EUROPEAN CENTRAL BANK

EUROSYSTEM

EN **ECB-PUBLIC**

OPINION OF THE EUROPEAN CENTRAL BANK

of 2 May 2019

on the security of network and information systems

(CON/2019/17)

Introduction and legal basis

On 4 March 2019 the European Central Bank (ECB) received a request from the *Αρχή Ψηφιακής Ασφάλειας* (DSA, Digital Security Authority) of the Republic of Cyprus for an opinion on certain draft legislative provisions (hereinafter the 'draft legislative provisions') which will form part of a draft law on the establishment, tasks and operation of the DSA (hereinafter the 'draft law'), which will replace Law 17 (I) of 2018 on the security of network and information systems[1] (hereinafter the 'existing 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 third, fifth and sixth indents of Article 2(1) of Council Decision 98/415/EC[2], as the draft legislative provisions relate to the Central Bank of Cyprus (CBC), payment and settlement systems, rules applicable to financial institutions insofar as they materially influence the stability of financial institutions and markets, and the tasks conferred upon the ECB 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 and the draft legal provisions

1.1 The purpose of the draft law is to more closely align the Cypriot legal framework with Directive (EU) 2016/1148 of the European Parliament and of the Council[3]. The draft law will replace the existing law which implemented Directive (EU) 2016/1148 in 2018.

1.2 The draft law establishes the DSA, creates the national computer security incident response team and ensures the security, integrity and resilience of electronic communications networks and services[4]. As part of its powers and tasks , the DSA may (a) ensure that operators of essential services and operators of critical information infrastructures take appropriate and proportionate technical and organisational measures to manage the security risks of the network and information

1 Ο περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμος του 2018 (Ν. 17(Ι)/2018).

2 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).

3 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).

4 The draft law also transposes Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24.4.2002, p. 33).

systems used in their activities and the appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used in the provision of such services, (b) impose administrative fines and other sanctions, (c) request for the purposes of its activities any relevant technical, financial and legal information from operators of essential services and operators of critical information infrastructures, (d) summon and compel the presence of witnesses in investigations, and (e) carry out on-site inspections[5].

1.3 The draft law provides that where a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are at least equivalent in effect to the obligations laid down in the draft law, those provisions of that sector-specific Union legal act as applied in the national legal order shall apply, in accordance with Article 1(7) of Directive (EU) 2016/1148.

1.4 The draft law does not identify the operators of essential services or the operators of critical information infrastructures, but empowers the DSA to do so by way of issuing a decree. In the explanatory memorandum which accompanies the request for an opinion, it is noted that in the context of determining the relevant critical information infrastructures, the financial sector indicated in Directive (EU) 2016/1148 will be considered[6]. In this regard, it is further noted that where there is no *lex specialis*, the draft law may capture sectors which fall under the responsibility of the CBC, such as systems and infrastructures of the CBC, systems which the CBC oversees but does not administer, and financial institutions supervised by the CBC.

1.5 The draft legislative provisions add to the powers and tasks of the DSA under the draft law concerning (a) the monitoring of compliance with the draft law, in the interest of which the DSA is empowered to request the assistance of persons subject to supervision under other legislation and of the relevant supervisory authorities and national authorities involved in supervision when such supervision is exercised by supranational authorities[7], and (b) the power to enter into memoranda of understanding with operators that are governed by the draft law or other authorities, organisations, companies or supervisory authorities that cooperate with the DSA. In addition, in cases where the CBC has been designated as an operator of critical infrastructures or otherwise pursuant to the draft law, such designation may be governed by a memorandum of understanding between the DSA and the CBC. Without prejudice to Union law, any information provided by the CBC to the DSA in the context of such cooperation does not constitute a breach of the CBC's professional secrecy obligation.

2. General observations

2.1 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

5 See Articles 17, 19 and 20 of the draft law.

6 See Article 4(4) of Directive (EU) 2016/1148.

7 See Article 17(hh) of the draft law.

the Directive. The draft law goes beyond Directive (EU) 2016/1148 by covering critical infrastructures and foreseeing the designation of operators of critical infrastructures. This opinion does not address whether the draft law, if adopted as proposed, would represent an effective means of implementing Directive (EU) 2016/1148 into Cypriot law.

2.2 As previously noted by the ECB[8], the ECB supports the aim of Directive (EU) 2016/1148 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. Concurrently, it should be ensured that the provisions of the national legislation transposing Directive (EU) 2016/1148 are coordinated with the Eurosystem's competences[9] (see paragraphs 3 to 4) and respect the principle of central bank independence enshrined in Article 130 of the Treaty. Indeed, and in line with the ECB's recommendation, recital 14 of Directive (EU) 2016/1148 states that the Directive does not affect the Eurosystem's oversight of payment and settlement systems[10]. On the other hand, NIS benefits from synergies and economies of scale. In particular, dedicated national DSAs have the potential to become repositories of considerable resources and expertise which the Eurosystem may draw upon in the area of NIS. Moreover, recognition of the ECB and its decision-making bodies' independence does not have the consequence of separating the Eurosystem entirely from the Union and exempting it from every rule of Union law[11]. The national implementing measures of Directive (EU) 2016/1148 are not *prima facie* precluded from applying to the Eurosystem.

