



EUROPEAN CENTRAL BANK

EUROSYSTEM

EN

ECB-PUBLIC

OPINION OF THE EUROPEAN CENTRAL BANK

of 27 April 2018

**on the identification and supervision of critical infrastructure for the purpose of information technology security
(CON/2018/22)**

Introduction and legal basis

On 5 April 2018 the European Central Bank (ECB) received a request from the Estonian Minister for Entrepreneurship and Information Technology for an opinion on a draft law on cyber security¹ implementing Directive (EU) 2016/1148 of the Parliament and of the Council² (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 and the second, third, fifth and sixth indents of Article 2(1) of Council Decision 98/415/EC³, as the draft law relates to means of payment, Eesti Pank, 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 pursuant to Article 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.

1. Purpose of the draft law

- 1.1 The purpose of the draft law is to identify critical infrastructures and their operators and to stipulate the obligations of such operators to take appropriate organisational, physical and information security measures prior to, during and after a cyber incident to protect infrastructure-related information technology (IT) systems and to report severe IT incidents to the *Riigi Infosüsteemi Amet* (RIA, Republic of Estonia Information System Authority). In addition, the RIA is obliged to take measures to prevent and resolve cyber incidents and to maintain a register of cyber incidents.
- 1.2 The draft law empowers the RIA to supervise and enforce compliance with the obligations specified in the draft law. The draft law, in conjunction with the Law on law enforcement⁴, gives the RIA the authority to question a person and request information and/or originals (or copies) of documents; summon a person to the RIA's offices and require a person's presence during procedural acts; take steps to establish a person's identity; examine movable assets, e.g. in the current case servers or

1 Küberturvalisuse seadus, eelnõu.

2 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

3 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).

4 Korrakaitse seadus, RT I, 22.03.2011, 4, RT I, 02.12.2016, 6.

other technical equipment; enter into and examine premises⁵. In addition the RIA has the authority to put into storage a movable asset (e.g. servers or other technical equipment).⁶ Under the draft law, the RIA is also authorised, in the event of a cyber incident or upon exercise of administrative supervision, as an *ultima ratio* measure, to restrict the use of or access to the system if: (a) a cyber incident poses a risk to or damages the security of another system; (b) the system operator cannot avert the higher risk or eliminate the violation itself or cannot do it at the right time; (c) no less intrusive measures are available; and (d) the planned measure will not cause disproportionate damage⁷. Lastly, the RIA is also the body conducting extrajudicial misdemeanour proceedings in relation to a breach of the draft law⁸.

- 1.3 The draft law defines the service providers to whom it applies and includes in this respect a cross-reference to the Law on emergency⁹. In particular, the draft law specifies that the providers of vital services, as specified in the Law on emergency, are subject to the draft law. The Law on emergency, in turn, lists cash circulation¹⁰ and payment services¹¹ as vital services¹². The power to designate the providers of vital services in cash circulation and payment services is delegated to Eesti Pank¹³. Under the Law on credit institutions, Eesti Pank may only designate credit institutions or Estonian branches of credit institutions as providers of vital services¹⁴. Eesti Pank has designated AS SEB Pank, Swedbank AS and Luminor Bank AS as providers of vital services in cash circulation and payment services¹⁵. The draft law obliges providers of vital services to take measures to prevent and resolve cyber incidents and report to the RIA serious cyber incidents.
- 1.4 According to the draft law, if the requirements for running the network or information system are regulated by an international treaty or by another law, then the draft law shall be applied with the specifications arising from the international treaty or from another law.

5 See Section 15(1) of the draft law and Sections 30, 31, 32, 49, 50 and 51 of the Law on law enforcement.

6 See Section 15(2) of the draft law and Section 52 of the Law on law enforcement.

7 See Sections 16 and 17 of the draft law.

8 See Sections 18 and 19 of the draft law.

9 Hädaolukorra seadus, RT I, 03.03.2017, 1, RT I, 28.12.2017, 49.

10 According to the drafting notes of the Law on emergency, a cash circulation service includes services that permit cash to be paid into and funds withdrawn from a payment account and for which infrastructure involving buildings, e.g. bank offices, devices, e.g. automated teller machines and other similar items and integrated services, including the uninterrupted transportation of cash, are needed. The drafting notes of the Law on emergency are available on the website of the Riigikogu (Estonian Parliament) at www.riigikogu.ee. It is understood that Eesti Pank will specify the exact services that are considered cash circulation services in a decree of the Governor of Eesti Pank following the enactment of the draft law.

