OPINION OF THE EUROPEAN CENTRAL BANK

of 11 April 2022

on the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Introduction and legal basis

On 16 December 2020 the European Commission adopted the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 ([1]) (hereinafter the 'proposed directive'). On 3 December 2021 the Council of the European Union agreed its general approach on the proposed directive ([2]). The competence of the European Central Bank (ECB) to deliver an opinion is based on the second subparagraph of Article 127(4) of the Treaty on the Functioning of the European Union, as the proposed directive contains provisions falling within the ECB's fields of competence, in particular, the promotion of the smooth operation of payment systems, the contribution to the smooth conduct of policies pursued by competent authorities relating to the stability of the financial market system, and the ECB's tasks concerning the prudential supervision of credit institutions pursuant to the fourth indent of Article 127(2), and Articles 127(5) and 127(6) of the Treaty. In accordance with the first sentence of Article 17.5 of the Rules of Procedure of the European Central Bank, the Governing Council has adopted this opinion.

General observations

The ECB strongly supports the objectives of the proposed directive to increase the level of cyber resilience across all relevant sectors, reduce inconsistencies across the internal market and improve the level of situational awareness and the collective capability to prepare and respond by ensuring efficient cooperation in the Union.

The ECB acknowledges the importance of maintaining strong links between the proposed directive and the financial sector, which should remain part of the network and information systems (NIS) ecosystem to promote the consistent assessment of risks related to information and communications technology (ICT) across the Union and foster effective cross-sectoral information exchange and collaboration when dealing with cyber threats. To that end, it should be possible for the competent authorities under the proposed regulation of the European Parliament and of the Council on digital operational resilience for the financial sector ([3]) (hereinafter 'DORA') to participate in the strategic policy discussions and the technical workings of the NIS Cooperation Group, as well as to exchange information and further cooperate with the single points of contact and the national Computer Security Incident Response Teams referred to in the proposed directive ([4]).

1. Scope of the proposed directive

1.1. The ECB understands that, in relation to financial sector entities, DORA will be regarded as sector-specific legislation introducing requirements on cybersecurity risk management and incident notification that are at least equivalent in effect to those laid down in the proposed directive ([5]). Therefore, the provisions of the proposed directive that relate to cybersecurity risk management, reporting obligations, information sharing, and supervision and enforcement will not apply to any financial entities covered by DORA ([6]). As clarified in the recitals of the proposed directive,

([1]) COM(2020) 823 final.
([2]) Available on the Council website at www.consilium.europa.eu
([3]) COM(2020) 595 final.
([4]) See paragraph 1.5 of Opinion CON/2021/20 of the European Central Bank of 4 June 2021 on a proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (OJ C 343, 26.8.2021, p. 1). All ECB opinions are published on EUR-Lex. Articles 17(5) and 42 of DORA; Article 11 of the proposed directive.
([5]) Article 2(6) of the proposed directive.
([6]) Recital 13 and Article 2(6) of the proposed directive.

the provisions of DORA that relate to ICT risk management measures, management of ICT-related incidents and incident reporting, digital operational resilience testing, information-sharing arrangements and ICT third-party risk should apply instead of those of the proposed directive ([7]).

1.2. The ECB also notes that the Council, in its general approach on the proposed directive, puts forward an amendment to exclude 'entities that carry out activities in the areas of judiciary, parliaments or central banks' ([8]) from the application of the proposed directive. The ECB understands that the proposed amendment would extend to all the basic tasks and competences of the European System of Central Banks (ESCB), as set out in Article 127(2) of the Treaty and in Article 3.1 of the Statute of the European System of Central Banks and of the European Central Bank (hereinafter the 'Statute of the ESCB'), such as the promotion of the smooth operation of payment systems. In this regard, Eurosystem-owned and operated financial market infrastructures, such as TARGET2 and TARGET2-Securities, are considered as falling under the Council's proposed exclusion of central banks from the application of the proposed directive.

2. **ESCB and Eurosystem oversight competences**

2.1. Alongside the ESCB's primary objective of maintaining price stability, and in accordance with Article 127(2) of the Treaty, one of the basic tasks to be carried out through the ESCB is to promote the smooth operation of payment systems ([9]). In the performance of this basic task, the ECB and the national central banks may provide facilities, and the ECB may make regulations, to ensure efficient and sound clearing and payments systems within the Union and with other countries ([10]). In the exercise of its oversight role, the ECB adopted Regulation of the European Central Bank (EU) No 795/2014 (ECB/2014/28) ([11]) (hereinafter the 'SIPS Regulation'), which translates the CPSS-IOSCO Principles for Financial Market Infrastructures ([12]) into directly applicable law. The SIPS Regulation sets out requirements for both large-value and retail payment systems of systemic importance, whether public or privately owned. The requirements under the SIPS Regulation already include, among others, operational risk management and the establishment of a cyber resilience framework ([13]).

2.2. In addition to systemically important payment systems, Eurosystem oversight covers non-systemically important payment systems, electronic payment instruments, schemes and arrangements, and other infrastructures and critical service providers, as set out in the Eurosystem oversight policy framework ([14]). Payment systems and other arrangements subject to Eurosystem oversight are not expressly included in the scope of the proposed directive ([15]). At the same time, given that the proposed directive is a minimum harmonisation instrument ([16]), implementing legislation adopted by the Member States could eventually overlap with the Eurosystem's oversight competence. To avoid this, the ESCB's competences under the Treaty and the Statute of the ESCB, and the Eurosystem's competences under the SIPS Regulation and generally under the Eurosystem oversight policy framework, should be expressly acknowledged in the recitals of the proposed directive.

