AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

DORA – reaction to amendments

Reaction to ECON amendments to the draft report on the Digital Operational Resilience Act proposal

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3 trillion in 2020, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

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

Reaction to ECON amendments to the draft report on the Digital Operational Resilience Act proposal

The Digital Operational Resilience Act (DORA) represents a good step towards a harmonised EU framework for digital resilience in financial operations, making the system both robust and future-proof as well as ready for the challenges of digitisation.

As the voice of American business invested in Europe, AmCham EU emphasises the transatlantic dimension and the need for a coordinated international approach to ICT risk management. The issues addressed in our position paper include recommendations from the banking sector, the cloud and software industry, as well as a data aggregator perspective of the framework.

Further to the amendments to the European Parliament's proposal for a Regulation on Digital Operational Resilience (DORA), AmCham EU has identified several areas that we welcome in the current amendments, as well as aspects in the proposed amendments where we believe further refinement is necessary. Some of our comments also relate to the Directive on Digital Operational Resilience, which amends Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341.

Positives

- **Scope of DORA increasingly focusing on critical or important functions**
- **Carve out of inter-group activities**
- **Treatment of intragroup (de-scoping of intragroup from the oversight framework)**
- **Due process of the oversight procedure**
- **Proportionality and risk-based approach to digital operational resilience**
- **Alignment of incident reporting under PSD2 and DORA, including for non-ICT related incidents**
- **NIS-DORA interplay & consistency**
- **Safeguards when delegating reporting to service providers, termination of outsourcing agreements and penalties**
- **Platform on Cybersecurity of Financial Sector**
- **Entry into force & application of the Regulation**

Areas for improvement

- **Provisions on third-country providers and subcontractors**
- **Attempts to turn oversight of critical third-party providers (CTPPs) into a supervisory requirement**
- **New obligations for financial institutions to report significant cyber threats**
- **Confusing amendments on the structure and governance of oversight**
- **Lack of clarity of definitions, especially for outsourced services**
- **Lack of clarity regarding overlap in reporting obligations for ICT service providers**
- **No inclusion of extra EU mutual recognition of threat-led penetration testing (TLPT)**
- **Recognising the importance of assessing the need for multi-vendor strategy**

AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Positives

The amendments to the draft proposal of the European Parliament address various issues of importance. AmCham EU welcomes the following proposed aspects of the amendments:

- **Scope of DORA oversight:** We generally welcome the increased focus of DORA on critical or important functions provided by financial entities. We welcome that several amendments bring an **enhanced focus on critical or important functions** (ie 201, 210, 211, 591, 606, 612, 613, 614, 615, 616, 617, 621, 622) as well as **clarifications on the scope of the oversight** (ie 658, 680, 697, 711, 712, 700 – *this last amendment is of particular importance*). In particular, amendment 658 helpfully supplements the list of criteria for designation of CTPP to include consideration of the materiality and importance of the services they provide and amendment 700 clarifies that it is primarily the critical or important services.

- **Carve out of inter-group activities:** Amendment 208 seeks to further clarify the scope of the designation by excluding non-critical 'ancillary' services which do not create operational resilience dependencies. Further to this, we recognise as a positive development the de-scoping of the intragroup from the oversight framework and the suggestion to de-scope insurance intermediaries due to the existing European Insurance and Occupational Pensions Authority (EIOPA) guidelines for the insurance intermediation sector (amendment 249).

- **Treatment of intragroup (de-scoping of intragroup from the oversight framework):** We welcome the recognition from several MEPs and groups that the role played and risks posed by intragroup ICT third party providers (TPPs) is not the same as external ICT TPPs, and as such they should not be defined and treated in the same way within DORA. We therefore fully support the proposed amendments seeking to remove intragroup ICT TPPs from the oversight framework intended for critical ICT TPPs (CTPPs). (Various amendments: 25 and 29 (rapporteur's original report); 262; 307; 659 and 677).

- **Due process of the oversight procedure:** Numerous amendments further define due process and transparency of the oversight procedures under chapter V. These changes are beneficial for the industry as a whole to make the oversight clearer, fairer and more effective (eg amendment 218, 225, 661, 662, 664, 665, 692, 705, 714).

- **Enhanced proportionality and risk-based approach to digital operational resilience:** Amendments (554, 556) propose that financial entities adopt a risk-based approach to digital operational resilience testing which is proportionate to the potential risk. We also welcome further clarifications on addressing the risks of third party provider participation in customer testing in a multi-tenant environment such as public cloud (amendments 559, 561, 564). The proposals in amendment 564, 566, 576 and 579 for mutual recognition of test results between competent authorities contribute towards efficiency and effective risk management.

