. Their material scope, however, tends to have a specific focus or does not go far enough for the financial sector: GDPR centers on controlling and/or processing of personal data, whereas the aim of NIS2 is to protect organizations that can be characterized as critical infrastructure within the EU from cyber threats by enforcing a higher level of common security practices across the EU. As NIS2 and DORA's material scope overlaps, the entities in the financial sector to whom both regimes apply (e.g. financial market infrastructure and banking) only need to comply with the stricter DORA-standards. DORA does not entirely disapply NIS2 for the financial sector, though, as there are interactions between both regimes at the supervisory and reporting level.

4. Timing and secondary legislation



DORA was published in the Official Journal of the EU on the 27th of December 2022 and entered into force on the 16th of January 2023. The Act will apply from 17 January 2025 (24 months after it entered into force) leaving firms with a little over half a year to implement the operational requirements and repaper/amend existing contracts.

DORA will also come with a whole suit of secondary legislation in the form of commission delegated regulations (in most cases based on regulatory and implementing technical standards (respectively "RTS" and ITS")), two batches of which have been adopted (but yet to be published in the Official Journal) at the time of writing in April. The expectation is for most of the secondary legislation to be available by the Summer of 2024.

The secondary legislation adopted so far includes:

- Regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents. The RTS sets out the criteria to be applied by competent authorities for the purpose of assessing the relevance of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, to relevant competent authorities in other Member States, and the details of reports of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, to be shared with other competent authorities.
- Regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. The RTS provide that the policy regarding contractual arrangements on the use of ICT services supporting critical or

important functions provided by ICT third-party service providers should set out an appropriate and proportionate process for selecting and assessing the prospective ICT third-party service providers taking into account whether or not the ICT third party service provider is an intragroup ICT service provider.

- Regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework. In this respect, financial entities will have to, when testing the ICT business continuity plans, take into account its business impact analysis (BIA) and the ICT risk assessment.
- Delegated Regulations:
  - determining the amount of the oversight fees to be charged by the Lead Overseer to critical ICT third-party service providers and the way in which those fees are to be paid. The Delegated Regulation focuses on the specification of the applicable turnover that is to be used to calculate the fees to be charged to the critical ICT third-party service providers.
  - specifying the criteria for the designation of ICT third-party service providers as critical for financial entities. The designation criteria are further specified in relation to, among others, the systemic impact that a failure or operational outage of an ICT third-party service provider could have on the financial entities to which it provides ICT services and the criticality or importance of the functions supported by the ICT services provided by the ICT third-party service provider.

5. Areas of interest for the Legal Function

5.1. Interpretation, gap analyses and impact assessments

As noted above, DORA applies to a range of financial entities, most of which are already subject to some form of regulation on operational resilience – the extent to which they are, however, varies depending on the type of entity. For example, asset managers have to date been regulated more lightly in this respect than, say, banks or investment firms, and so are likely to face a more onerous implementation burden. One of the first exercises a legal function can organize and facilitate is a gap analysis of the existing ruleset against the future requirements of DORA. The outcome of this analysis should be to have a list of actions that can serve as a blueprint for any compliance roadmap or DORA implementation project that the financial entity chooses to launch.

Equally, non-regulated firms with clients in the financial sector may want to seek advice on whether they satisfy the definition of ICT third-party service provider. This turns on whether the entity provides ICT services, which is broadly defined 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." We suspect that out of the 15,000+ ICT third-party service providers the ESAs have identified, a significant proportion will not be deemed to be critical and, accordingly, will not be subject to the oversight of a "Lead Overseer". Nevertheless, we believe that any ICT third-party service provider stands to benefit from having a well-grounded internal view on the extent to which DORA applies to it, both at the definitional level and in terms of the articles that will impact them.

ICT third-party service providers will likely be facing a range of requests from their financial services clients from testing to repapering of existing contracts (as to which, see further below) as part of their implementation project. As such, the legal function of the entity (assisted by external counsel, as the case may be) may want to carry out an application and impact assessment for DORA, to ensure it is prepared to deal with any such requests as they come in. Such an assessment can also be used to inform any readiness packs the entity chooses to prepare for its business/commercial staff (e.g. Q&A documents or client talking points) or ICT contract negotiation guides.

5.2. Training

There are a number of provisions in DORA that expressly reference training. These include:

- Regular training for the management body to keep up to date on ICT risk and its impact of the operations of the financial entity; and
- Developing ICT security awareness programs and digital operational resilience training as compulsory modules in its staff (meaning all employees and senior management) training schemes – where appropriate and in accordance with the applicable contractual arrangements, ICT third-party service providers may even need to be included in the training scheme.

Depending on the organization, legal may or may not take the lead in developing such training sessions or modules, but it is likely to have a role in ensuring the contents match the requirements of the regulation, particularly for those sections that relate to legal documentation and regulatory liaison.

5.3. Regulatory liaison – Financial Entities

Several provisions in DORA require a financial entity to share information with, notify, or obtain approval from

the competent authority, including the following:

- Reporting the number of new ICT arrangements, categories of ICT third-party service providers, type of contractual arrangements and ICT services and functions which are being provided on at least an annual basis.
- Regarding ICT services supporting critical or important functions, informing the competent authority in a timely manner of any planned contractual arrangement.
- Notifying information-sharing arrangements with other financial entities.
- Seeking approval from the competent authority to use of internal testers to perform Threat Led Penetration Testing (where possible).

Especially for those reporting requirements relating to contractual arrangements, we expect that legal counsel will have an important role in gathering the relevant data and liaising with the competent authority. More broadly, legal counsel may also be involved in completing such other notification and/or approval forms as the competent authority requires for the occasion, and in taking the lead or providing input on resolving any follow-up queries from the competent authority.

