European Payment Institutions Federation aisbl

EPIF Secretariat
c/o Afore Consulting
14B Rue de la Science
1040 Brussels

17 February 2021

Dear all,

We understand that during the latest Council Working Group meeting on DORA, the European Commission's proposal for ICT operational resilience in the financial services sector, a number of Member States raised the question whether payment institutions authorised under the Payment Services Directive should be exempted from the scope of DORA.

The European Payment Institutions Federation (EPIF) represents the interests of the non-bank payment sector in the EU. EPIF brings together European and international companies in the remittance sector, three party card schemes, third party providers, cross-border acquirers, payment processors, electronic payment providers, fx traders, electronic wallet providers and operators of mobile payments.

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. These requirements 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.

EPIF members are of course also already subject to the existing ICT and outsourcing guidelines by the European Banking Authority.

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. Specifically, under DORA, payment institutions will be excluded from ICT-related incident reporting under PSD2 but would still have to report other major operational or security incidents that are not considered ICT-related incidents under Article 96 (1) PSD2. Moreover, the reporting deadlines 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.

A third concern by 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. One 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.

A fourth concern is that according to the proposal, all ICT third-party service providers that are deemed critical must have a business/presence in the EU. While we understand the aim of the provision, we believe that as it currently stands it creates many levels of legal uncertainty. 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.

In the light of these comments, 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.

We look forward to hearing from you and a very constructive dialogue.

Yours sincerely,

Nickolas Reinhardt, Head of the EPIF Secretariat