11 According to the drafting notes of the Law on emergency, a payment service includes services that permit payment transactions to be carried out, including the transfer of funds to a payment account opened with the payment service providers and transfer of funds that have been provided to the client as credit. A payment service also covers the fulfilment of the payment instructions via telecommunication, digital or IT devices. The drafting notes also specify that provision of payment services requires a continuous operation of telecommunication and information or similar networks and continuous operation of payment cards and other similar payment instruments. It is understood that Eesti Pank will specify the exact services that are considered payment services in a decree of the Governor of Eesti Pank following the enactment of the draft law.

12 See Section 36(3) of the Law on emergency.

13 See Section 3(3) of the Law on credit institutions, Krediidiasutuste seadus¹, RT I 1999, 23, 349, RT I, 30.12.2017, 31.

14 See Section 3(2) of the Law on credit institutions.

15 See Section 2(1) of Decree No. 4 of the Governor of Eesti Pank dated 28 February 2017.

2. General observations

- 2.1 The draft law implements Directive (EU) 2016/1148 in relation to which the ECB has issued two opinions¹⁶. According to Article 3 of Directive (EU) 2016/1148, Directive (EU) 2016/1148 is a minimum harmonisation directive, meaning that Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems than provided for under the directive. The ECB notes in this regard that, in a number of respects, the draft law goes further than provided for under Directive (EU) 2016/1148.
- 2.2 In previous opinions¹⁷, the ECB has supported the aim of Directive (EU) 2016/1148 to ensure a high common level of network and information security (NIS) across the Union and to achieve 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 cyber-security incidents.
- 2.3 The ECB has also previously called for establishing effective cooperation and information-sharing arrangements between the competent national authorities, including the RIA, and the other competent national authorities, including Eesti Pank, the *Finantsinspeksioon* (the Estonian Financial Supervision Authority) and, through Eesti Pank and the *Finantsinspeksioon*, the ECB.
- 2.4 According to the draft law, if the providers of vital services use third-party service providers for the provision of vital services, then providers of vital services must ensure that such third-party service providers comply with specific elements of the draft law¹⁸. It is the understanding of the ECB that based on this, the requirements under the draft law for running a network or information system could also become indirectly applicable to payments system operators and critical service providers and that the providers of vital services using payment systems or critical service providers for the provision of cash circulation and payment services could be required to ensure that such third-party operators comply with any supervisory orders from the RIA.

3. Impact of the draft law on payment and securities settlement systems

3.1 *Impact of the draft law on systemically important payments systems (SIPS)*

- 3.1.1 While the draft law seeks to enhance the overall resilience of critical infrastructures by identifying infrastructures that have key functions for society, providing rules for such infrastructure providers and ensuring supervision over and enforcement of the said rules, it should be ensured that the provisions of the draft law do not encroach on the Eurosystem's competences. This could be achieved by explicitly exempting payment systems overseen and/or operated by the Eurosystem (including Eesti Pank) from the scope of application of the draft law, as these are subject to comparable or more stringent requirements. Essentially, it must be ensured that implementation of the draft law's requirements does not conflict with Regulation (EU) No 795/2014 of the European

¹⁶ See Opinion CON/2014/58 and Opinion CON/2017/10. All ECB opinions are published on the ECB's website at www.ecb.europa.eu.

¹⁷ See paragraph 2.1 of Opinion CON/2014/58 and paragraph 2.1 of Opinion CON/2017/10.

¹⁸ See Section 7(3) of the draft law.

Central Bank (ECB/2014/28)¹⁹ and the Eurosystem's oversight policy framework²⁰. Regulation (EU) No 795/2014, as amended²¹, requires the operators of systemically important payment systems to establish an effective cyber resilience framework with appropriate governance measures in place to manage cyber risk.

