DIGITALEUROPE

8 FEBRUARY 2021

DIGITALEUROPE's response for the Commission's public consultation on the Digital Operational Resilience of Financial Services (DORA) legislative proposal

Executive Summary

90% of data worldwide has been created only in the last two years.[1] The financial sector is front and centre in reaping the benefits of a global shift to data-fuelled operations. The financial sector is using data to increase customer services and other important goals such as improving fraud detection. As a result, partnerships between ICT actors such as cloud service providers and financial institutions have been intensifying over the last few years to help manage safely and securely this ever-growing amount of data.

The draft DORA regulation is an opportunity to further accelerate the digital transformation of finance and show the EU's global leadership in defining a first-of-its-kind framework for outsourced ICT operations in financial services. Yet, unclear and potentially overlapping provisions in the existing draft risk to dramatically hamper the achievement of these goals. It is absolutely essential that the Council and Parliament work on the text to substantially improve the ability of DORA to accelerate the deployment of digital technologies for finance. DIGITALEUROPE urges focus on the following aspects moving forward:

- **An efficient regulatory framework and material consistency with the NIS Directive:** The EU needs an efficient and (as much as possible) harmonised regulatory regime ensuring consistency among the different legislative initiatives on resilience and security. DORA must not unnecessarily introduce duplication, complexity, or legal uncertainty, especially since the functioning of the proposed multi-layered Oversight Framework is already complex. In particular, the proposal for a revised NIS Directive has introduced substantial overlaps with DORA which makes it crucial that policymakers design a clearer hierarchy between DORA and NIS Directive for ICT providers.

[1] Axis Corporate, Understanding Big Data in Financial Services, 2020

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- **Proportionality:** This should be a unifying element across DORA's provisions. Elements like scope, powers of authorities and requirements for outsourcing to ICT providers should all be proportional to the intended goal of enhancing digital operational resilience and trust in finance as well as be proportionate to the identified risks. The oversight framework must be based on the materiality and importance of the outsourced services, not the type or scale of the outsourcing provider. Digital services which do not create critical operational and/or outsourcing dependencies (such as digital marketing and advertising) should be clearly exempted from the scope of the oversight. This is fundamental for the concrete viability of DORA and its adaptability to a fast-evolving technology context. Size and scope of penalties and oversight fees should be also proportionate to the business of provision of the critical services to the EU financial entities.
- **The ability to rely on third-country technologies**: DORA must avoid limiting the technology choices available to EU financial entities on the basis of the geographical profile of the ICT provider. The material gains in terms of customer well-being and improved security of ICT operations from the deployment of best-in-class digital technologies should remain the DORA's prevailing goals. Existing provisions would jeopardise this and should be swiftly changed.
- **Oversight due processes:** There needs to be a transparent process of consultation and - where needed - appeal of recommendations between the Lead Overseer and the designated Critical Third-Party Providers (CTPPs), as well as proportionate safe harbour protections for the providers' customers (financial entities and their customer data) so that privacy, security and integrity of the provided services is not unintentionally compromised while providers are complying with their obligations under the oversight. We are concerned over the lack of technical details on how the oversight framework would operate - especially with regards to innovative multi-tenant cloud environment. It is also key to streamline the oversight at the EU level as much as possible, and to ensure the NCAs are not taking any unilateral actions against the CTTPs and their customers without coordination and explicit agreement from the Lead Overseer.
- **ICT innovation:** DORA should stimulate, not impede innovation. We call on EU institutions to put in place a framework encouraging the adoption of technologies such as cloud. Technology-neutrality and the creation of a clear label of trust for the ICT providers in scope are essential to achieve that.

