DORA series episode 2:

Implications for technology service providers

Heenal: Welcome to the second episode in the Allen & Overy podcast series on the European Union's Digital Operational Resilience Regulation, known as DORA. Our two part series looks at the implications of DORA for both financial entities and technology providers. I'm Heenal Vasu, a senior Professional Support Lawyer in Allen & Overy's financial regulation practice, and in this second episode I'm joined by Ben Regnard-Weinrabe, who co-leads our fintech practice in London, and Catherine Di Lorenzo, who leads our Data and Tech practice in our Luxembourg office. We're going to discuss the changes that DORA will bring for technology service providers in the EU, and some of the practical steps that these service providers should take to prepare.

But first, Ben, how are technology providers caught by DORA?

Ben: Many thanks, Heenal. To begin with some background.

DORA is part of a *broader Digital Finance Package* which was published by the European Commission in September 2020 and that package aims to foster *sustainable* innovation and competition in the EU, which are laudable aims.

DORA itself sets a regulatory framework for financial entities and their so-called *Information and Communication Technology – or "ICT" – third party service providers*. The regulatory framework under DORA is intended to mitigate the *risks from digitalisation* of a range of financial and related services.

DORA supplements, most notably, the existing EU financial services *outsourcing* regime, which imposes obligations on *regulated* financial entities *rather* than on their service providers directly.

The financial entities are then expected to apply the outsourcing requirements *indirectly* to their service providers through *contractual* and *oversight* arrangements under the outsourcing regime.

DORA, however, departs from that traditional approach to financial services regulation, in that it imposes obligations *directly* on *critical* ICT service providers.

However, DORA *will* also, similarly to the outsourcing regime, have an *indirect* impact on *non-critical* ICT providers.

Heenal: Thanks, Ben. Catherine, could you explain a little more which technology providers will be caught by DORA?

Catherine: DORA will apply to critical service providers, as just mentioned by Ben, and to those providers who provide digital and data services to financial entities, and financial entities are very broadly defined by DORA. They include not only banks and investment firms, but also insurance companies, managers of alternative investment funds, credit rating agencies and the like. The digital and data services covered by DORA include cloud computing services,

software or, for instance, data analytics services. The regulation will not apply to providers of hardware or telecommunications services.

As Ben just mentioned, DORA will only directly apply to critical service providers. The regulation sets out a list of criteria that supervisory authorities must take into account when assessing whether such a provider is “critical” and the criteria look not only at the role and importance of the financial institution but also at the role and importance of the service provider. The criteria that we look at are:

- the systemic impact on the provision of financial services if the ICT third-party service provider suffers a large-scale operational failure;
- the systemic character or importance of the financial entities that rely on the ICT third-party service provider;
- the reliance of financial entities on the same service provider in relation to several critical or important functions of these entities;
- whether the service provider can be easily substituted; and
- the number of Member States in which the services are provided and the number of Member States in which financial entities using the relevant ICT third-party service providers operate.

Even if a supervisory authority does not designate a service provider as critical, the service provider can request to be included in the list of critical providers.

But, as Ben mentioned, non-critical service providers will still be indirectly impacted by DORA because of the contractual obligations that financial entities must impose on them according to the regulation.

Heenal: Thank you, Catherine. Ben, what does it mean for ICT third-party service providers if they are considered as critical?

Ben: Well, *designated* critical ICT providers will become directly supervised entities.

Specifically, one of the European supervisory authorities would become the Lead Overseer for a designated critical provider. Now the European supervisory agencies include the European Banking Authority (the EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA), and as to which would be the Lead Overseer for a particular critical service provider we’d expect that to depend upon which sector the service provider is serving.

The job of the Lead Overseer is to ensure that the critical ICT provider has effective *rules*, *procedures and mechanisms* to manage the risks that it may pose to the financial entities depending on it.

It has a number of powers and they include

- the Lead Overseer being given access to information, business and operational documents, contracts and policies insofar as necessary for the Overseer to perform its duties; and
- the ability for the Lead Overseer to conduct on-site inspections of any premises of the critical ICT provider, and so indeed those powers of the Lead Overseer are quite invasive.

As to the obligations on the critical ICT provider itself…well, it would be obliged to cooperate "in good faith" with the Lead Overseer and to pay oversight fees.

In addition, worth noting that DORA precludes EU financial entities from using a critical ICT provider incorporated outside of the EU. Now while some might see this as protectionist, it can potentially be addressed by setting up an EU-incorporated operating company.

Happily, the incorporation requirement does not also necessarily mean that data storage or processing functions of that critical service provider also need to take place within the EU. It seems those activities could take place outside of the EU but in which case, in our view, the Lead Overseer's oversight powers, including to conduct on-site inspections, could extend to any premises and systems located outside of the EU.

Heenal: Thanks, Ben. So, Catherine, what do critical technology service providers need to do in practice?