- 3.1.2 Regulation (EU) No 795/2014 was adopted on the basis of Article 127(2) of the Treaty and Articles 3.1, 22 and 34.1 of the Statute of the European System of Central Banks and of the European Central Bank (hereinafter the 'Statute of the ESCB'). According to the fourth indent of Article 127(2) of the Treaty, the promotion of the smooth operation of payment systems is one of the core tasks of the European System of Central Banks. Furthermore, pursuant to Article 22 of the Statute of the ESCB, the ECB and the national central banks (including Eesti Pank) may provide facilities, and the ECB may make regulations, to ensure efficient and sound clearing and payment systems within the Union. Among listed SIPS, TARGET2 plays a distinct role, as it is owned and operated by the Eurosystem, and subject to strict regulation and oversight²².
- 3.1.3 As noted previously, the ECB understands that SIPS could not be designated as providers of vital services. Hence, the draft law could not directly apply to the SIPS operators. Moreover, the draft law provides that if the requirements for running the network or information system are regulated by an international treaty or by another law, then the draft law shall be applied subject to the differences arising from the international treaty or from another law. Based on this, the ECB understands that Regulation (EU) No 795/2014 is to be understood as another law or as a regulation under an international treaty, and that there is therefore no scope for the draft law to apply to SIPS, even indirectly. Based on this, the ECB also understands that the supervisory powers of the RIA under the draft law will, in any case, not directly or indirectly encompass SIPS regulated by Regulation (EU) No 795/2014. This interpretation is also consistent with the status of Union law as part of the Estonian constitutional order²³. For the sake of legal certainty, the ECB suggests that the Estonian legislator should explicitly clarify that the draft law should be without prejudice to the tasks and powers of the ECB under Regulation (EU) No 795/2014.

3.2 *Impact of the draft law on non-SIPS*

- 3.2.1 Non-SIPS include non-systemically important large-value payment systems (LVPS) and non-systemically important retail payment systems (non-SIRPS). The following focuses on non-SIRPS

¹⁹ 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), here and below 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).

²⁰ See paragraph 2.2 of Opinion CON/2017/10.

²¹ 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).

²² See paragraph 3.1 of Opinion CON/2017/10.

²³ See Section 2 of the Law amending the Constitution of the Republic of Estonia; Decision No 3-4-1-33-09 of the Estonian Supreme Court (paragraph 39); Eesti Põhiseaduse kommenteeritud väljaanne, Juura 2017, 715; *Costa v E.N.E.L.*, C-6/64, ECLI:EU:C:1964:66; *Bernhard Pfeiffer (C-397/01)*, *Wilhelm Roith (C-398/01)*, *Albert Süß (C-399/01)*, *Michael Winter (C-400/01)*, *Klaus Nestvogel (C-401/01)*, *Roswitha Zeller (C-402/01)* and *Matthias Döbele (C-403/01) v Deutsches Rotes Kreuz, Kreisverband Waldshut eV*, C-397/01 to C-403/01, ECLI:EU:C:2004:584.

as the ECB understands that LVPS are not covered by the draft law²⁴.

- 3.2.2 Under the revised oversight framework for retail payment systems²⁵ non-SIRPS have been divided into two distinct groups: prominently important retail payments systems (PIRPS) and other important retail payments systems (ORPS). The Estonian local clearing system for card payments has been classified as a PIRPS²⁶.
- 3.2.3 Under the above referenced oversight framework, non-SIRPS must follow the Principles for financial market infrastructures (PFMIs) of the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements and the Technical Committee of the International Organization of Securities Commissions (IOSCO)²⁷ and the oversight expectations for links between retail payment systems (OELRPS)²⁸. Both the CPSS-IOSCO PFMI and the OELRPS are soft law instruments, meaning that PIRPS and ORPS are subject to oversight standards, but there is, strictly speaking, no Union regulation or legislation regulating the oversight or supervision of these systems²⁹. The possibility cannot therefore be excluded that the draft law and the supervisory powers of the RIA thereunder could cover (indirectly through credit institutions designated as vital service providers) non-SIRPS, such as the Estonian local clearing system for card payments, as the CPSS-IOSCO PFMI and OELRPS would not be considered a law or international treaty within the meaning of the draft law.
- 3.2.4 The revised oversight framework for retail payment systems specifies that all retail payment systems are an integral part of the payment and settlement landscape of the euro area and thus fall within the scope of oversight. Hence, the Eurosystem has an interest in ensuring that the oversight framework and standards applicable to such systems would not be prejudiced through the implementation of Directive (EU) 2016/1148 or when introducing other NIS-related laws or regulations. If the Estonian authorities wish to exclude non-SIRPS from the scope of application of the draft law, then this could be done expressly. If the Estonian authorities consider it necessary to include the non-SIRPS within the (indirect) scope of application of the draft law, then the ECB suggests that effective information-sharing and cooperation arrangements should be put in place (as specified below in Section 6) to ensure that the RIA shares information about actual and potential cyber incidents affecting non-SIRPS with Eesti Pank in a timely and efficient manner in order to enable the Eesti Pank to fulfil the tasks assigned to them under the Treaty and applicable Estonian law. It would, in any case, be advisable to clarify the exact scope of application of the draft law in relation to non-SIRPS to avoid potential confusion on the applicable standards and powers of the relevant authorities.