Table of Contents

Alignment between DORA and a revised NIS Directive

We appreciate that Article 1 (2) of DORA foresees a clear hierarchy between DORA and the NISD for financial entities. Yet, we point out how the proposal does not foresee such hierarchy between DORA and NISD for ICT providers (or CTPPs). This creates uncertainty and redundancy between the two frameworks, which has been exacerbated after the Commission published its proposal for a revised NIS Directive (so called NISD2), creating substantial overlaps. This makes it all the more important to ensure that the DORA proposal builds on the foundation of horizontal frameworks and requirements and foresees methods to remain aligned with them without introducing unnecessary duplication, complexity or legal uncertainty. This necessity is also recognised in recitals 16-19 of the DORA proposal. In terms of supervision & oversight, DORA proposes an oversight regime by which CTPPs will be designated among the ICT third party service providers - which include providers of cloud computing, data centres, software and data analytics services. Those CTPPs will be placed under the oversight of a Lead Overseer, being one of the ESAs. Their oversight will be complemented in practice by the ESA Joint Committee, an Oversight Forum, and Joint Inspection Teams, while the execution will take place through national competent authorities, with penalties enforced by national bodies (see further assessment of the oversight in chapter 6). Under the newly launched NISD2 proposal, those same providers of cloud computing services and data centers are considered providers of essential services and thereby placed under the supervision of the national competent authority of their main establishment. Hence, the current drafts of DORA and NISD 2 foresee a very similar oversight/supervision of identical digital/ICT services but entrusted to two entirely different regulatory instances. This will lead to an unnecessary duplication of regulatory bodies and expertise, and to material overlaps, complexity, and legal uncertainty for ICT providers.

- To ensure consistent resilience and security requirements for digital/ICT services in the EU, DORA should foresee that its CTPP oversight requirements and powers shall apply only if not already materially covered by NISD2. Alternatively, and/or additionally, one may envisage entrusting the oversight of the 3rd party ICT service providers under DORA - in any event for providers of cloud computing and data centres - to the competent bodies appointed under NISD2. That should not prevent ESAs from continuing to play a key role in setting requirements for the ICT risk management of the financial sector under DORA.

- In all circumstances, we propose to strengthen the role of ENISA under Article 42 of DORA, and more particularly e.g., as a full member of the Oversight Forum (Article 29 (3)), in the processes for setting ESAs guidance on incident reporting (Article 18 (1) DORA) and testing (Article 23 (4)), so as to allow for continuous alignment between the various regulatory resilience frameworks.

The above suggested changes are in our view necessary to ensure consistency between the different legislative initiatives around resilience and security to the benefit of the development of the digital single market.

The remainder of our observations will assess the existing DORA version while making abstractions of possible future changes that appear nonetheless necessary after the launch of the NISD2 proposal.

The need for a harmonised, consistent and proportionate resilience framework

- *Harmonisation and consolidation of existing requirements*, rather than introducing conflicting obligations for the firms and their ICT third-party providers. The outsourcing guidelines, such as those produced by the EBA[2], EIOPA[3] and the ESMA[4] guidelines, represent a welcome effort to harmonise requirements for cloud outsourcing across Europe and provide additional regulatory certainty to firms and their providers. A global approach to outsourcing will be further defined in the new IOSCO Principles on Outsourcing[5] and the by the Financial Stability Board (FSB) who recently completed a consultation on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships. All of these need to be taken into consideration by European policymakers to ensure consistency with the international benchmarks. While the draft DORA proposal builds on the valuable work and principles of the existing ESA outsourcing guidelines, we see also overlapping areas between the respective instruments. To avoid such overlaps, we believe that at the very least, for outsourcing to CTPPs, DORA should ultimately supersede or revise the current outsourcing regime. This is key to shaping a clear and consistent framework not only in the text of DORA, the delegated acts and the outsourcing guidelines, but also in the recommendations, the oversight plans and the possible decisions of national competent authorities.

---

[2] European Banking Authority (EBA), Guidelines on outsourcing arrangements, 2019

[3] European Insurance and Occupational Pensions Authority (EIOPA), Guidelines on outsourcing to cloud service providers, 2020

[4] ESMA, ESMA publishes cloud outsourcing guidelines, 2020

[5] ISOSCO, Principles on outsourcing: consultation report, 2020

- *Proportionality*: As a general principle, DIGITALEUROPE insists on the need to set proportionate resilience rules, that truly enhance the operational resilience and trust in the financial sector by adequately protecting services used by financial entities for critical or important functions. The issue of proportionality should not be reduced to delimiting the scope of the financial entities having to comply with DORA, notably through the definition of microenterprises. Proportionality should also be understood as refraining from overly prescriptive requirements setting out specific means for financial entities and ICT providers to ensure operational resilience. It is critical that DORA is future-proof. That is, adaptable to the fast-evolving development of cybersecurity technologies, for instance in the area of testing.

