European Payment Institutions Federation aisbl

EPIF's views on the Digital Operational Resilience Act (DORA)

April 2021

EPIF's views on DORA

EPIF welcomes the opportunity to provide our views on the Digital Operational Resilience Act (DORA). We believe that DORA is a good initiative to harmonise and streamline the EU framework for digital resilience in the financial sector. With the financial sector making ever-greater use of information and communications technology (ICT), we agree that it is important to update the rules to ensure that financial-sector ICT systems can withstand security threats and that third-party ICT providers are monitored. However, we have identified a number of areas where the Commission's proposal could be further refined as, in its current form, **DORA could have far-reaching consequences for payment and e-money institutions.**

While our members believe that DORA is seen as a good initiative to streamline the ICT operational resilience requirements across the entire sector, the **PSD2 already includes such tailored requirements for the non-bank payment sector**. Furthermore, EPIF members are of course also already subject to the **existing ICT and outsourcing guidelines** by the European Banking Authority (EBA).

The ICT risk management requirements in the PSD2 are intrinsically linked to other provisions in the PSD2 related to secure communications and access to customers' accounts for the purpose of payment initiation and account information services. EPIF therefore expresses some concern that **compliance with DORA will duplicate the existing provisions and inadvertently create new barriers for payment institutions to access client information**. This would run counter to the EU's wider objective of advancing its goals of data sharing and open finance.

In the light of this, EPIF would support the discussions in Council to **treat the PSD2 as a *lex specialis* to DORA** and continue to have payment institutions subject to the provisions in the PSD2, rather than DORA. Should any of the PSD2 ICT operational resilience requirements require updating in the light of DORA this could in any case be included in any future revision of the PSD2, as already announced by the European Commission.

In the absence of this we would urge the EU co-legislators to ensure DORA and any possible Level 2 measures remain in line with **pre-existing international standards, as well as the existing EBA Guidelines.**

Moreover, there are other provisions in the **draft proposal that should be aligned with the PSD2**.

Please find our detailed comments below:

ICT Risk Management Framework - Consistency with EBA Guidelines on Outsourcing Arrangements

Article 4(3) states that "Financial entities other than microenterprises shall establish a role to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or shall designate a member of senior management as responsible for overseeing the related risk exposure and relevant

documentation." The EBA GL on outsourcing arrangements foresee an "Outsourcing Function/Officer", which is a second line of defence role responsible for managing and overseeing the risk of outsourcing arrangements and overseeing the documentation of outsourcing arrangements. The question arises if the same person can fulfil both the role of "Outsourcing Officer" and "ICT third party Officer" and we would suggest to include clarifications that "For Institutions in scope of EBA/GL/2019/02 on Outsourcing Arrangements the role of "Outsourcing Officer" as foreseen under EBA/GL/2019/02 and the role of "ICT third-party officer" as foreseen under this regulation, can be fulfilled by the same person."

Furthermore, the EBA GL on outsourcing arrangements foresee that, in case of small and less complex institutions/ payment institutions, the outsourcing function may be assigned to a member of the institution's/payment institution's management body. Under the draft of DORA, this is formulated as an *OR* option. Would this imply that, no matter the size of the institution, the "ICT third-party Officer" role can be assigned to a member of senior management?

Article 5(10) states that "Upon approval of competent authorities, financial entities may delegate the tasks of verifying compliance with the ICT risk management requirements to intra-group or external undertakings." According to the EBA GL, approval from the competent authorities is required only for major outsourcing, thus would the Article imply that this type of outsourcing is considered as major outsourcing by default?

Article 10 foresees the establishment of an 'ICT Business Continuity Policy'. The EBA GL on ICT and Security Risk management foresee the establishment of a Business Continuity Management (BCM) process, which is something different than a Business Continuity Policy. The BCM should consist off a Business Impact Analysis (BIA), a Business Continuity Plan (BCP) and response and recovery plan (Disaster Recovery Plan (DRP)). The EBA GL also foresee the implementation of an incident and problem management process (GL 59), which is separate from the BCP. Only in case of certain types of incidents, the BCP is being invoked and the DRP should be activated. The provision in Article 10 of DORA, as it is formulated in the Commission proposal, would require payment/e-money institutions to create an **additional** ICT Business Continuity Policy, without having the obligation to implement an operational business continuity policy. Our suggestion would be to replace the wording by "ICT Business Continuity Management Process" or "ICT Business Continuity Management Arrangements" throughout the DORA proposal.