24 It is noted that non-systemically important LVPSs have to respect the PFMI in their entirety (see the Eurosystem's 'Assessment methodology for payment systems', available on the ECB's website).

25 See the Eurosystem's 'Revised oversight framework for retail payment systems' (February 2016), available on the ECB's website.

26 See the Eurosystem's 'Overview of payment systems', available on the ECB's website.

27 See the Bank for International Settlements' CPSS and the IOSCO Technical Committee Principles for financial market infrastructures, available on the Bank for International Settlements' website at www.bis.org.

28 See the Eurosystem's 'Oversight expectations for links between retail payment systems', available on the ECB's website.

29 See paragraph 2.4.4 of ECB Opinion CON/2017/31.

3.3 *Critical service providers*

3.3.1 The revised Eurosystem oversight policy framework³⁰ covers critical service providers (CSPs). Similar to the case of non-SIPS, the possibility cannot be excluded that the draft law and the supervisory powers of the RIA thereunder could cover (indirectly through credit institutions designated as vital service providers) critical service providers for which the above applicable oversight frameworks would not be considered a law or international treaty within the meaning of the draft law. In light thereof, it is suggested that the Estonian authorities take existing oversight arrangements into consideration in the application of the draft law to providers of vital services.

3.4 *Impact of the draft law on payment services and payment instruments and schemes*

3.4.1 Directive (EU) 2015/2366 of the European Parliament and of the Council³¹, as implemented into national law, regulates payment services. Even though Directive (EU) 2015/2366 includes provisions on the management of operational risk, which have also been transposed into Estonian law, this directive and applicable national law do not directly prevent any other laws from being, at least partially, applicable. Hence, the ECB understands that the draft law is still partially applicable to such services, and that this also extends the supervisory powers of the RIA.

3.4.2 The revised Eurosystem oversight policy framework³² identifies payment instruments, such as payment cards, credit transfers, direct debits and e-money, as an 'integral part of payment systems', and thus includes these within the scope of its central bank oversight. For payment instruments, the role of primary overseer for the Eurosystem is assigned by reference to the national anchor of the payment scheme and the legal incorporation of its governance authority. For credit transfer and direct debit schemes within the Single Euro Payments Area, as well as some of the international card payment schemes, the ECB has the primary oversight role³³.

3.4.3 If the Estonian authorities wish to exclude payment schemes and instruments from the direct and indirect scope of application of the draft law, this could be done expressly. If the Estonian authorities consider it necessary to include various payment schemes and instruments within the direct and/or indirect scope of application of the draft law, then the ECB suggests that an effective information sharing and cooperation framework should be put in place (as specified below in Section 6) to ensure that the RIA shares information about actual and potential cyber incidents affecting card schemes and other payment instruments with the Eesti Pank in a timely and efficient manner in order to enable Eesti Pank to fulfil the tasks assigned to them under the Treaty and applicable Estonian law. It would, in any case, be advisable to clarify the exact scope of application of the draft law and the supervisory powers of the RIA in relation to payment instruments to avoid potential confusion on the applicable standards and powers of the relevant authorities.

³⁰ See the Eurosystem's 'Eurosystem oversight policy framework' (revised version), p. 9, available on the ECB's website.

³¹ 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).

³² See 'Eurosystem oversight policy framework' (revised version), p. 2.