    - Principles of proportionality should equally apply to the scope of the Lead Overseer's powers over designated CTPPs. The scope of Lead Overseer powers needs to be limited to supervising those arrangements which support outsourcing of critical and important functions only. It would be disproportionate and unnecessary to grant Lead Overseers powers over all the ICT services that an ICT third-party service provider provides just because one of those services is found to be used by financial entities for critical or important functions. Finally, proportionality is also needed in respect of the penalties regime by limiting these to the providers' business in scope of the regulation.

- *Stimulation of trust in technology*. DORA should also stimulate innovative ICT adoption, not impede innovation. Cloud technology in particular has become an important driver of innovation for the financial services sector. For instance, it allows the adoption of AI and machine learning to improve consumer experiences, increase accuracy and efficiency of internal compliance, risk assessment processes and regulatory reporting. Today, we are also seeing increased trust and confidence in the safety and security of public cloud technology across the globe, both from the industry and regulatory community. In a 2018 paper by the Basel Committee on Banking Supervision (BCBS) on "Sound Practices - Implications of fintech developments for banks and bank supervisors" [6], the Committee refers to the cloud as an "enabling technology" that provides the underlying infrastructure for many FinTech activities and other technology solutions, such as advanced analytics. We urge EU policymakers to support and champion an approach that not only allows but also encourages innovation, noting it also allows for competitive

[6] BCBS, Sound Practices: implications of fintech developments for banks and bank supervisors, 2018

differentiation for financial services entities, with an overall positive impact on consumers. In this sense, the introduction of a new oversight regime for CTTPs should grant additional assurances and incentives for the European financial services sector to move to the public cloud at scale. In particular, DORA should clearly recognise that when a provider becomes subject to continuous regulatory monitoring activities under the oversight, the exposure to risk by the financial entities decreases when migrating to this provider. DORA should therefore be creating a clear label of trust for the providers in scope which needs to be clarified in the recitals.

- *Definition of ICT Services and ICT third-party service provider:* We urge more clarity on the specific type of ICT services falling under DORA. Clarity would help both financial entities and potential ICT service providers. We understand the benefits of avoiding overly prescriptive definitions to make legislation adaptable to any future technology development, yet we notice overlapping definitions of ICT Services and ICT third-party service provider in the current text. Under DORA's framework, financial institutions bearing the obligation to prevent any ICT risk may be unduly prompted to consider a provider of *any* ICT-related service as a regulated ICT third-party provider. The logic that a chain is only as strong as any one of its links may prompt financial institutions to require the providers of smaller scale services (e.g. consulting, advisory, design, system integration or other incremental ICT services) to agree to DORA-specified contractual obligations which such service providers may be unable to economically and practically perform.

  The current ICT definitions under DORA appear somewhat confusing and lacking consistency. While we understand that the concept of 'ICT risk' is meant to be broader than that of 'ICT 3rd party risk' (Article 13 (4)), we struggle to see the relation between these two concepts on the one hand and the concept of 'ICT services' (Article 3 (16)) on the other. In addition, the substantial provisions of DORA introduce other concepts like 'ICT systems', 'ICT security tools/strategies', 'ICT related business functions' which are nowhere defined and are therefore uncertain in scope. We therefore strongly recommend finetuning the provisions regarding the material scope of DORA. In that sense, it is worth recalling that the current DORA draft already expands ambitiously the definition of ICT 3rd party service providers (and thus of ICT 3rd party risk) beyond the scope of the current ESA Guidelines on outsourcing and cloud to include also on-premise software and data analytics services.

- *Date of application:* It should be after the publication in the OJEU[7] of the regulatory technical standards drafted by the ESAs, not prior to it. The proposal for a 12-month period for compliance with DORA, as envisaged in Article 56, is unrealistic and inconsistent with provisions in Article 23 and 24, which foresee compliance with regulatory technical standards 12-36 months after DORA enters into force. We recommend postponing the date of DORA's application to 24-36 months after the date of entry into force. This will ensure consistency and alignment with the application timelines for regulatory technical standards.

ICT and security incident reporting requirements

The EU must design a more harmonised ICT and security incident reporting framework, this would greatly benefit innovation in the digital space for banking and cloud computing. Today, there are unnecessary costs stemming from fragmented and inconsistent provisions among Member States, which in the case of multi-tenant public cloud services are even higher.

