EUROPEAN CENTRAL BANK

EUROSYSTEM

EN **ECB-PUBLIC**

OPINION OF THE EUROPEAN CENTRAL BANK

of 18 May 2018

on the establishment of a framework for the security of network and information systems of general interest

(CON/2018/27)

Introduction and legal basis

On 18 April 2018 the European Central Bank (ECB) received a request from the Belgian Minister for Finance for an opinion on a draft law establishing a framework for the security of network and information systems of general interest (hereinafter the 'draft law').

The ECB's competence to deliver an opinion is based on Articles 127(4) and 282(5) of the Treaty on the Functioning of the European Union, in conjunction with Article 127(6) of the Treaty and the third, fifth and sixth indents of Article 2(1) of Council Decision 98/415/EC[1], as the draft law relates to the Nationale Bank van België /Banque Nationale de Belgique (NBB), payment and settlement systems, rules applicable to financial institutions insofar as they materially influence the stability of financial institutions and markets and the ECB's tasks concerning the prudential supervision of credit institutions. 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.

1. Purpose of the draft law

1.1 The purpose of the draft law is to implement Directive (EU) 2016/1148 of 6 July 2016 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union[2] (hereinafter the 'NIS Directive'), taking into account Article 1(7) thereof, whereby sector-specific Union legal acts imposing equivalent obligations on operators of essential services either to ensure the security of their network and information systems or to notify incidents apply[3].

1.2 In particular, the Law of 1 July 2011 on the security and protection of critical infrastructures[4] (hereinafter the 'Law on critical infrastructures'), which implemented Directive 2008/114/EU of 8 December 2008 on the identification and designation of European critical infrastructures and the

1 Council Decision 98/415/EC of 29 June 1998 on the consultation of the European Central Bank by national authorities regarding draft legislative provisions (OJ L 189, 3.7.1998, p. 42).

2 OJ L 194, 19.7.2016, p. 1.

3 Explanatory memorandum to the draft law, p. 6.

4 *Loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques/wet van 1 juli betreffende de beveiliging en de bescherming van de kritieke infrastructuren*.

assessment of the need to improve their protection[5], established in Belgium a comprehensive framework for critical infrastructures, defined as an asset, system or part thereof which is essential for the maintenance of vital societal functions, health, security, economic or social well-being of people, the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions. These critical infrastructures are identified, designated and closely monitored by sectoral authorities, which must ensure that the operators thereof adopt and implement a security plan with a view to anticipating, alleviating and neutralising the risk of interruption of their functioning or destruction. The NBB has been appointed as the sectoral authority for the financial sector.

1.3 For the sake of consistency with the Law on critical infrastructures, critical infrastructures designated by the NBB automatically qualify as operators of essential services under the draft law. Furthermore, all of the provisions of the draft law whereby sectoral authorities may subject operators of essential services to security requirements, internal and external audit, control, verifications and inspections apply to all sectors, with the exception of the financial sector. The operators of essential services falling within the ambit of the financial sector are only subject to the provisions of the draft law relating to incident notifications and administrative sanctions. While the NBB will, for this purpose, act as the sectoral authority for credit institutions and central counterparties, the Authority for Financial Services and Markets will act in this capacity for the operators of trading platforms.

1.4 The draft law furthermore establishes mechanisms of cooperation and/or exchange of information at the domestic and international levels. At the domestic level, such cooperation and exchange of information, including for incident notifications, take place between the Centre for Cybersecurity Belgium (CCB), the Directorate General of the Crisis Centre of the internal public federal service ('DGCC'), the sectoral authorities as well as, if need be, the public prosecutors, police and the Belgian Authority for Data Protection. At the international level, the exchange of information takes place with European Union authorities and foreign or national authorities when it is necessary for the implementation of the draft law.