³³ See paragraph 5.2 of Opinion CON/2017/10.

3.5 *Impact of the draft law on securities settlement systems*

The ECB understands that the draft law does not apply to securities settlement systems or to TARGET2-securities.

4. **Impact of the draft law on the prudential supervision of credit institutions**

- 4.1 Council Regulation (EU) No 1024/2013³⁴ confers tasks on the ECB concerning the prudential supervision of credit institutions with a view to contributing to their safety and soundness and in order to protect the stability of the financial system of the Union and each Member State. The ECB is responsible for the effective and consistent functioning of the single supervisory mechanism (SSM) and exercises oversight over the system's functioning, based on the distribution of responsibilities between the ECB and national competent authorities (NCAs), including the *Finantsinspeksioon* in Estonia. In particular, the ECB carries out its task to authorise and withdraw the authorisations of all credit institutions. For significant credit institutions the ECB also has the task, among others, to ensure compliance with the relevant Union law acts which impose prudential requirements on credit institutions, including the requirement to have in place robust governance arrangements, including sound risk management processes and internal control mechanisms³⁵. To this end, the ECB shall be given all supervisory powers to intervene in the activity of credit institutions that are necessary for the exercise of its functions³⁶.
- 4.2 All Estonian credit institutions that would fall within the scope of the draft law upon its enactment are significant credit institutions subject to ECB prudential supervision³⁷. Nonetheless, the application of the draft law to non-significant credit institutions thereafter cannot be excluded.
- 4.3 The prudential supervision of credit institutions also covers NIS-related topics as part of the prudential supervision of operational risk, meaning the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events³⁸. Since the assessment of the adequacy of the internal governance arrangements of credit institutions is one of the core competences of prudential supervisors, the requirements under the draft law should not interfere with the tasks of prudential supervisors³⁹. In this respect, the ECB has the power, *inter alia*, to

³⁴ 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).

³⁵ See Articles 4(1)(e) and 6(4) of Regulation (EU) No 1024/2013.

³⁶ See Article 64(1) 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 and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

³⁷ See paragraph 1.3. A list of SSM supervised entities is available on the SSM's website at <https://www.bankingsupervision.europa.eu>.

³⁸ See Article 4(1)(52) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1); Article 3(1)(48) 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 and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p 338).

³⁹ See paragraph 3.5 of Opinion CON/2014/58 and paragraph 2.12 of Opinion CON/2014/9.

restrict or limit the business, operations or network of institutions or to request the divestment of activities that pose excessive risks to the soundness of an institution⁴⁰.

- 4.4 It is acknowledged that the tasks of the ECB and the *Finantsinspeksioon* as prudential supervisors are in a number of critical respects distinct from the tasks and authorities of computer security incident response teams (CSIRTs). Nevertheless, there is an overlap where the actions of a CSIRT, such as the RIA in Estonia, can affect the prudential supervision of credit institutions under relevant Union and Estonian laws.
- 4.5 This would be most evident should the RIA choose, when potentially using its *ultima ratio* authorities under the draft law, to restrict the use of a system. If the RIA uses its authority to restrict the use of an information system used by a significant credit institution for the provision of payment services, then this could significantly impact the continuous operation and financial standing of the credit institution. Additionally, informing the affected persons or the general public about cyber incidents, as anticipated in the draft law⁴¹, may have an impact on public confidence in the affected credit institution. The ECB and the NCAs within the SSM are responsible for the assessment of recovery plans and taking early intervention measures under Directive 2014/59/EU of the European Parliament and of the Council⁴² (as implemented into national law). Further, the primary responsibility for determining that a significant credit institution is failing or likely to fail as a condition to the resolution of a credit institution lies with the ECB⁴³. In the case of resolution, one of the resolution objectives is to ensure the continuity of critical functions⁴⁴, which can include the continuing functioning of the credit institution's payment and cash circulation systems.
- 4.6 To enable the ECB and the *Finantsinspeksioon* to fulfil the tasks assigned to them within the SSM, the ECB suggests explicitly clarifying the scope of the draft law and any powers granted to the RIA in this respect. The ECB also suggests clarifying that the scope of the draft law and any powers granted to the RIA thereunder are without prejudice to the tasks and powers of the ECB and the *Finantsinspeksioon* under Council Regulation (EU) No 1024/2013 and applicable Estonian law. The ECB also recommends that an effective framework should be put in place (as specified in Section 6 below) to ensure that the RIA shares information about actual and potential cyber incidents affecting significant supervised entities, as well as measures planned or adopted by the RIA. Where relevant, the RIA should share information with the *Finantsinspeksioon* and, through the *Finantsinspeksioon*, with the ECB in a timely and efficient manner. The Estonian legislator may also wish to consider the interaction of the RIA's powers under the draft law with the resolution-related procedures and powers of the relevant authorities.