DIGITALEUROPE urges EU policy-makers to focus on the following:

- *Major ICT-related incidents*: Article 17 requires financial entities to report "major ICT-related incidents", which are defined as ICT-related incidents with a "potentially" high adverse impact on the network and information systems. This contrasts with current similar EBA and EIOPA requirements which require notification of a "disruption or emergency" i.e., not something that *may* occur, but something that *is* occurring or *has* occurred. This also contrasts with notification thresholds for incidents such as those under the EECC, GDPR or ePrivacy Directive which all require notification of incidents with actual impact or at the very least "likely" impact. Thus, we believe the threshold under Article 17 is too low and could create legal uncertainty with the financial institution about the need to notify or not. It would also lead to an unhelpful situation where regulators are overwhelmed with incident notifications. Therefore, we ask the Member States to consider changing the threshold in DORA so that it is closer to the threshold in other relevant instruments, by for example replacing "potentially high adverse impact" with "reasonably likely high adverse impact" or similar language.

- *Delegated reporting:* The EU should ensure that delegated reporting as proposed in Article 17 (4) can only be imposed in full agreement with the ICT provider concerned. Indeed, as the relevant reports are to be submitted to competent authorities regulating financial entities, rather

[7] OJEU stands for the Official Journal of the European Union

than the Lead Overseer with oversight of the ICT provider, we generally fail to see in which circumstances it would be appropriate to task ICT providers with the reporting of major incidents on behalf of financial entities. In most situations, ICT providers – who are practically offering only a part of a financial entity's ICT – will also lack sufficient information to do such incident reporting. This is especially true in the case of CSPs. Also, they will often be unable to determine whether an ICT related incident is major. If the option is kept, further clarification is required that the approval of the competent authority can only be given following an agreement / request from both the financial entity and the ICT provider. Moreover, it should be clarified that accountability for reports submitted to the competent authorities remains with the financial entities, and that the ICT providers will not be held responsible for the content of such reports.

- *Incident assessment*: We recommend to include specific parameters in DORA to assess the impact of ICT-related incidents. This would boost legal certainty.
- *Reporting timeframes*: The EU should clarify in DORA that incident reporting timeframes should run from the moment the financial entity becomes aware of the incident (17 (3)). This is also common practice in other regulations that impose incident reporting duties.

Testing

- *Technology context*: Any requirement for operational resilience and penetration testing by financial institutions that include third-party providers need to be assessed against the technological reality of these processes, potential risks and trade-offs. Whilst we agree that cooperation between firms and their providers for testing purposes is important, as recognised for example in the FSB's Effective Practices for Cyber Incident Response and Recovery Consultation,[8] it needs to take into account that cloud services are a one-to-many multi-tenant environment. From this perspective, a public cloud provider cannot simulate a disruption of its service to support a single customer's testing because this could impact the integrity and security of the operations of other customers. At the same time, cloud service providers offer tools to customers to perform independent testing and simulate disruptions of their own cloud resources. If collaborative testing is required, it is critically important that such exercises remain voluntary, risk-based and bilaterally agreed upon between the customers and their providers.

[8] FSB, FSB consults on effective practices for cyber incident response and recovery, 2020

- *Information sharing:* We deem it inappropriate to share the level of information required in Article 23 on vulnerabilities on a client-only and/or regulator-only basis, especially as threat-led penetration testing of production systems must take into account the risks to other clients in a multi-tenant environment. If such information must be revealed, it should be done at once, to all customers at the same time and only after the issues have been fixed. Concretely, we suggest to complement Article 23(2)(4) with a provision recognising that "Those ICT third-party service providers cannot be required to communicate information about any unpatched vulnerabilities or about items which are not relevant to the concerned critical or important services of the financial entities."
- *Recognition of test results*: There are currently no provisions allowing recognition of threat-led penetration testing frameworks (TLPT) test results undertaken in jurisdictions outside the EU. International financial services groups operating around the world may be subject to different digital operational resilience and testing frameworks in different jurisdictions. To avoid the risk of regulatory fragmentation and potentially costly requirements for separate tests to be undertaken in each jurisdiction, policymakers should include in the regulation a mutual recognition framework allowing TLPT tests undertaken in trusted third countries to be recognised under this framework.
- *ENISA involvement*: We recommend involving ENISA in the standards setting process foreseen by Article 23 (4) to ensure consistency with other possible regulatory requirements.