Furthermore, **Article 10(2)** provisions state that the ICT Business Continuity Policy would **(a)** record all ICT-related incidents, as well as **(c)** quickly, appropriately and effectively responding to and resolving all ICT-related incidents, in particular but not limited to cyber-attacks, in a way which limits damage and prioritises resumption of activities and recovery actions. We would suggest to move these two sub-provisions to Article 15 (ICT Incident Management Process).

Article 12(2) refers to "significant ICT disruptions." There is a lack of clarity as to how to define 'significant' or, alternatively, is it meant to be a reference to 'major ICT-related incidents'?

ICT-related incident reporting

We welcome that the proposed ICT risk management requirements in DORA seem for now to align with those in the PSD2. This is not the case as regards incident reporting. The interaction between DORA and PSD2 could lead to a **more fragmented incident reporting framework** as payment institutions might have to set up separate reporting systems for incidents to be reported under the PSD2 and DORA. Specifically, payment institutions will have to report major-ICT related incidents under the DORA framework and would be excluded from ICT-related

incident reporting under PSD2. However, they would still have to report other major operational or security incidents that are not considered ICT-related incidents under Article 96(1) of the PSD2.

Moreover, different **reporting deadlines and incident classification criteria** apply in DORA and the PSD2 are substantially different, which would lead to a duplication of work for payments institutions and therefore culminating in a more burdensome situation for those who fall under the two pieces of legislation.

More concretely, many of the criteria set out in **Article 16(1)** are not in line with the EBA Guidelines on Major Incident Reporting when determining whether an incident is to be considered as major or not. These criteria could result in a different assessment methodology for ICT-related incidents versus other incidents, which would lead to complexity and fragmentation. The classification criteria should be aligned as much as possible with existing criteria. Consequently, also when developing Level 2 measures specifying the criteria set out in Article 16(1), the ESAs should take into account the EBA guidelines, which are currently under review as too many operation vs. security incidents were being reported.

Regarding **reporting** of major ICT-related incidents, the terms of the requirement in **Article 17(2)** are too vague. It is not clear when an incident has or "may have" an "impact" on "financial interests". The required **timeframe** for the reporting is not clear either ("without undue delay" and "as soon as possible"). The unclear wording of this requirement leads to the risk that too many incidents are reported to consumers, which could hamper consumer confidence. Regulatory and/or supervisory guidance would be needed to implement this requirement in an effective and coherent manner across the EU. Furthermore, it is unclear whether the requirement is only an objective duty or whether it also confers subjective rights on customers.

The **reporting deadlines** under **Article 17(3)** are not in line with the reporting deadlines under EBA Guidelines on major incident reporting nor with the proposed reporting deadlines of the revision of the EBA Guidelines. This will lead to complexity and fragmentation of reporting frameworks for payment and e-money institutions. The reporting deadlines should be aligned as much as possible with existing deadlines under the EBA Guidelines and its currently ongoing revision.

Proportionality

Another concern of EPIF relates to the principle of **proportionality** when it comes to the application of the rules proposed under DORA. Many payment institutions are highly specialised and small in relative size to other financial services providers covered by DORA, such as investment banks, credit institutions or insurance companies.

Article 4(4) foresees that "Members of the management body shall, on a regular basis, follow specific training to gain and keep up to date sufficient knowledge and skills to understand and assess ICT risks and their impact on the operations of the financial entity." However, it is not specified **what type of training** would this be and can this be freely decided by the financial entity or would there be pre-defined training courses assessed as suitable by the NCAs. Our preference would be that there is free choice by the financial institution, as it is best placed to determine which training is relevant for its specific business.

Article 10(3) states that "Financial entities other than microenterprises, shall have their ICT Disaster recovery framework audited by an independent auditor." This is a very heavy requirement, which will bring an important additional cost. There should be more room for proportionality for sectors which are relatively small, such as payment/e-money institutions.

Article 10(9) states that "Financial entities other than microenterprises shall report to competent authorities all costs and losses caused by ICT disruptions and ICT-related incidents." This is also an onerous requirement, as under the PSD2, such reporting is foreseen only for major incidents. We would suggest to include the clarification that such reporting should be done only for '**major** ICT disruptions and ICT-related incidents.'