We also note that DORA requires financial entities to assess the criticality of the services affected by an ICT-related incident, including whether it affects or has affected financial services provided by the financial entity that require authorisation, registration or that are supervised by competent authorities. The legal function is likely to play a crucial role in such an assessment, particularly with respect to the regulated nature of the affected service.

5.4. Regulatory Liaison – Critical ICT third-party service providers

For critical ICT third-party service provider, the ESAs through the Joint Committee will appoint a Lead Overseer. The Lead Overseer will be the ESA that is responsible for the financial entities that are most exposed to the critical ICT third-party service provider. DORA grants extensive powers to the Lead Overseer to request information, including all relevant business or operational documents, contracts, policies, documentation, ICT security audit reports, ICT-related incident reports, as well as any information relating to parties to whom the critical ICT third-party service provider has outsourced operational functions or activities. Importantly for the legal function, DORA permits critical ICT third-party service providers to authorize lawyers to supply this information on behalf of them. The legal function of the provider will have an important role in managing this process.

Finally, DORA also empowers the Lead Overseer to carry out investigations or onsite inspections – in principle, notice needs to be given of such inspections, unless this is not possible due to there being an emergency or crisis situation. As with any onsite inspection or dawn raid, legal counsel should be present to monitor the proceedings, advise the business and mediate any discussions with the Lead Overseer. (The same logic applies to any such action undertaken in relation to financial entities, although DORA is less prescriptive as to the powers of competent authorities than it is for Lead Overseers, as financial entities are already regulated and subject to supervision and potentially pre-existing investigatory and sanctioning powers.)

5.5. Contract management, contract review and repapering (including specific requirements in relation to providers in third-countries)

As part of DORA risk management framework, financial entities are expected to maintain a register of information in relation to all contractual arrangement on the use of ICT services. In addition, DORA expects financial entities to:

- conduct due diligence on any ICT third-party service provider ;
- adopt a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers in order to set out certain key principles to manage ICT third-party risk, to specify the planning of contractual arrangements, including the risk assessment, the due diligence, the approval process for new or material changes to those contractual arrangements and to specify an appropriate and proportionate process to select and assess the suitability of prospective ICT third-party service providers;
- monitor on an ongoing basis the contractual arrangements regarding the performance of ICT third-party service providers, including measures to monitor compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information, and the compliance of the ICT third-party service providers with the financial entity's relevant policies and procedures;
- consider the use of standard contractual clauses on mutual obligations of the financial entities and the ICT third-party service providers which reflect the right for the financial entity to access information, to carry out inspections and audits, and to perform tests on ICT whereby the aforementioned policy sets out the framework to ensure that material changes to these standard contractual clauses are formalised in a written document; and
- ensure the contractual arrangement in place on the use of ICT services reflects certain key contractual provisions – note that DORA applies to all ICT contracts, not just to those qualifying as outsourcing.

We expect that these minimum content requirements

will result in an extensive repapering exercise for which preparedness is key. Legal counsel is likely to need to be involved in making an inventory of existing contractual arrangements and developing a multi-option repapering strategy along with an analysis of the associated risks and mitigants for each option (e.g. contract-by-contract negotiation, one-way amendments through a 'patch' or side-letter, working with newly developed standard clauses etc.). Legal counsel will also need to raise resourcing needs (FTEs) for any resulting contract negotiations early on with DORA project management, including the need for external resource both in staffing the negotiations and/or developing tools to facilitate the negotiations (such as a negotiation guide with fallback options in the event of pushback).

In addition, DORA requires financial entities to adopt and regularly review a strategy on ICT third-party risk. That strategy is to include a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers which needs to be reviewed by the management body of the financial entity. The legal function of the entity is likely to need to be involved with the drafting of the policy that assigns the internal responsibilities for the approval, management, control, and documentation of relevant contractual arrangements.

Finally, critical ICT third-party service providers established outside the EU will need to establish a subsidiary in the EU. The resulting transfer of legal arrangements or repapering will also need to be carefully managed both from the perspective of the provider and the financial entity. More generally, contracting with third country service providers gives rise to a number of additional checks that need to be performed, including as to what the impact would be on compliance with EU data protection rules and the effective enforcement of the law in that third country.

5.6. Contract review/drafting for TLPT Testers

Financial entities need to carry out advanced testing by means of Threat Led Penetration Testing (TLPT) at least every three years and contract testers for this purpose. When internal testers are used (where permitted), a financial entity needs to contract external testers every three tests. Some of the requirements in DORA relating to these tests will need to be reflected in the underlying contract between the financial entity and the tester – for example, for external testers, the financial entity needs to ensure that the contract requires a sound management of the TLPT results and that any attendant data processing does not create risks to the financial entity.

5.7. Insolvency law analysis

For contracts supporting critical or important functions, DORA requires financial entities to consider the insolvency law provisions that would apply in the event of the bankruptcy of an ICT third-party service provider as well as any constraints that may arise in respect of the urgent recovery of the financial entity's data. Legal counsel will need to reflect on the form this 'consideration' should take – absent further guidance, this may mean seeking external counsel advice or a formal insolvency law opinion to support these contractual arrangements.

6. Conclusion

Both KPMG and the lawyers of KPMG Law are here to help, whether you have yet to launch your DORA implementation project or are already well-advanced along your DORA trajectory. Please contact us in case you have any questions or would like to discuss.

Contact

Isabelle Blomme
Partner Banking & Finance
KPMG Law
iblomme@kpmglaw.be

Joris Latui
Senior Counsel - Banking & Finance
KPMG Law
jlatui@kpmglaw.be

kpmg.com/be
kpmglaw.be