Multi-vendor and interoperability requirements

- *Article 5 (9) and Article 26*: We appreciate the regulators' concerns over the perceived market concentration risk, however, we strongly believe that those should focus purely on the security and operational resilience of ICTsystems. In the case of cloud, hyperscale cloud providers have security and operational resilience capabilities that benefit financial services customers and surpass those features that are available on-premise. The overall threat of a single point of failure is, in our view, unjustified. With this in mind, principles of flexibility and industry-led best practices in approaching portability and interoperability need to be maintained, consistent with ongoing multi-stakeholder efforts like those under SWIPO. Equally, a multi-vendor strategy needs to remain a customer's choice, based on their risk assessment and business priorities, not a regulatory provision. Policymakers should further support the developments of principles of openness and interoperability in the industry, but it is too early to formulate any of those in prescriptive regulatory requirements, which

would slow down the adoption of cloud as a whole. It is key that the multi-stakeholder assessment under DORA does not overly constrain financial entities' flexibility beyond what is necessary for security reasons, and still allow them to outsource certain specific functions or services to certain ICT providers when this best meets their needs and resilience requirements.

Oversight of third-party providers (including outsourcing)

In the effort to develop a new direct oversight framework for CTPPs, it is important the EU adheres to the principles of technology-neutrality and proportionality, as well as aligns with the established international solutions. Given the global nature of both the financial and ICT sectors, it is critical the EU framework maintains a level playing field to ensure EU financial services organisations remain competitive. Moreover, whatever approach Europe is going to take will set a new, unprecedented example for cloud governance and outsourcing in other parts of the world. It is therefore absolutely critical to consider its proportionality and effectiveness, as well as a principles-based and risk-based foundation.

DIGITALEUROPE, which represents financial services firms, cloud services providers (CSPs) and other service providers, firmly believes the EU oversight framework for third-party providers should observe the following principles:

- *CTPP designation and scope of the oversight:* The critical designation and oversight by the Lead Overseer should be limited to the relevant part of the providers' business. It would be disproportionate and inefficient to grant Lead Overseers powers over all the ICT services of a given CTPP, including those which are not used by financial entities at all or not for critical and important functions, simply because one of its services is used for critical functions of financial entities. It is indeed imperative to assess the criticality of services and functions outsourced by financial organisations to evaluate the potential level of systemic risk. Not all outsourced tasks have the same level of risk. Such assessment must treat all outsourcing providers in the same way, regardless of whether they are active in the public cloud, private cloud, or some variant. It must also duly acknowledge influential studies[9] concluding there is no immediate financial stability risk for financial institutions from the use of cloud services.

[9] FSB, Third-party dependencies in cloud services: Considerations on financial stability implications', 2019

Ultimately, **the oversight needs to be performed based on the materiality and importance of the outsourced services, not the type or scale of the outsourcing provider**, and be principled and risk-based.

In practice, this should be addressed by narrowing the scope of Article 28 (1), i.e., having this article only apply to the ICT services of the provider that are identified as critical for financial entities (used for critical and important services - in line with the ESAs Outsourcing Guidelines) or; by clarifying that the scope of the Lead Overseer's powers under Article 31 is limited to the ICT services of the provider that are identified as critical for financial entities. In the same vein, we recommend to:

- recognise in Article 32 that the Lead Overseer should only be able to require ICT third party providers to provide information about financial entities subject to DORA who are using the services for critical or important functions; in the interest of transparency and due process, regulators should also provide notice to the relevant financial entity of requests specific to that financial entity.
- specify in Article 33 that during investigations the Lead Overseer should only be able to require ICT third party providers to provide information about financial entities subject to DORA who are using the services for critical or important functions.
- limit the scope in Article 34 of the on-site inspections by the Lead Overseer to the provider's EU premises actually used to provide services to in-scope financial entities for critical or important functions.