([7]) Recital 13 of the proposed directive.
([8]) Article 2(3a), first subparagraph, point (b) of the Council general approach on the proposed directive.
([9]) Article 127(2) TFEU, as mirrored in Article 3.1 of the Statute of the ESCB.
([10]) Article 22 of the Statute of the ESCB.
([11]) Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems *(ECB/2014/28)* (OJ L 217, 23.7.2014, p. 16).
([12]) See Committee on Payment and Settlement Systems (CPSS) and Technical Committee of the International Organization of Securities Commissions (IOSCO), Principles for Financial Market Infrastructures, April 2012, available on the Bank for International Settlements website at www.bis.org. Responsibility D thereof states that 'all CPSS and IOSCO members are expected to apply the principles to the relevant FMIs in their jurisdictions to the fullest extent allowed by the legal framework in their jurisdiction'.
([13]) Article 15 of Regulation (EU) No 795/2014 (ECB/2014/28).
([14]) Eurosystem oversight policy framework, revised version (July 2016), available on the ECB website at www.ecb.europa.eu
([15]) Article 2 of the proposed directive and Annexes I and II to the proposed directive.
([16]) Article 3 of the proposed directive.

3. ICT third-party risk, management of large-scale incidents and crises, information-sharing and national cybersecurity strategy

3.1. *ICT third-party risk management*

3.1.1. The proposed directive empowers competent authorities, when exercising their enforcement powers in relation to essential entities, to issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations of the proposed directive ([17]). At the same time, the 'Lead Overseer' designated under DORA may address recommendations to critical ICT third-party service providers to manage the potential systemic risks entailed by outsourcing practices and ICT third-party concentration ([18]).

3.1.2. Considering that an essential entity under the proposed directive may also be designated a critical ICT third-party service provider pursuant to DORA, the ECB reiterates ([19]) that the issuance of conflicting recommendations and binding instructions should be avoided. In this regard, the ECB welcomes the Council's general approach on the proposed directive. According to that approach competent authorities are to inform the 'Oversight Forum', established under DORA, when exercising their supervisory and enforcement powers in relation to an essential entity designated as a critical ICT third-party service provider under DORA ([20]).

3.2. *Management of large-scale incidents and crises*

3.2.1. In accordance with the proposed directive ([21]), Member States must designate one or more competent authorities responsible for the management of large-scale incidents and crises. As the recitals of the proposed directive clarify, a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Large-scale incidents may turn into fully-fledged crises, disrupting the proper functioning of the internal market ([22]).

3.2.2. While the competent authorities designated under DORA remain responsible for the management of cybersecurity incidents concerning financial entities, cooperation with the structures and authorities established pursuant to the proposed directive will be critical to ensuring a coordinated response across the Union. To this end, the ECB would welcome the participation of competent authorities designated under DORA, including the ECB, in the European Cyber Crises Liaison Organisation Network (EU-CyCLONe) ([23]), when large-scale cybersecurity incidents and crises affect the financial sector.

3.3. *Information-sharing*

3.3.1. As indicated above, the ECB strongly supports cooperation between competent authorities designated under DORA with the structures and authorities established pursuant to the proposed directive. In particular, information sharing among authorities may enable cross-sectoral learning, contribute to the prevention and effective management of cyberattacks, and promote the consistent assessment of ICT-related risks across the Union. Nonetheless, the ECB emphasises that information exchange should take place where there are clearly established classification and information-sharing mechanisms, coupled with adequate safeguards to ensure confidentiality ([24]). The ECB welcomes the Council's general approach on the proposed directive, which proposes the regular exchange of

([17]) Article 29(4), point (b) of the proposed directive.
([18]) Article 31 of DORA.
([19]) See paragraph 1.2 of Opinion CON/2021/20.
([20]) Article 29(10) of the Council general approach on the proposed directive.
([21]) Article 7(1) of the proposed directive.
([22]) Recital 27 of the proposed directive.
([23]) Article 14 of the proposed directive.
([24]) See paragraph 1.5 of Opinion CON/2021/20.

relevant information between authorities ([25]), the establishment of cooperation arrangements specifying a mechanism for the exchange of information ([26]), and the automatic and direct forwarding of incident notifications ([27]). In this respect, it should be ensured that information that is confidential pursuant to the provisions on professional secrecy under DORA ([28]) or the relevant sector-specific legislation ([29]) can be exchanged with the competent authorities referred to in the proposed directive only where that exchange is needed for the competent authorities to apply the provisions of the proposed directive ([30]).

3.4. *National cybersecurity strategy*

3.4.1. Under the proposed directive, Member States are required to adopt national cybersecurity strategies to define the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of cybersecurity ([31]). As clarified in the recitals of the proposed directive, Member States should continue to include the financial sector in their respective cybersecurity strategies ([32]). Indicatively, as part of their national cybersecurity strategies, Member States should adopt policies addressing cybersecurity in the supply chain for ICT products and services used by entities for the provision of their services. Insofar as the financial sector is concerned, national cybersecurity strategies should be consistent with the regulatory framework that emanates from DORA. In this respect, the ECB considers that further clarifications are needed to ensure that national cybersecurity strategies are consistent with sector-specific legislation.

Where the ECB recommends that the proposed directive is amended, a specific drafting proposal is set out in a separate technical working document accompanied by an explanatory text to this effect. The technical working document is available in English on EUR-Lex.

Done at Frankfurt am Main, 11 April 2022.

The President of the ECB
Christine LAGARDE

([25]) Article 11(5) of the Council general approach on the proposed directive.
([26]) Recital 23a of the Council general approach on the proposed directive.
([27]) Recital 13 of the Council general approach on the proposed directive.
([28]) Article 49 of DORA.
([29]) Articles 53 to 62 of Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).
([30]) Articles 2(5) and 11(4) of the proposed directive.
([31]) Article 5 of the proposed directive.
([32]) Recital 13 of the proposed directive.