Digital Finance: amending Directive regarding Digital Operational Resilience requirements

2020/0268(COD) - 10/11/2022 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 553 votes to 19, with 40 abstentions, a legislative resolution on the proposal for a directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341.

This amending Directive is part of the Digital Finance Package. It introduces **targeted changes to the existing EU financial services directives** to align them with the risk management and reporting requirements for ICT and networks and information systems set out in the Digital Operational Resilience of the Financial Sector (DORA) Regulation, and to clarify certain provisions to ensure that ICT risks are fully taken into account.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amends the proposal as follows:

Objective of the amendments

The Directive provides for a series of amendments which are necessary to provide legal clarity and consistency with regard to the application by financial entities authorised and supervised under the existing Directives of **various digital operational resilience requirements** which are necessary for the conduct of their business and the provision of services, thereby ensuring the proper functioning of the internal market.

The amended text emphasises the need to ensure that these requirements are in line with market developments, while promoting **proportionality**, in particular with regard to the size of financial entities and the specific regimes to which they are subject, in order to reduce 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.

In addition, institutions should have **adequate contingency and business continuity plans**, including information and communications technology (ICT) business continuity policies and plans and **ICT response and recovery plans**. These plans should be established, managed and tested in accordance with the DORA Regulation to ensure that institutions can continue to operate in the event of a serious business disruption and limit the losses incurred as a result 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)

According to the amended text, the resolution plan should include:

- a demonstration of how critical functions and core business lines could be legally and economically separated, to the extent necessary, from other functions so as to ensure continuity and digital operational resilience upon the failure of the institution;

- a description of essential operations and systems for maintaining the continuous functioning of the institution's operational processes, including network and information systems as referred to in the DORA Regulation.

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. These authorisation rules to align them with the DORA Regulation.

Furthermore, in order to reduce the administrative burden and to avoid complexity and duplication of reporting obligations, the incident reporting rules contained in that Directive should cease to apply to payment service providers which are covered by that Directive and which are also covered by the DORA Regulation, thus allowing them to benefit from a single and fully harmonised incident reporting mechanism for payment service providers, whether or not such incidents are ICT-related.

Under the amended text, authorisation as a payment institution should be conditional on the submission of an application to the competent authorities of the home Member State, accompanied by the following information:

- a description of the applicant's governance arrangements and internal control mechanisms, including administrative, risk management and accounting procedures as well as arrangements for the use of ICT services in accordance with the DORA Regulation, which demonstrates that those governance arrangements and internal control mechanisms are proportionate, appropriate, sound and adequate;

- a description of the procedure in place to monitor, handle and follow up a security incident and security related customer complaints, including an incident reporting mechanism which takes account of the notification obligations of the payment institution laid down in the DORA Regulation;

- a description of business continuity arrangements including a clear identification of the critical operations, effective ICT business continuity policy and plans and ICT response and recovery plans and a procedure to regularly test and review the adequacy and efficiency of such plans.

Transposition

Member States should transpose the Directive no later than 24 months after the date of entry into force of this amending Directive.