- *Instruments for the designation of CTTPs:* We also raise concern that foreseeing additional criteria-setting by delegated act (Article 28 (3)) would lead to uncertainty on the market. All criteria for the designation of CTPPs should appear in the text of the DORA Regulation so as to create clarity for both financial services entities and potential CTPPs. This is all the more relevant since there may be a period of transition and uncertainty between the adoption of the Regulation and the designation of CTTPs. Furthermore, we note that the in the appointment of one of the ESAs as the Lead Overseer for each CTPP, the formula outlined in article 28 (1) b) needs to be clarified. In addition, making the appointment of the Lead Overseer depend on such a formula creates the risk that, for a given CTPP, the Lead Overseer changes over time, creating uncertainty and inefficiencies.

- *Trust and a clear passport to operate for the CTPPs in scope and for their financial services customers.* Once the direct oversight framework over CTPPs is adopted, **it should replace the existing requirements for financial services customers to notify or seek regulatory review (non-objection)** when implementing cloud deployments with CTPPs. This will help to **streamline the compliance process**. Outsourcing to CTPPs should be exempt from this notification process in the EU, as their security and operational practices would be independently verified by the competent overseeing authorities throughout the enhanced regulatory monitoring activity introduced by the direct oversight - regardless of the specific customer deployments. As part of this process, it will be important for overseeing authorities to ensure that National Competent Authorities are sufficiently informed of deployments and developments, in order for them to satisfy their supervisory mandates. Financial entities should also take into consideration the Oversight findings when they perform their due diligence on the third-party providers that are subject to the Direct Oversight Framework.

- *Competent authority*: It is crucial that the supervisory power leverages an effective mechanism which allows for the relevant expertise and inter-agency collaboration. The EU framework will be the first of its kind globally, hence we strongly believe this demands an effective and well-coordinated effort to ensure its success. While we agree with the current proposal granting core oversight powers to the ESAs which will help ensure the effectiveness of this approach, one may consider appointing only one ESA as Lead Overseer rather than three to ensure capacity building and expertise. To avoid fragmentation, NCAs should not have additional oversight powers at the national level. We think that this should ideally be clarified in Article 29 (4) and Article 30 (4).

With these principles in mind, the oversight framework needs to acknowledge that not all traditional prudential regulatory and enforcement measures would be appropriate and effective in the context of ICT regulation:

- *Follow-up actions by supervisors*: Any findings by regulators as a result of the oversight process should be subject to discussion with the relevant third-party provider to ensure effective implementation and balance the twin desires of robust regulation and high levels of innovation - in line with the existing audit procedures. The US Bank Service Company Act[10] could present a constructive example of an existing international practice in this area, where financial services regulators have a direct audit right over technology providers as part of the oversight but the audit does not

[10] Section 7 of the US Bank Service Company Act

include remediation measures impeding providers' ability to maintain appropriate controls. We also caution against potential supervisory action to mandate **changes or termination to the firms' relationship with their providers**. Termination of contracts by the NCAs (Art 37) should be a last resort following a due process in coordination with the Lead Overseer or Oversight Forum. This ultimately needs to be a business decision of the financial services institutions based on their thorough risk assessment and exit strategies.

Unilateral regulatory action could be harmful to the integrity and security of the firms' outsourced services. There are also considerations around complexity, costs and timings of migration issues to take into account in such unilateral regulatory action. We strongly recommend that the EU adopts a proportionate approach where the regulatory observations and findings resulting from the oversight regime should form ***recommendations*** for technology providers to **implement changes in a risk-based, proportionate way, tailored to the nature of their services and over a reasonable amount of time**.

More broadly, contractual requirements need to be scoped consistent with the ESAs guidelines based on materiality/provisions of services for critical and important functions. It should also be clear how we transition from the current outsourcing guidelines to the new framework, especially given financial entities and providers will already have existing contractual arrangements.

- *A clear appeal process* should also be introduced for the technology providers to address potential gaps in the identified recommendations. Any further considerations to sanctions and penalties as part of remediation should equally be proportionate and well-measured. We question the proposal that periodic penalty payments are always fixed at 1% of the average daily worldwide turnover of the CTPP. To be consistent with the principle of proportionality and with the approach adopted under numerous other regulations, we recommend foreseeing that periodic penalty payments shall not amount to more than 1% of the average daily worldwide turnover of the CTPP and be proportionate to the nature and gravity of the non-compliance.