1.5 The draft law amends the Law of 22 February 1998 setting out the Organic Statute of the NBB[6] (hereinafter 'the NBB Organic Law') in order to formally lay down the NBB's competence to control the compliance by financial sector operators with its provisions, to empower the Commission for Sanctions to apply the administrative sanctions stipulated and to authorise exchange of information with the domestic authorities competent for the security of network and information systems of general interest.

2. General observations

2.1 The draft law implements the NIS Directive which is, according to its Article 3, a minimum harmonisation directive, meaning that Member States may adopt or maintain provisions with a view

5 OJ L 345, 23.12.2008, p. 75

6 *Loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique/wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België*.

to achieving a higher level of security of network and information systems than provided for under the Directive.

2.2 As previously noted by the ECB[7], the ECB supports the aim of the NIS Directive of ensuring a high common level of network and information security (NIS) across the Union and of achieving a consistency of approach in this field across business sectors and Member States. It is important to ensure that the internal market is a safe place to do business and that all Member States have a certain minimum level of preparedness for cybersecurity incidents.

2.3 In a previous opinion[8], the ECB also welcomed the appointment of the NBB as the relevant authority for the purpose of the Law on critical infrastructures, which enhances the NBB's ability to ensure financial stability and prevent or mitigate systemic risks.

2.4 The ECB takes note of the particular legislative approach taken by the draft law.

On the one hand, the draft law expands the scope of application beyond the NIS Directive, which applies to credit institutions, central counterparties (CCPs) and operators of trading platforms which have an establishment in Belgium and which effectively exercise in Belgium an activity linked to the provision of at least one essential service. Under the draft law critical infrastructures notified by the NBB under the Law on critical infrastructures also automatically qualify as operators of essential services.

On the other hand, the draft law subjects operators of essential services in the financial sector to mere incident notification duties and administrative sanctions. All other provisions on security requirements, internal and external audit, control, verifications and inspections, which apply to all other sectors, are waived in respect of the financial sector. In this manner, and in accordance with Article 1(7) of the NIS Directive, the draft law relies on the existing supervisory and oversight competences of the relevant competent authorities, which already impose equivalent obligations on operators of essential services to ensure the security of their network and information systems. These relevant authorities encompass, at the European level, the ECB in the context of the Single Supervisory Mechanism and the Eurosystem in the context of the oversight of market infrastructures. At the national level, the existing supervisory and oversight competences of the NBB are stipulated in the NBB Organic Law, which also grants the NBB regulatory, investigative and sanctioning powers over all financial institutions in the discharge of its tasks. Specific requirements and recommendations on the management of operational risk are provided in sectoral legislation and frameworks applicable to credit institutions[9], systemically important

7 See paragraph 2.1 of Opinion CON/2014/58, paragraph 2.1 of Opinion CON/2017/10 and paragraph 2.2 of Opinion CON/2018/22. All ECB opinions are published on the ECB's website at www.ecb.europa.eu.

8 See paragraphs 1.2 and 3.1 of Opinion CON/2014/17.

9 Under Article 85 of Directive (EU) 2013/36 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 and investments firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338), credit institutions implement policies and processes to evaluate and manage exposure to operational risk, which must also be taken into account in calculating capital requirements under Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investments firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

payment systems[10], prominently important retail payment systems and other retail payment systems[11], other financial market infrastructures (including CCPs and central securities depositories)[12], payment cards, credit transfers, direct debits and e-money[13], payment service providers[14], critical service providers within the meaning of the Eurosystem's Oversight Policy Framework[15] as well as processors of payment transactions within the meaning of the Belgian Law of 24 March 2017 on the processors of payment transactions[16].

2.5 As a consequence of this legislative approach, the draft law does not prejudice the existing competences of the ECB and the NBB as regards the supervision of credit and financial institutions and the oversight of market infrastructures. In this respect, the NBB remains exclusively competent, under its existing supervisory and oversight competences, including under the Law on critical infrastructures, to subject operators of essential services to security requirements, internal and external audit, control, verifications and inspections as well as to impose sanctions. The new administrative authorities created in Belgium under the draft law (namely, the CCB and the DGCC) may not interfere with these powers of the NBB, whose institutional and operational independence is therefore guaranteed.