40 See Article 16(2)(e) of Regulation (EU) No 1024/2013.

41 See Section 8(5) and (6) of the draft law.

42 See Articles 27 to 30 of Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (OJ L 173, 12.6.2014, p. 190).

43 See Article 32(1)(a) of Directive 2014/59/EU.

44 See Article 31(2)(a) of Directive 2014/59/EU.

5. Impact of the draft law on cash circulation

- 5.1 Under Article 128(1) of the Treaty, the ECB has the exclusive right to authorise the issue of euro banknotes within the Union. The ECB, together with the national central banks, may issue such notes. The euro banknotes issued are the only such notes to have the status of legal tender within the Union. Under Council Regulation (EC) No 1338/2001⁴⁵ credit institutions and other cash handlers are obliged to ensure that euro notes which they have received and which they intend to put back into circulation are checked for authenticity and that counterfeits are detected in line with procedures defined by the ECB. Eurosystem national central banks, including Eesti Pank, play an important role in these procedures⁴⁶. From a practical perspective, the interest of the ECB and the Eurosystem encompasses the adequate NIS protection of the systems ensuring the circulation of euro banknotes, such as automated teller machine (ATM) networks and cash circulation support networks, in view of the further increasing automation of the cash supply infrastructure. This trend not only concerns the banking sector and the cash-handling industry, but is also becoming a more pronounced trend in the retail sector.
- 5.2 Therefore, the ECB suggests that an effective information-sharing and cooperation framework should be put in place (as specified below in Section 6) to ensure that the RIA shares information about actual and potential cyber incidents affecting ATM and cash circulation support networks with Eesti Pank. Additionally, the RIA should, through Eesti Pank, share information with the ECB in a timely and efficient manner in order to enable the ECB and Eesti Pank to fulfil the tasks assigned to them under the Treaty and applicable Estonian law.

6. Conclusion

- 6.1 To sum up, the ECB suggests that the Estonian legislator explicitly clarifies that the draft law, including the tasks and powers of the RIA, should be without prejudice to the tasks and powers of the ECB under Regulation (EU) No 795/2014 and to the tasks and powers of the ECB and the *Finantsinspektsioon* under Council Regulation (EU) No 1024/2013 and applicable Estonian law.
- 6.2 Arrangements should be put in place to ensure that the RIA shares information about actual and potential cyber incidents, as well as measures planned or adopted by the RIA where relevant, which affect significant credit institutions, non-SIPS, CSPs, payment services and instruments/schemes, ATM and cash circulation support networks with Eesti Pank, and the *Finantsinspektsioon*. Additionally, the ECB suggests ensuring that the RIA shares this information, through Eesti Pank and the *Finantsinspektsioon*, with the ECB in a timely and efficient manner, within the framework of their respective responsibilities for the oversight of payment systems, the prudential supervision of credit institutions and the authorisation of the issuance of euro banknotes.

⁴⁵ Article 6(1) of Council Regulation (EC) No 1338/2001 of 28 June 2001 laying down measures necessary for the protection of the euro against counterfeiting (OJ L 181, 4.7.2001, p. 6).

⁴⁶ See Decision ECB/2010/14 of the European Central Bank of 16 September 2010 on the authenticity and fitness checking and recirculation of euro banknotes, (OJ L 267, 9.10.2010, p. 1).

6.3 For its part, the ECB stands ready, within the framework of its responsibilities for the oversight of payment systems, the prudential supervision of credit institutions and the issuance and circulation of euro banknotes, to cooperate in ensuring that best practices with regard to NIS are established and followed.

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

Done at Frankfurt am Main, 27 April 2018.

[signed]

The President of the ECB

Mario DRAGHI