- *Approach to sub-outsourcing*: This needs to be consistent with the current EBA and EIOPA outsourcing guidelines and consider the nature of cloud one-to-many multitenant services. We believe that today's outsourcing frameworks already grant supervisors sufficient control over providers' sub-outsourcing arrangements which is equally reflected in customer contractual commitments. A similar approach was taken in the U.S., where regulators have the authority to request information about the sub-

outsourcing arrangements of technology service providers, but they do not have the authority to place restrictions on these relationships which would disrupt the secure provision of technology services.

- *Third-country regime*: We note some problematic language in the proposal to dissuade firms from using third-country providers. These provisions need to be clarified as they would ultimately deter European firms against global technology players, despite the quality and commercial benefits of their services, and would create competitive challenges for the EU market denying its financial firms access to the benefits of global technology innovation. More precisely:

    - Article 31 (1) d iv, which allows the Lead Overseer to recommend that CTPPs refrain from subcontracting critical functions when the subcontractor is established in a third country, does not sufficiently consider the reality of the globalized ICT world. Most large ICT providers have a business/presence in the EU, but are largely subcontracting around the world. In its current form, this provision risks having unmanageable implications by risking casting too big of a shadow over operational business continuity policies of ICT providers who generally serve many other sectors than only the financial sector and are not able to assess to which extent one or more financial services use their services for critical and important functions. In addition, the provision goes beyond and imposes a more prohibitive regime on ICT providers than the already strict requirements imposed on financial entities under Article 26 (2). This additional prohibitive layer is not justified nor proportionate. Therefore, we propose to scrap the provision and to leave the accountability with the financial entities as proposed in Article 26 (2).

    - Third country provisions in Art 28 (9) need to be clarified: the requirement for financial entities to assess whether an ICT provider would be designated critical or not in the EU is very complex and uncertain as the financial entities will normally not have the needed level of information or expertise to make this assessment. It is regulators' competence and responsibility. This will be all the more problematic because of the delaying impact of Article 28 (4) – during the initial period, financial services institutions will be under total uncertainty.

    - More generally, the aforementioned provisions - which treat foreign service suppliers less favourably than domestic EU service suppliers – may amount to an unpermitted discrimination under WTO law, more precisely a violation of the EU's national treatment obligation under Article XVII GATS.

- *Data residence:* The global footprint of technology operators and reliance on a geographically distributed infrastructure are key factors to ensure security and operational resilience of cloud services. Similarly, global financial institutions with customers across the world may choose to locate and transfer their data internationally for latency and other business purposes, maintaining the appropriate legal and security safeguards. For these reasons, any forced data localisation requirement, as suggested by some Member States are overall incompatible with the security and resilience of cloud services. We welcome the EC approach confirming that no additional data localisation requirements should be introduced as part of DORA and the oversight practice. **Data location should remain the customer choice based on risk assessment**, and their providers need to offer technological capabilities and contractual commitments to support these choices.

- *Customer data privacy and security*: We note in the proposal the regulators' broad powers to request customer data from the CTTPs as part of the oversight and general investigations, particularly Article 33 (2) e). We caution policymakers against an overreaching approach, that is likely to conflict with existing ePrivacy regulations, and urge them to institute appropriate safe harbours to guarantee that privacy and security of the financial institutions' and their customer data are not compromised in the course of the audits.

- *Contractual arrangements:* The language in Article 25(8), mandating contractual arrangements to be "*terminated at least*" in the event of prescribed scenarios (including where there has been a breach of "*applicable laws, regulations or contractual terms*") is not proportionate or effective in achieving DORA's goal of improving digital operational resilience. As currently drafted, this wording may result in circumstances where financial institutions are required to terminate their contractual arrangements where the breaches themselves may be non-material, may have caused no detriment or where the service provide may be capable of remedying the breach. Article 25(8) should be amended such that contractual arrangements "*may* be terminated'' rather than "are terminated at least". This would bring various benefits:

    - Consistency with the remainder of DORA, including Article 27(2)(d) which provides that contractual arrangements should "*enable without undue delay appropriate corrective actions when agreed service levels are not met*". Article 27(2)(d) envisages a scenario where remediation measures can be taken or that breaches will not meet a materiality threshold requiring termination of the contract.

