AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

DORA: Potential overlaps with other legislation and implementation challenges

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive summary

American Chamber of Commerce to the EU (AmCham EU) is a strong supporter of the Digital Operational Resilience Act (DORA), as it brings clarity to the applicable cybersecurity rules for the regulated financial services sector and its Information and Communication Technology (ICT) service providers. In order for the industry to adopt a consistent set of high-quality standards and practices globally in this regard, the European Commission and European Supervisory Authorities (ESAs) should foster international cooperation and collaboration.

The following document highlights the overlaps between DORA and other EU legislation, outlines industry concerns stemming from these links and explains the potential challenges that might arise during DORA's implementation. Concerns of our members are particularly related to the following two aspects:

1. The overlap and potential inconsistencies between DORA and other existing or proposed EU cybersecurity legislation.
2. The lack of legal certainty and clarity on definitions when it comes to DORA's implementation.

1. Potential overlaps and inconsistencies between DORA and other legislation

The link between DORA and the planned EU Cloud Providers Certification Scheme (EUCS)

Background

DORA has been recently published in the Official Journal, but even before it became EU law, the European Commission and Member States were advancing new and related proposals, notably on cloud certification and the Cyber Resilience Act. These proposals could potentially amend some of the existing provisions in DORA and the second Network and Information Security Directive (NIS2), which would undermine the importance of DORA as a *lex specialis* for the financial services sector.

In regard to cloud certification – and in line with the already adopted Cyber Security Act from 2019 – the European Union Agency for Cybersecurity (ENISA) has started work on three certification schemes, including one dedicated to certifying Cloud Services (EUCS). In this context, some Member States have called for the inclusion of data localisation and European headquartering or ownership requirements for cloud service providers seeking the highest level of assurance of the EUCS certification. Financial services will, in all likelihood, fall into the highest level of assurance of cybersecurity certification.

ENISA will deliver a candidate scheme of the EU, that must be transformed into an EU Implementing Act by the European Commission. In advance, EU Member States should continue to engage with ENISA and the Commission through the European Cybersecurity Certification Group (ECCG), a public certification expert group. It has become a public debate that 27 EU Member States are not aligned on the inclusion of the above mentioned requirements on data localisation and ownership. We understand the latest draft will be discussed by the Member States sometime in January 2023. Hence, policymakers should consider using DORA's approach, which explicitly provisions that data localisation obligation is not imposed as it does not require data storage or processing to be undertaken in the EU.

Concerns in relation to the EUCS

- While the EU Implementing Act is meant to address technical standards, it could be potentially used to enforce political decisions on EU sovereignty, which could lead to the fragmentation of capital markets and make it harder for global financial institutions to manage their risk exposures, voiding DORA of its practical positive effects.

- The EUCS' development process is not transparent. There was an ENISA-led public consultation in 2021, but both the substance and political context have completely changed since, notably through the inclusion of ownership and localisation requirements opposed to DORA and the NIS2 Directive.
- The certification, as currently proposed, could have a number of unintended effects:
    - Force the use of certain technologies and providers, which potentially adds complexity and risk to the operations of cloud users such as financial services.
    - Force onshoring ICT providers in a way that was directly rejected in DORA.
- These provisions of the EUCS could negatively impact the availability of innovations and different cloud services in Europe, which would limit actions on security protections and potentially harm security objectives.
- The EUCS could lead to increased fragmentation of the cybersecurity requirements across the EU in case EU Member States are not aligned on the set of harmonized requirements. This will in particular affect (critical infrastructure) sectors in scope of the NIS2 that require a high level of certification.

The link between DORA and the proposed Cyber Resilience Act (CRA)

Background

The proposed Cyber Resilience Act creates a set of minimum requirements for products and software destined for the European market. The type of requirements depend on the design of the respective products, and the producers of basic products will have to self-assess and conform. Critical products require a conformity assessment and common EU standards, while highly critical products require full conformity assessment. An added challenge is that the respective standards have not yet been defined. This will create delays and bottlenecks.

The scope of the proposed Cyber Resilience Act is also extremely wide. As a result, it is likely that a number of financial services, products and software will be deemed critical or highly critical. Such products and software are now governed by DORA, meaning the CRA creates direct duplication in areas such as incident reporting and vulnerability management. Duplication undermines the core objective of DORA which was to create a single harmonised rule book for cyber and ICT risk management.

Concerns in relation to the proposed CRA

- Given the potentially very broad scope of CRA, the proposed certifications under this Act could overlap with measures that DORA or the Lead Overseers may recommend on ICT providers, thus potentially leading to duplications or even inconsistencies. The proposed CRA makes cross-references to the NIS2 Directive, but it does not do so with DORA. Including these references and identifying DORA as lex specialis is crucial to ensure regulatory certainty.
- If a product or application is deemed critical or highly critical, the provider has to go through conformity assessments before entering the European market. While this will help remove some complexity in the product approval process, it also makes the EU a harder place in which to do business.