Article 12(2) asks that "When implementing changes, financial entities other than microenterprises shall communicate those changes to the competent authority." This could be a burdensome requirement. EPIF suggests to rephrase the Article as follows: "When implementing changes to *its ICT operations*, financial entities other than microenterprises shall communicate those changes to the competent authorities."

Another example is **digital operational resilience testing**. Article 21 of DORA states that institutions shall maintain a testing programme with due consideration to the size, business and risk profiles. However, the list of tests that the testing programme must include by virtue of Articles 21(2) and 22(1) of the proposal does not seem to leave room for a proportionate approach. The proposal requires the establishment of a testing programme that includes vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing or penetration testing. EPIF believes that DORA should take a more nuanced approach with regard to the list of tests that must be included in the testing programme. Consequently, EPIF would suggest to change Article 22(1) by including the phrase "*which might include*". This would highlight that each financial entity is best placed to determined which tests are relevant for their specific business, taking their size and complexity into account.

Furthermore, the term 'critical ICT systems' used in **Article 21(6)** has not been defined.

Definition of ICT Third-Party Service Provider

The definition of an 'ICT Third-Part Service Provider' in the Commission's DORA proposal is formulated in a very broad and abstract way which may cause **difficulties in establishing a clear-cut classification of service providers** in practice. Further clarification on this definition would be welcome.

More concretely, the term "undertakings providing digital and data services" could cause questions whether a payment service provider (PSP) functioning as an intermediary PSP could fall inside the definition vis-à-vis the Originating PSP. If this would be the case, this would mean that if it concerns an EU based intermediary PSP, it would fall in scope of the DORA but it would also have to be classified as an "ICT third-party service provider" under the DORA by the Originating PSP. In order to avoid a situation where a financial entity in scope of the DORA will at the same time be classified as an "ICT third-party service provider" by another financial entity and thus potentially be classified as an "Critical ICT third-party service provider" by the ESAs, we would suggest to include language that **financial entities in scope of the DORA cannot be considered as "ICT third-party service provider" by other financial entities in scope of the DORA**.

Furthermore, the EBA Guidelines on Outsourcing arrangements foresee an **exemption** for market information services, global network infrastructures, clearing and settlement arrangements between clearing houses, central counterparties and settlement institutions and their members, global financial messaging infrastructures that are subject to oversight by relevant authorities, correspondent banking services. These arrangements are not to be considered as outsourcing arrangements under the EBA Guidelines and we would suggest that **a similar exemption would be included in DORA to align the frameworks**.

ICT Third-Party Risk – Consistency with EBA Guidelines on Outsourcing Arrangements and other issues

The EBA Guidelines foresee an Outsourcing policy to be put in place under the responsibility of the management body. The requirement in **Article 25** would mean that on top of the Outsourcing policy, an additional Policy on the use of ICT services provided by ICT third-party service providers should be put in place. This could create complexity and potentially confusion. EPIF would therefore suggest to add the following language to this section: "For Institutions in scope of the EBA/GL/2019/02 on Outsourcing Arrangements, the policy on the use of ICT services provided by ICT third-party service providers can be integrated in the Outsourcing Policy of the Institution."

Article 25(4) foresees that "Financial entities shall report at least yearly to the competent authorities information on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the services and functions which are being provided." Under the EBA GL, there is no yearly separate report required. This will constitute an additional reporting on top of all other reporting obligation already in place for payment and e-money institutions. Furthermore, if institutions would make the Register of Information available to Competent Authorities as mentioned in Article 25(4), this should be sufficient to properly inform the Competent Authorities and would be in line with the requirements under the EBA Guidelines.

Article 25(5)(a) states that financial entities shall 'assess whether the contractual arrangement covers a critical or important function', however, there is no guidance as to what assessment criteria should be taken into consideration in order to determine if a function is to be considered as critical or important. EBA Guidelines foresee extensive guidance on this (see EBA/GL/2019/02, section 4, GL 29-31).

Furthermore, the EBA GL foresees the possibility of the use of pooled audits organised jointly with other clients of the same provider and third-party certifications and third-party or internal audit reports, made available by the service provider (see GL 91 and 93). EPIF would suggest to also foresee this possibility under the DORA.