- Reflecting the practical reality of contractual relationships between financial institutions and service providers. These contracts are heavily negotiated and provide for materiality thresholds, remediation procedures and where remediation is not possible, termination and exit strategies. Further, financial institutions and service providers often enter into compartmentalised service agreements, under which different services may be provided and if necessary, terminated without impacting the remainder of the agreed services. The current drafted language would disproportionately terminate contractual arrangements where any disruptions are limited to specific services which may be non-material, and which may not relate to critical or important functions. The proposed change in language would likely be welcomed from a financial institution's perspective as it provides flexibility to ensure remediation rather than uncertain financial costs and the resource consuming process of sourcing alternative arrangements for minor contractual breaches where there has been no detriment to the institution or its clients.

- Alignment with other EU guidelines, which do not currently mandate that contracts be terminated without the possibility of remediation. For example, paragraph 98 of the EBA's Guidelines on Outsourcing Arrangements (2019), requires only that the outsourcing arrangement *"expressly allow the possibility […] to terminate the arrangement"* in certain circumstances.

  Section 4.8 of the EBA's Recommendations on Cloud Outsourcing envisages that institutions have the flexibility to define those breaches which trigger exit strategies. This allows for the possibility of minor breaches of service levels and remediation exercises.

  Paragraph 55 of the EIOPA Guidelines on Outsourcing to Cloud Service Providers only requires that a "clearly defined exit strategy clause ensure that it is able to terminate the arrangement, where necessary". Such exit clause may include timelines and fees, select transitional intellectual property licenses and adequate protections for the client data to ensure a smooth transition to a new cloud service provider. Under paragraph 56 of the Guidelines, parties are granted the flexibility to define such trigger events, such as unacceptable levels of service, licenses and wind down terms.

The ESMA's Guidelines on outsourcing to cloud service providers,[11] similar to the above, do not mandate that institutions terminate contractual relationships.

Exclusion of payment systems and schemes from the DORA's scope

We support the Commission's approach to exclude payment systems and schemes from the scope of the regulation, as shown in the draft tabled to Council and Parliament. The European Central Bank (ECB) oversight framework already addresses payment system operational resilience, regulating comprehensively ICT risk management in payment systems. Payment systems deemed as ''systemically important payment systems'' (SIPS) are covered specifically by Regulation 795/2014 of the ECB[12]. The latter integrates into its framework the principles for financial market infrastructures (PFMI) developed by IOSCO and the Committee on Payment and Settlement Systems of the Bank for International Settlements (CPSS)[13], thereby setting high international risk management standards for payment systems. In addition, other (non-SIPS) payment systems operating in the Eurozone are also required to adhere to the PFMI, or a subset of the PFMI.

Payment systems need also to comply with the ECB's Cyber Resilience Oversight Expectations for Financial Market Infrastructures[14] which regulates in detail the set-up of cyber resilience strategies and frameworks, including incident management, testing and crisis communication. The ECB has also put in place an incident reporting framework for Retail Payment Systems and Payment Schemes. It requires institutions to report major payment security incidents to their Overseer.

In light of the existing, well-defining and sound regulatory requirements, extending the scope of DORA to payment schemes would create unnecessary regulatory burden on market players and potentially generate conflicting provisions.

---

[11] ESMA, ESMA publishes cloud outsourcing guidelines, 2020

[12] Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28)

[13] Bank for International Settlements, Principles for financial market infrastructures, 2012. The PFMI contains provisions addressing inter alia operational risk management (including the obligation to establish clear policies and procedures that mitigate and manage the sources of operational risk, conduct internal controls, periodically test and review operational procedures); incident management; and measures related to safe outsourcing of operations.

[14] ECB, Cyber resilience oversight expectations for financial market, 2018

FOR MORE INFORMATION, PLEASE CONTACT:

Ray Pinto

Digital Transformation Policy Director

ray.pinto@digitaleurope.org / +32 472 55 84 02

Vincenzo Renda

Senior Policy Manager for Digital Industrial Transformation

vincenzo.renda@digitaleurope.org / +32 490 11 42 15

Thomas Hellebrand

Policy Officer Digital Transformation

thomas.hellebrand@digitaleurope.org / +32 492 46 78 17

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Workday, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK