












Procedure file

Basic information	
<p>COD - Ordinary legislative procedure (ex-codecision procedure) 2020/0268(COD) Directive</p>	Procedure completed
<p>Digital Finance: amending Directive regarding Digital Operational Resilience requirements</p> <p>Amending Directive 2006/43 2004/0065(COD) Amending Directive 2009/138 2007/0143(COD) Amending Directive 2009/65 2008/0153(COD) Amending Directive 2011/61 2009/0064(COD) Amending Directive 2013/36 2011/0203(COD) Amending Directive 2014/65 2011/0298(COD) Amending Directive 2015/2366 2013/0264(COD) Amending Directive 2016/2341 2014/0091(COD)</p> <p>Subject</p> <p>2.50.03 Securities and financial markets, stock exchange, CIUTS, investments 2.50.04 Banks and credit 2.50.05 Insurance, pension funds 2.50.08 Financial services, financial reporting and auditing 2.50.10 Financial supervision 3.45.03 Financial management of undertakings, business loans, accounting</p> <p>Legislative priorities Joint Declaration 2022 Joint Declaration 2021</p>	

Key players			
European Parliament	Committee responsible	Rapporteur	Appointed
	 Economic and Monetary Affairs	 PEKSA Mikuláš	15/10/2020
		Shadow rapporteur	
		 BENJUMEA BENJUMEA Isabel	
		 FUGLSANG Niels	
		 YON-COURTIN Stéphanie	
		 BECK Gunnar	
		 ZĪLE Roberts	
		 SCHIRDEWAN Martin	
	Committee for opinion	Rapporteur for opinion	Appointed
	 Industry, Research and Energy	The committee decided not to give an opinion.	
	 Internal Market and Consumer Protection	The committee decided not to give an opinion.	

Key events

24/09/2020	Legislative proposal published	COM(2020)0596	Summary
17/12/2020	Committee referral announced in Parliament, 1st reading		
11/02/2021	Referral to associated committees announced in Parliament		
01/12/2021	Vote in committee, 1st reading		
01/12/2021	Committee decision to open interinstitutional negotiations with report adopted in committee		
07/12/2021	Committee report tabled for plenary, 1st reading	A9-0340/2021	Summary
13/12/2021	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 71)		
15/12/2021	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 71)		
12/07/2022	Approval in committee of the text agreed at 1st reading interinstitutional negotiations	PE734.197 GEDA/A/(2022)005010	
09/11/2022	Debate in Parliament		
10/11/2022	Results of vote in Parliament		
10/11/2022	Decision by Parliament, 1st reading	T9-0382/2022	Summary
28/11/2022	Act adopted by Council after Parliament's 1st reading		
14/12/2022	Final act signed		
27/12/2022	Final act published in Official Journal		

Technical information

Procedure reference	2020/0268(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Directive
	Amending Directive 2006/43 2004/0065(COD) Amending Directive 2009/138 2007/0143(COD) Amending Directive 2009/65 2008/0153(COD)

	Amending Directive 2011/61 2009/0064(COD) Amending Directive 2013/36 2011/0203(COD) Amending Directive 2014/65 2011/0298(COD) Amending Directive 2015/2366 2013/0264(COD) Amending Directive 2016/2341 2014/0091(COD)
Legal basis	Treaty on the Functioning of the EU TFEU 114-p1; Rules of Procedure EP 57; Treaty on the Functioning of the EU TFEU 053-p1
Other legal basis	Rules of Procedure EP 159
Mandatory consultation of other institutions	European Economic and Social Committee
Stage reached in procedure	Procedure completed
Committee dossier	ECON/9/04233

Documentation gateway					
Legislative proposal		COM(2020)0596	24/09/2020	EC	Summary
Document attached to the procedure		SEC(2020)0309	24/09/2020	EC	
Document attached to the procedure		SWD(2020)0203	24/09/2020	EC	
Document attached to the procedure		SWD(2020)0204	24/09/2020	EC	
Committee draft report		PE689.790	18/03/2021	EP	
Amendments tabled in committee		PE693.614	27/05/2021	EP	
Committee opinion	JURI	PE693.586	06/07/2021	EP	
Committee report tabled for plenary, 1st reading/single reading		A9-0340/2021	07/12/2021	EP	Summary
Coreper letter confirming interinstitutional agreement		GEDA/A/(2022)005010	29/06/2022	CSL	
Text agreed during interinstitutional negotiations		PE734.197	07/07/2022	EP	
Text adopted by Parliament, 1st reading/single reading		T9-0382/2022	10/11/2022	EP	Summary
Draft final act		00042/2022/LEX	14/12/2022	CSL	
Commission response to text adopted in plenary		SP(2022)688	17/01/2023	EC	

Final act
Directive 2022/2556 OJ L 333 27.12.2022, p. 0153 Summary

Digital Finance: amending Directive regarding Digital Operational Resilience requirements

PURPOSE: to amend or clarify certain provisions in existing EU financial services directives.