2.3 Against this background, the ECB welcomes the establishment of cooperation arrangements between the DSA and the CBC. The ECB suggests that, in the context of such cooperation, effective information-sharing mechanisms are put in place in order to enable the CBC to fulfil its tasks under the Treaty and under national law. Such information-sharing arrangements will also ensure that the DSA and the CBC exchange information on actual and potential cyber incidents or threats in the financial sector's systems and infrastructures and on planned and adopted measures in an effective and timely manner[12].

2.4 In addition, the ECB stands ready to cooperate with the DSA in relation to the systems and infrastructures which the Eurosystem oversees or operates, such as payment systems, instruments and schemes, and the prudential supervision of credit institutions, with a view to ensuring that best practices with regard to NIS are established and followed[13]. The ECB has previously called for establishing such effective cooperation and information-sharing arrangements between the national

---

8 See paragraph 2.1 of Opinion CON/2014/58, paragraph 2.1 of Opinion CON/2017/10, paragraph 2.2 of Opinion CON/2018/22 and paragraph 2.2 of Opinion CON/2018/27. All ECB opinions are published on the ECB's website at www.ecb.europa.eu.

9 See also paragraph 2.2 of Opinion CON/2017/10; paragraph 3.1.1 of Opinion CON/2018/22; and paragraph 2.2 of Opinion CON/2014/58.

10 See paragraph 3.1 of Opinion CON/2014/58 and paragraph 3.5 of Opinion CON/2017/10.

11 See judgment of the Court of Justice of 10 July 2003, *Commission* v *ECB*, C-11/00, ECLI:EU:C:2003:395, paragraphs 134 to 136.

12 See paragraphs 3.2.4 and 3.4.3 of Opinion CON/2018/22 and paragraph 4.4 of Opinion CON/2018/47.

13 See paragraph 6.3 of Opinion CON/2018/22.

competent authorities, including the DSA, and the other national competent authorities, including national central banks (NCBs), and, through the NCBs, the ECB[14]. Additionally the ECB suggests ensuring that the DSA shares relevant information, through the CBC, with the ECB in a timely and efficient manner within the framework of their respective responsibilities[15].

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 The ECB has in its oversight role, on the basis of Articles 3.1 and 22 and the first indent of Article 34.1 of the Statute of the ESCB, adopted Regulation (EU) No 795/2014 (ECB/2014/28)[16]. Regulation (EU) No 795/2014 (ECB/2014/28) implements the Principles for financial market infrastructures (PFMIs) issued by the Committee on Payment and Settlement Systems (CPSS) and the International Organization of Securities Commissions (IOSCO)[17] which are legally binding and cover both large-value and retail payment systems of systemic importance, operated either by a Eurosystem central bank or a private entity.

3.1.2 Thus, SIPS are subject to regular assessment against the requirements of Regulation (EU) No 795/2014 (ECB/2014/28) related to operational risk[18], which allows the competent Eurosystem central bank, as competent authority, to verify that the systems are in compliance. In cases of non-compliance, the competent Eurosystem central bank has the power to impose sanctions or corrective measures to ensure compliance[19]. The amended Regulation (EU) No 795/2014 (ECB/2014/28) recently introduced a number of new requirements for SIPS operators addressing new risks, including those related to operational and security risks, such as cyber resilience[20], taking into account, inter alia, the Guidance on cyber resilience for financial market infrastructures which was published in 2016 by the Committee on Payments and Market Infrastructures (CPMI) and IOSCO[21].

3.1.3 Furthermore, in line with the requirements set out in Directive (EU) 2016/1148, Regulation (EU) No 795/2014 (ECB/2014/28) already provides competent Eurosystem central banks with the power to obtain information concerning, inter alia, major and minor incidents, the nature and type of the

14 See paragraphs 2.3 and 6.2 of Opinion CON/2018/22.

15 See paragraph 4.3 of Opinion CON/2018/27 and paragraph 6.2 of Opinion CON/2018/47.

16 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).

17 Available on the Bank for International Settlements' website at www.bis.org.

18 See Article 15 of Regulation (EU) No 795/2014 (ECB/2014/28), which imposes an obligation on SIPS operators to take steps such as: (a) establish comprehensive physical and information security policies that adequately identify, assess and manage all potential vulnerabilities and threats, (b) to ensure that critical information technology systems can resume operations within specified timeframes where an event poses a significant risk of disrupting the SIPS' operations etc.