With relation to **Article 25(9),** the EBA GL foresee that an **exit strategy** should be put in place in case of 'critical or major outsourcing.' The wording in Article 25 (9) seems to suggest that an exit strategy should be put in place for all ICT third-party service providers. This would create an important additional burden for payment and e-money institutions and is not aligned with the requirements under the EBA GL. EPIF suggest to rephrase as follows: "*Financial entities shall put in place exit strategies for critical or important functions in order to take into account risks that may emerge at the level of ICT third-party service provider […]".*

We also encourage the ESAs to align the content of the **Register of Information** with the requirements under EBA Guidelines (see GL 54 and 55) listing the information items that should be contained in the Outsourcing Register. EPIF would also suggest to fully align the **key contractual provisions** of Article 27 with the EBA GL.

With regards to the possibility of **contractual arrangement termination** between a critical ICT TPP and the financial entity , competent authorities should give financial entities sufficient time to migrate to a new ICT third-party service provider. In some cases this will be a very complex and time consuming exercise. Moreover, a possibility for financial entities to appeal the decision of the competent authorities should be considered.

The use of third-country ICT service providers

According to the proposal, **all ICT third-party service providers that are deemed critical must have a business/presence in the EU.** Following Brexit, many members of EPIF now find themselves in a situation where

either within the same group or through the provision of a third party services are provided from Great Britain or Northern Ireland.

While we understand the aim of the provision, we believe that as it currently stands it creates many levels of legal uncertainty. It might entail that a financial institution is limiting the choice of use of a critical ICT third-party service provider by giving preference to those established in the EU. These provisions would limit the payment/e-money institutions free choice as to their third-party ICT providers and hinder their ability to adopt the most innovative technological solutions, and thus the competitiveness of financial entities in the Union. Therefore, further clarification is needed, namely on the criteria and definition of Third-Country ICT Service Provider in relation to the concept of 'business/presence' in the EU.

EPIF is also concerned about the operational impact regarding the powers of the Lead Overseer to address recommendations around **subcontracting**, if the envisaged sub-contractor is an ICT third-party service provider or an ICT sub-contractor established in a third country (Article 31(d)(iv)). If such a restriction would be imposed, sufficient time should be given to implement any required changes.

Other comments

Definition of 'management body' – for payment/e-money institutions, management body is defined in the EBA Guidelines on ICT and security Risk Management and we would suggest to include that reference in Article 3(22).

Information sharing arrangements – A legal basis for information sharing is considered a positive development. However, it could be useful to clarify the interaction of the provisions in Article 40 with the GDP, as certain elements of cyber threat information or intelligence may potentially contain personal data. It is not clear if such information can be shared on the basis of the "public interest" ground for processing.

EPIF also fears that a 12-month deadline is too short to achieve the implementation of the provisions of the Regulation. Financial entities will need to carry out a full gap-analysis and, where appropriate, amend their internal policies and procedures, and create a framework for their implementation. Therefore, an extension of the deadline would be needed to implement the requirements successfully. A **24-month implementation deadline** seems more reasonable. Alternatively, an extension could take the form of a prioritization of requirements with differentiated stages of implementation, comparable to what is already foreseen for Articles 23 and 24 of the proposal.

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 190 authorised payment institutions and other non-bank payment providers as our members offering services in every part of Europe. **EPIF** thus represents roughly one third of all authorized Payment Institutions ("PI") in Europe. All of our members operate online. Our diverse membership includes a broad range of business models, including:

- Three-party Card Network Schemes
- E-Money Providers
- E-Payment Service Providers and Gateways
- Money Transfer Operators
- Acquirers
- Digital Wallets
- FX Payment Providers and Operators
- Payment Processing Services
- Card Issuers
- Independent Card Processors
- Third Party Providers
- Payment Collectors

EPIF seeks to represent the voice of the PI industry and the non-bank payment sector with EU institutions, policy-makers and stakeholders. We aim to play a constructive role in shaping and developing market conditions for payments in a modern and constantly evolving environment. It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

We wish to be seen as a provider for efficient payments in that single market and it is our aim to increase payment product diversification and innovation tailored to the needs of payment users (e.g. via mobile and internet).