PROPOSED ACT: Directive of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: this proposal is part of the Digital Finance package, a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks. The digital finance package includes a new [Strategy on digital finance for the EU financial sector](#) with the aim to ensure that the Unions financial services legislation is fit for the digital age, and contributes to a future-ready economy that works for the people, including by enabling the use of innovative technologies. The Union has a stated and confirmed policy interest in developing and promoting the uptake of transformative technologies in the financial sector, including blockchain and distributed ledger technology (DLT).

This package also includes a proposal for a [proposal](#) on crypto-asset markets, a [proposal](#) for digital operational resilience, and a [proposal](#) on a common a EU pilot regime.

The particular reasons for this proposal for a directive is that, in order to provide legal certainty as regards crypto assets and achieve the objectives of strengthening digital operational resilience, it is necessary to establish a temporary exemption for multilateral trading facilities and amend or clarify certain provisions in existing EU financial services directives.

CONTENT: the proposed Directive puts forward a set of amendments that appear necessary to bring legal clarity and consistency in relation to the application by financial entities that are authorised and supervised in accordance with those Directives of various digital operational resilience requirements that are necessary in the pursuit of their activities, thus guaranteeing the smooth functioning of the internal market.

All Articles relate to and complement the proposal for a regulation on digital operational resilience.

In particular, they amend the various operational risk or risk management requirements foreseen in the following Directives:

- 2006/43/EC on statutory audits of annual accounts and consolidated accounts,
- 2009/65/EC on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities,
- 2009/138/EU on the taking-up and pursuit of the business of insurance and reinsurance,
- 2011/61/EU on alternative investment fund managers,
- EU/2013/36 on access to the activity of credit institutions and the prudential regulation of credit institutions and investment firms,
- 2014/65/EU on markets in financial instruments,
- (EU) 2015/2366 on payment services in the internal market,
- EU/2016/2341 on the activities and supervision of institutions for occupational retirement provision, by introducing precise cross-references in those provisions and thus attain legal clarity.

Digital Finance: amending Directive regarding Digital Operational Resilience requirements

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.

Digital Finance: amending Directive regarding Digital Operational Resilience requirements

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 institutions 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 applicants 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.

Digital Finance: amending Directive regarding Digital Operational Resilience requirements

PURPOSE: to introduce targeted amendments to existing EU financial services directives to align them with the requirements set out in the Digital Operational Resilience of the Financial Sector (DORA) Regulation.

LEGISLATIVE ACT: Directive (EU) 2022/2556 of the European Parliament and of the Council -amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector.

CONTENT: the amending Directive 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 Digital Operational Resilience of the Financial Sector ([DORA Regulation](#)) and clarify certain provisions to ensure information and communication technology (ICT) risks are fully addressed.

The Directive provides for a set of amendments that appear necessary to bring legal clarity and consistency in relation to the application by financial entities that are authorised and supervised in accordance with those Directives of various digital operational resilience requirements that are necessary in the pursuit of their activities, thus guaranteeing the smooth functioning of the internal market.

The Directive emphasises the need to ensure the adequacy of those requirements in relation to market developments, while encouraging proportionality in particular with regard to the size of financial entities and the specific regimes to which they are subject, with the aim of reducing compliance costs.

The Directive amends the various operational risk or risk management requirements foreseen in the following Directives:

- 2009/65/EC on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities,

- 2009/138/EU on the taking-up and pursuit of the business of insurance and reinsurance,

- 2011/61/EU on alternative investment fund managers,

- 2013/36/EU on access to the activity of credit institutions and the prudential regulation of credit institutions and investment firms,

- 2014/65/EU on markets in financial instruments,

- 2015/2366/EU on payment services in the internal market,

- 2016/2341/EU on the activities and supervision of institutions for occupational retirement provision

ENTRY INTO FORCE: 16.1.2023.

TRANSPPOSITION AND APPLICATION: from 17.1.2025.