2. DORA's implementation

The functioning of the DORA oversight regime will determine which third parties ICT providers will be labelled as critical under DORA. This decision is left to the ESAs based on a Delegated Act to be drawn up by the European Commission.

As part of DORA's implementation process, ESAs have begun working on a methodology by collecting data from financial entities on their third-party ICT providers. They have conducted a one-off voluntary survey for financial entities across the EU to obtain information on all third party ICT providers and technology providers with a two-

months deadline for responses. The definitions used in the survey, such as that of a third-party provider, come from DORA. However, in some cases there are no DORA definitions.

Therefore, while DORA has introduced proportionality by striking the right balance between rule consistency, supervisory efficiency and cooperation, such proportionality should also apply to the scope of the forthcoming oversight of critical ICT third-party service providers (CTPPs). This is particularly important given the breadth of the definition of ICT services, which in turn brings the need for a clear set of supplementing CTPP designation criteria under DORA's article 31. That raises questions such as: Is it linked to critical functions in a recovery and resolution context of a financial institution? Does it relate to critical infrastructure in the customer-facing front office or the maybe more systemically relevant application of back office services within a financial institution?

Concerns in relation to DORA's implementation

- Current publication schedule for DORA's regulatory technical standards (RTS) may not allow financial entities adequate time to safely comply. While DORA allowed 24 months for financial entities to comply with its rules, a number of the requirements will be clarified through the RTS, which will only be published in the coming 18 months. In some instances, these RTS cover highly technical areas such as requirements related to cryptographic techniques. It is highly unlikely that financial entities will be able to safely make such technical changes in the timelines allowed. Therefore, national competent authorities should be prepared to grant allowances to the firms they supervise.
- Registers of third parties: This approach has been tried by different regulators in various ways. Collecting data on third party ICT providers has proved to be much more complex than it would appear and also affects the management of supply chains and sub-outsourcing. High levels of cooperation with the industry to develop meaningful data fields are required to ensure an effective register.
- DORA does not provide a clear definition of 'criticality' and a sufficiently clear list of criteria that would help to appropriately anticipate which third-party ICT providers would be deemed as 'critical third party ICT providers' (CTPP). This means it is unknown which third party ICT providers will be captured by the oversight framework under DORA, making it very challenging for a financial services institution or ICT provider to currently plan for their cyber strategy, investments and legal entities structure.
- While DORA foresees that the oversight (particularly the Lead Overseer's oversight plans) will primarily focus on ICT services used for critical or important functions of financial entities, the provisioned CTPP designation mechanism is in theory meant to appoint a provider in its entirety. It would be inefficient if the Lead Overseer focuses its oversight powers over all the services provided by a CTPP, including those which are not used by financial entities for critical and important functions (or those services which are not relevant at all, think for example of gaming or advertising services), simply because one or more services provided by the CTPP are used for a critical or important function of a financial entity. Therefore, the Commission and the ESAs should consider the need for efficiency when refining the parameters for the CTPP designation in the forthcoming act in order to concentrate the efforts of both the CTPPs and the oversight bodies on critical or important functions that effectively matter for the stability of financial entities.
- Industry participants continue supporting the harmonisation of requirements across regulations and the intention of the ESA's the ensure DORA remains *lex specialis* over NIS II. There should not be conflicting rules that apply to firms while seeking to result in the same outcomes. ESA should remain mindful concerning any fragmentation in requirements throughout the development of standards.
- Threat-led penetration testing should be aligned with existing Threat Intelligence-based Ethical Red Teaming (TIBER-EU) standards and be applicable across all EU Member States. Firms should not be required to test on multiple occasions across Member States. The industry continues to support all attempts to harmonise testing globally with recognition of tests across regulatory jurisdictions.
- There are multiple requirements on third party ICT providers in relation to their cooperation with and disclosure to the financial services institutions. This has contractual implications. When third party ICT providers find out that they are designated as critical, every financial services institution that is a customer

of that ICT provider will need to renegotiate their contracts with that provider in a very short period of time, which will create severe challenges.

Conclusion

DORA is crucial to obtain clear guidelines for the cybersecurity rules applicable to financial services. However, the legislation overlaps with other existing or proposed EU cyber security legislation and lacks clarity in some of its definitions. For the industry to successfully adopt high-quality standards and practices, several concerns should be addressed. For instance, policymakers should prevent any inconsistencies between DORA, EUCS and CRA. Furthermore, with regards to the concept of criticality, the relevant criteria must be clarified further during the implementation process in order to ensure legal certainty. Finally, national competent authorities should consider what allowances they are prepared to provide financial entities as they work under constrained timelines to become compliant.