- **Alignment of incident reporting under the Payment Services Directive (PSD2) and DORA, including for non-ICT related incidents:** The Parliament recognises that there cannot be legal ambiguity or conflicting regimes for payment institutions when it comes to ICT vs non-ICT incident reporting (amendments 286, 291, 470, 471, 474, 478, 479 and revisions to the DORA directive). We welcome clarity on the scope and wish to highlight that any payment system or scheme already subject to the ECB's oversight framework should not fall in the scope of DORA to avoid overlap or conflicting regimes.

- **Network and Information Security Directive (NIS)-DORA interplay and consistency:** We welcome positive progress on the clarification of the cooperation between both supervisory structures and particularly the introduction of ***obligatory coordination by the Lead Overseer*** with the NIS competent authority before issuing oversight plans and recommendations. We therefore strongly support amendments 170, 172, 225, 226, 693, 694, 701, 702, 704, 748, 749, 750. We equally welcome the amendments 527 as well as 571, 572 and 575 proposing greater involvement of the European Network

and Information Security Agency (ENISA) in the preparation of regulatory technical standards on incident reporting and testing.

- **Safeguards when delegating reporting to service providers:** (Deleted in amendment 516) while amendment 517 mentions that delegating reporting to service providers is possible only after agreeing a contractual provision with the ICT third-party service provider concerned, amendment 518 and amendment 519 stipulate for this to happen after an explicit request from both the financial entity and the ICT third-party service provider (financial entity shall remain fully accountable for the fulfilment of the incident reporting requirements).

- **Safeguards when it comes to termination of outsourcing agreements**: As a measure of last resort and after corrective or remedial actions (amendment 212, 593, 594 – 598) and as in amendment 599 only due to a **significant** breach by service provider; amendment 602 only when **verifiable** circumstances where the competent authority **demonstrably** can no longer effectively supervise the financial entity; amendment 736 the financial entity to be informed of decision to terminate by competent authority at least 60 days in advance.

- **Safeguards when it comes to penalties:** Amendment 708 specifying that in case of full or partial non-compliance a periodic penalty (amendment 706, 1% average daily turnover related to provision of services in scope of regulation (amendment 708), measure of last resort (amendment 709), although the level of penalties in article 31 (6) should ideally amount to '***up to*** *1%'* of the relevant turnover to allow the lead overseer to set penalties that correspond to the nature of the behaviour.

- **Suggestion to create platform on cybersecurity of financial sector** (amendment 752) to also include experts representing relevant private stakeholders, and experts appointed in a personal capacity, who have proven knowledge and experience in the areas covered by this regulation. We welcome opportunities to bring all sectors together for informed decisions especially when it comes to working together on technical standards.

- **Entry into force and application of the regulation**: To allow for increased legal certainty following its entry into force, AmCham EU welcomes that MEPs have aimed for 24 months before the Regulation becomes applicable and even 36 months following its entry into force. This would provide industry with the crucial time to adapt to the new regulatory requirements.

Areas with potential for further improvement

Further to the positive areas of improvement through the amendments, AmCham EU would also like to highlight a plethora of areas where industry would like to see further improvements:

- **Provisions on third country providers and subcontractors** (amendment 216, 642): There is room for additional improvement when it comes to the third country provisions, especially in relation to amendment 216 regarding the deletion of the clarifying recital on data localisation and amendment 642, concerning requirements regarding contractual arrangements for third-country CTPPs. On this latter point we strongly believe that simply requiring CTPPs to establish or maintain a presence in the EU would provide the EU authorities with the enhanced oversight and improved dialogue sought. We are concerned about the Parliament's proposed amendments on article 28.9 related to third-country ICT third-party service providers. As regards amendments 671-677, we believe that the European Commission has found a balanced approach to the treatment of third-country ICT providers in its original proposal, which ensures oversight but does not create barriers to the international use of new technologies and technology providers. Moreover, the third-country provisions for subcontractors should be further improved. Article 31 (1) d) iv) grants the lead overseer broad powers towards the critical ICT TPPs sub-outsourcing arrangements. Rapporteur Kelleher's amendment 114 to Article 31 already proposed to clarify the powers of the overseer on sub-outsourcing arrangements by proposing

that these apply only to subcontractors which do not have a legal entity in the EU. We suggest adding more legal certainty on the conditions for the powers to be used by clarifying in Article 31(1) d) iv that the lead overseer can issue such recommendations on condition that it deems that *the use of such subcontracting poses a clear and serious risk to the financial entity.*

- **Attempts to turn oversight of CTPPs into a supervisory requirement:** A number of amendments would change the underlying instrument in DORA from Oversight into Supervision (amendments 220, 649, 651, 678, 698, 726, 729). This approach will make ICT providers regulated entities under the EU financial services regulation without there being a clear framework in place, nor a passport. We find these suggestions have no legal basis.

