Digital Finance: amending Directive regarding Digital Operational Resilience requirements

2020/0268(COD) - 07/12/2021 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Economic and Monetary Affairs adopted the report by Mikuláš PEKSA (Greens/EFA, CZ) on the proposal for a directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341.

This legislative proposal is part of the Digital Finance Package. It introduces:

- targeted changes to existing EU financial services directives to align them with the requirements on network and information systems and ICT risk management and reporting laid down in the DORA Regulation and clarify certain provisions to ensure ICT risks are fully addressed;

- targeted changes to the Markets in Financial Instruments Directive (MiFID) to provide legal certainty as regards the definition of crypto assets and to establish a temporary exemption allowing natural persons to participate to the pilot regime for a distributed ledger technology (DLT) Multilateral Trading Facility, under certain conditions.

The committee responsible recommended that the European Parliament's position adopted at first reading under the ordinary legislative procedure should amend the proposal as follows:

ICT risk requirements

As the existing provisions of EU law are not fully harmonised, Members stressed the need to avoid over-regulation and to ensure that these provisions are appropriate to the constantly changing reality in this area. It is also a question of ensuring the proper functioning of the internal market while promoting **proportionality**, especially as regards SMEs, other small financial entities and other micro-enterprises, with a view to reducing compliance costs.

Amendment to Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (CRD)

The relevant provisions of the CRD have been clarified so that ICT risk is explicitly taken into account.

The amendments stipulate that institutions must have robust governance arrangements, including: (i) a clear organisational structure with well-defined, transparent and consistent division of responsibilities; (ii) effective processes to identify, manage, monitor and report the risks to which they are or may be exposed; (iii) adequate internal control mechanisms, including sound administrative and accounting procedures, network and information systems set up and managed in accordance with the DORA Regulation, and remuneration policies and practices that promote sound and effective risk management.

Institutions should implement policies and processes to **identify, monitor and manage their exposures to operational risk**, including risk arising from outsourcing of functions and ICT third-party risk service providers as defined in the DORA, and to model risk and to cover low-frequency high-severity events.

In addition, institutions should have adequate contingency and business continuity plans, including ICT business continuity policy and disaster recovery plans in place, managed and tested so that they can

continue to operate in the event of severe business disruption and limit losses incurred as a consequence of such a disruption.

Amendment to Directive 2014/59/EU establishing a framework for the recovery and resolution of credit institutions and investment firms (BBRD)

ICT risks and vulnerabilities to digital operational resilience may impact the network and information systems that support critical functions of the banks and undermine the resolution objectives. It is essential to select the right IT service contracts to ensure business continuity and provide the necessary data in the event of resolution.

In order to be aligned with the objectives of the Union framework for operational resilience, it is proposed to amend Directive 2014/59/EU to ensure that information on operational resilience is taken into account in the context of resolution planning and the assessment of institutions' resolvability.

Amendment to Directive (EU) 2015/849 (prevention of the use of the financial system for the purpose of money laundering or terrorist financing)

The amended text stresses the need to ensure operational resilience to strengthen the ability of financial institutions to combat money laundering and terrorist financing, especially in light of the increasing and emerging risks opened up in the post-COVID environment, where it is easier for criminals to exploit weaknesses and gaps in institutions' systems and controls.

Therefore, it is proposed to amend Directive (EU) 2015/849 to explicitly include, in respect of obligated entities that fall within the scope of the DORA Regulation, digital operational resilience requirements as part of the policies, controls and procedures put in place by those obliged entities to mitigate and effectively manage money laundering and terrorist financing risks.

Amendment to Directive (EU) 2015/2366 (payment services)

The Directive sets out specific rules on ICT security controls and mitigation elements for the purposes of authorisation to perform payment services. Members propose to amend these authorisation rules to align them with the DORA Regulation.

Furthermore, in order to reduce the administrative burden and avoid complexity and duplication of reporting obligations, the incident reporting rules in that Directive should cease to apply to payment service providers falling within the scope of Chapter III of the DORA Regulation, thus creating a single and fully harmonised incident reporting mechanism for payment service providers, applicable to all operational or security incidents related to payments or non-payments.