Catherine: Unlike the rules for financial entities, which were discussed in episode one of our podcast series, DORA does not foresee rules directly addressed to third-party service providers. But by saying that the Lead Overseer must assess that effective rules and procedures are implemented, as Ben just explained, critical service providers need to make sure that they have implemented security measures, including for access to their premises, have a risk management process, including ICT risk management policies, business and disaster recovery plans and governance arrangements. They must also be able to identify, monitor and report ICT incidents and resolve those, perform testing and audits, and so on. So, you see, the obligations are rather broad. In essence they must therefore implement similar measures as those that are imposed on financial entities. Where DORA does not provide more details on these requirements when applying to critical ICT service providers, the detailed rules foreseen for financial entities can be used as a benchmark for the measures, procedures and policies that the service providers should implement.

Ben: An important point here is that supervisory authorities could conceivably require financial entities to suspend or even terminate their use of a critical service provider until risks identified in a Lead Overseer's recommendations to the service provider have been addressed.

So therefore not complying with DORA requirements could have a major impact on the activities of a critical service provider.

Heenal: Thanks very much, both. Separately, you mentioned that DORA also indirectly applies to non-critical service providers. Could you explain how?

Ben: In our first podcast, we described many of the obligations that will apply to financial entities under DORA.

To give a selection here, when using an ICT service provider a financial entity will need to *ensure* that the service provider enables the financial entity itself to comply with its ICT risk management obligations imposed by DORA.

Consequently, the financial entity will need to perform due diligence and impose certain *mandatory* contractual obligations on its service provider, irrespective of whether the service provider is critical or not.

Heenal: Thanks, Ben. Could you provide a few examples of contractual obligations that DORA will impose?

Ben: Sure. Many of the contractual requirements that a financial entity would need to impose on its ICT provider will already be familiar from, for example, the EBA guidelines on outsourcing, or similar requirements. For example:

- contracts would need to include a clear description of the services to be provided by an ICT service provider, and related service levels;
- there would need to be appropriate termination rights and mandatory transition periods;
- audit rights for the financial entity; and
- of course, obligations for the service provider to cooperate with the financial entity's supervisory authority.

Those are generic obligations. Some obligations are more specific to ICT risks, such as:

- a requirement to implement and test business contingency plans; and
- an obligation for the service provider to provide assistance, in the event of an ICT incident, to the financial entity, such assistance from the service provider to be at either no cost to the financial entity or at a contractually pre-agreed cost.

Catherine: I think this latter requirement will be a challenge for service providers in practice. Actually we know that it is extremely difficult to foresee all costs for ICT incidents beforehand. Let's take the example of a major cyberattack, which can generate very significant costs. It is impossible to foresee all of those beforehand, so the question is if it is sufficient for the service provider to determine the costs right after the incident occurred, which would already be difficult enough, but the wording of DORA seems to go against such an interpretation.

Heenal: Thank you. Does DORA foresee any sanctions for ICT third-party providers and if so, in which cases?

Ben: DORA doesn't have regulatory sanctions for non-critical service providers.

However, for critical service providers, administrative sanctions can be imposed if the service provider:

- doesn't provide requested information to its Lead Overseer; or
- submit itself for investigation or on-site inspections by that Overseer; or
- indeed doesn't address recommendations issued by their Lead Overseer (and those recommendations could be, for example, as to implementation of security requirements or in relation to subcontracting to providers outside of the EU).

DORA itself is not prescriptive as to the sanctions which can be imposed. This is largely left to EU member states to determine and so we could see potentially a diverse variety of sanctions and practice across the EU.

Heenal: What comes next? Should ICT providers already take steps to prepare for DORA?

Ben: The proposal is now going through the EU's ordinary legislative procedure and the aim is to have the regulations in the EU Digital Finance Package, including DORA itself, in full effect by 2024.

Catherine: While this sounds far away ICT service providers, especially those who will likely be critical, should start looking into DORA already now. They can start by assessing whether they are critical, based on the criteria set out in DORA, and then undertake a gap analysis to assess which requirements they do comply with already today and then draft the business, strategy and financial plans to cover the gaps they will need to close to comply with DORA.

Ben: Absolutely agreed, Catherine. Processes, policies and procedures may need to be adapted, new operating companies may need to be set up.

With all the organisational and resourcing requirements that that implies, it's not too early to start planning for this now.

Heenal: Catherine, Ben, thank you both very much. That brings us to the end of this episode. As ever, if listeners have any questions about DORA, or indeed requests on what you would like us to cover in future podcasts, then please do contact us by phone or email, and of course do check out our dedicated website on the European Digital Finance Package. All that remains to be said is thank you for listening and goodbye.

Speakers

Ben Regnard-Weinrabe
Partner
Fintech & Payments
Tel +44 20 3088 3207
ben.regnard-weinrabe@allenovery.com

Catherine Di Lorenzo
Counsel
Data & Tech
Tel +352 44 44 5 5129
catherine.dilorenzo@allenovery.com

Heenal Vasu
Senior PSL
Fintech & Payments
Tel +44 20 3088 1447
heenal.vasu@allenovery.com