2.6 In adopting this approach, the draft law neither encroaches on the ECB or the Eurosystem's competences nor conflicts with existing Union legal acts, as the incident notification duties applicable to operators of essential services in the financial sector are in addition to the existing supervisory and oversight framework which continues to apply, without any undue interference by the draft law.

3. Tasks of the NBB

3.1 The draft law introduces into the NBB Organic Law a new chapter in which the NBB's competence to control the compliance by operators of the financial sector with the draft law is formalised. This new chapter, which is inserted into the chapter relating to the micro and macrosupervision of

10 See Article 15 of Regulation (EU) No 795/2014 of the European Central Bank of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28) (OJ L 217, 23.7.2014, p. 16), as amended by Regulation (EU) 2017/2094 of the European Central Bank of 3 November 2017 amending Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (ECB/2017/32) (OJ L 299, 16.11.2017, p. 11). The amendment further strengthened operational risk and NIS requirements, taking into account, inter alia, the Committee on Payments and Market Infrastructures-International Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures, June 2016 (available on the BIS's website at www.bis.org).

11 See in particular Principle 17 of the Eurosystem's 'Revised Oversight Framework for retail payment systems', February 2016, available on the ECB's website.

12 Article 45 of Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L, 257, 28.4.2014, p. 172) imposes strict requirements concerning operational risks.

13 See the Eurosystem's 'Oversight Policy Framework', July 2016, available on the ECB's website.

14 See Articles of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35) on incident reporting (Article 96), security measures for operational and security risk (Article 95) and regulatory technical standards on strong customer authentification and secure communication (Article 98).

15 See footnote 13.

16 See Article 11 of the *loi du 24 mars 2017 relative à la surveillance des processeurs de transactions de paiement/wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties*.

financial institutions and the oversight of market infrastructures, complements the existing supervisory and oversight competences of the NBB over the financial sector, in particular from the perspective of the security, integrity and resilience of network and information systems. Moreover, as noted previously, the NBB is the competent authority with regard to the security of critical financial infrastructures[17] on the basis of the Law on critical infrastructures, As the draft law does not, therefore, confer any genuinely new tasks on the NBB, the issue of assessing the conferral of new tasks on a national central bank from the perspective of the prohibition of monetary financing does not arise[18].

4. Exchange of information with the ECB

4.1 Under Article 9, paragraph 1 of the draft law, information relating to operators of essential services may be shared with EU authorities 'when this exchange is necessary for the implementation of the present law'.

4.2 This wording is too restrictive, as information on incident notifications submitted by operators of essential services to the NBB may be of relevance in other contexts. Such information may, for instance, be relevant to the carrying out of oversight activities in which the ECB is involved. Such information may also be relevant in connection with the ECB's tasks concerning the prudential supervision of credit institutions in Belgium[19]. This prudential supervision covers NIS-related topics as part of the prudential supervision of operational risk (i.e., the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events)[20].

4.3 Against this backdrop the ECB recommends enhancing the wording of Article 9 of the draft law to ensure that the NBB shares this information with the ECB in a timely and efficient manner, within the framework of the ECB's responsibilities for the oversight of payment systems and the prudential supervision of credit institutions[21].

This opinion will be published on the ECB's website.

Done at Frankfurt am Main, 18 May 2018.

[signed]

The President of the ECB

Mario DRAGHI

17 With regard to the NBB's role as competent authority for the security and protection of critical infrastructures, see CON/2014/17, paragraphs 3.1 and 3.5.

18 See paragraph 2.3 of Opinion CON/2018/15.

19 See Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63).

20 See paragraph 4.3 of Opinion CON/2018/22.

21 See paragraph 6.2 of Opinion CON/2018/22.