- **New obligation for financial institutions to report significant cyber threats**: Amendments (195, 292, 475, 482, 487, 492) introduce into DORA new requirements for financial entities to report cyber threats. We urge against this broad approach which will lead to over-reporting and could also jeopardise the trusted relationship built between financial entities and their customers, as we as financial entities and their third party providers. Interestingly, the ITRE draft report on NISD2 suggested making threat notification voluntary. We welcome this pragmatic approach, also to avoid creating a double standard with the NISD2. Whilst we support consistency regarding definition, scope and frequency of reporting, we do not support extending the DORA reporting framework beyond what is proposed by the European Commission to also include the reporting of significant cyber threats. Whether the reporting framework is ultimately covered in DORA or NISD2, we strongly believe the scope should be limited to reporting of actual incidents rather than all cyber threats. We therefore do not support amendments 279, 284, 292 and 474 seeking to introduce the reporting of significant cyber threats.

- **Structure and governance of the oversight**: we are confused by the different MEPs' approaches to the governance of the oversight with some supporting the rapporteur's proposal for creation of a new joint oversight body (JOEB) whilst others suggesting to maintain the lead overseer/oversight forum structure from the original proposal (and suggesting to nominate EBA as a single lead overseer). Any model needs to avoid the risks of national fragmentation of DORA implementation - more specifically under the Article 37 (3) no follow up action should be taken by the national authorities without the approval of the EU oversight body. In this regard we are strongly supportive of the suggestions made by the MEPs under Amendment 732 and 733 which aim at ensuring mandatory coordination of the follow up activities by the NCAs (under Article 37.3) at the EU level.

- **Lack of clarity of definitions leading to uncertainty regarding expectations of outsourced services:** Amendment 287 citing a 'major ICT-related incident' with an anticipated significant adverse impact lacks clarity. The word 'anticipated' implies a major ICT-related incident would be equal to a 'near miss' or cyber 'threat'. The definition should delete the word 'anticipated' to ensure that truly major events are reported. Similarly, the definition of 'significant cyber threat' as per amendment 292 ought to be aligned with the definitions of the NISD2 draft report. We also support Am 493 and 494 that clarify that notification obligations kick in only when the incident has a **material** impact.

- **Lack of clarity regarding overlap in reporting obligations for ICT service providers** (amendment 506): As service providers we are bound by our contractual agreements with our clients. Currently, neither DORA nor NISD 2 address the overlap in reporting obligations for ICT service providers. In this instance, we would ask for a clarification and clear delineation of obligations, hierarchy, and incident reporting recipients. In addition, it is important to include a Safe Harbour for service providers. To reflect this angle accordingly, we suggest the following change to amendment 605: 'In case of a major ICT-related incident, a notification from critical ICT third-party providers to the **financial entity** ~~competent authority~~ of the major ICT-related incident, without undue delay and not later than 72 hours after becoming aware.' The reporting should be done by the financial entity or as a joint report by the service provider and financial entity.

- **No inclusion of extra EU mutual recognition of TLPT:** In order to make DORA more interoperable with other third-country jurisdictional frameworks, AmCham EU believes it is essential to include extra EU mutual recognition of TLPTs. Many other major jurisdictions are developing their own frameworks for digital operational resilience, and many have their own TLPT frameworks, building on international standards developed and agreed by multilateral organisations of which the EU and its Member States are members. Given many global banks operate in a number of these jurisdictions, we believe a mechanism for mutual recognition of equivalent tests undertaken in trusted third country jurisdictions or module accreditation on non-EU regulator mandated testing would further enhance digital operational resilience at a global level.

- **Recognising the value of assessing the need for a multi-vendor strategy** (amendment 363, 364, 587, 588): A balanced multi-vendor or multi-cloud strategy is fast becoming a core part of global financial institutions' cloud strategy. We expect that this trend will continue as cloud adoption increases within financial services, together with the creation of hybrid architectures across cloud service providers (CSPs) to further prevent single-points-of-failure and leverage best-of-breed services. We would therefore advocate to maintain the language from amendment 365 imposing an obligation to assess the need for a multivendor strategy, while considering the relevant risks.