19 See paragraph 3.4 of Opinion CON/2017/10.

20 See Articles 15(1a) and (4a), which imposes an obligation on SIPS operators to take the following steps: (i) review, audit and test systems, operational policies, procedures and controls periodically and after significant changes; (ii) establish an effective cyber resilience framework with appropriate governance measures in place; (iii) identify their critical operations and supporting assets, and have appropriate measures in place to protect them from, detect, respond to and recover from cyber-attacks; (iv) regularly test the established measures; and (v) have a sound level of situational awareness of cyber threats, including through a process of continuous learning.

21 Available on the Bank for International Settlements' website.

incidents, their seriousness and their duration[22]. The amended Regulation (EU) No 795/2014 (ECB/2014/28) further enhanced competent Eurosystem central banks' powers to conduct on-site inspections and request independent reviews of and investigations into the functioning of the systems.[23]

3.1.4 The ECB understands that the DSA may, by virtue of a decree, capture within the scope of the draft law services which are provided using information systems operated by the Eurosystem or operated by the CBC and overseen by the Eurosystem.

3.1.5 Among listed SIPS, TARGET2 plays a distinct role, as it is owned and operated by the Eurosystem and subject to strict regulation and oversight.[24] The ECB understands that the Cypriot component of TARGET2, TARGET2-CY for which the CBC acts as the operator, could potentially fall within the scope of the draft law. TARGET2 has been identified, pursuant to Decision ECB/2014/35 of the European Central Bank[25], as a SIPS and is overseen by the ECB as a competent authority under Regulation (EU) No 795/2014 (ECB/2014/28).

3.1.6 While SIPS may fall within the scope of the draft law, the ECB understands that the draft law should be without prejudice to the oversight of SIPS given that such oversight is performed on the basis of ECB regulations. As noted in paragraph 2.3, the ECB suggests that effective information-sharing and cooperation arrangements are put in place to ensure that the DSA shares information with the CBC about actual and potential cyber incidents, as well as planned or adopted measures which may affect SIPS and TARGET2 in a timely and efficient manner in order to enable the CBC to fulfil its tasks under the Treaty and national law. The ECB also suggests that respective cooperation and information-sharing arrangements are established between the DSA and the ECB, through the CBC.

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). Under the revised oversight framework for retail payment systems[26], non-SIRPS have been divided into two distinct groups: prominently important retail payments systems (PIRPS) and other retail payments systems (ORPS). The Cypriot local retail payment systems, JCC Payment Card System, Cyprus Clearing House for cheques and JCC SDD, have been classified as PIRPS or ORPS[27] and the ECB understands that their services could be included in the list of essential services pursuant to the draft law and that the operators of those systems or some of those systems might be designated as operators of essential services.

---

22 See Article 21(1a) of Regulation (EU) No 795/795/2014 (ECB/2014/28).

23 See Articles 21(1b) and (1c) of Regulation (EU) No 795/2014 (ECB/2014/28).

24 See paragraph 3.1 of Opinion CON/2018/47.

25 Decision ECB/2014/35 of the European Central Bank of 13 August 2014 on the identification of TARGET2 as a systemically important payment system pursuant to Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (OJ L 245, 20.8.2014, p. 5).

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

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

3.2.2 Under the Eurosystem's oversight policy framework, non-systemically important LVPS and non-SIRPS must follow the CPSS-IOSCO PFMIs and non-SIRPS must additionally follow the Oversight expectations for links between retail payment systems (OELRPS)[28]. Both the CPSS-IOSCO PFMIs and the OELRPS are soft law instruments, meaning that non-systemically important LVPS, PIRPS and ORPS are subject to oversight standards (which are comparable to the standards under Regulation (EU) No 795/2014 (ECB/2014/28)); however there is, strictly speaking, no Union legislation regulating the oversight or supervision of these systems[29]. The CBC is given supervisory and oversight competence over non-SIPS pursuant primarily to section 48 of the Law on the CBC[30], which in this particular respect does not implement Union 'laws' as described above[31].

3.2.3 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 are not prejudiced through the implementation of Directive (EU) 2016/1148 or when introducing other NIS-related laws[32].

3.2.4 If the intention is for non-SIPS to be captured under the scope of the draft law, the ECB suggests that, the same clarifications and effective information-sharing and cooperation framework as mentioned in paragraph 3.1.6 are established in relation to and between the CBC and the DSA, and if necessary, with the ECB through the CBC.

3.3 *Impact of the draft law on critical service providers*

3.3.1 The revised Eurosystem oversight policy framework[33] covers critical service providers such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT is a limited liability cooperative company established in Belgium, which supplies secure messaging services in a large number of countries. Nationale Bank van België/Banque Nationale de Belgique acts as the lead overseer of SWIFT, and conducts, on the basis of a cooperative oversight arrangement, oversight in respect of SWIFT in cooperation with the other G10 central banks, including the ECB. The G10 overseers recognise that the main focus of oversight is SWIFT's operational risk, as this is considered to be the primary risk category through which SWIFT could pose a systemic risk to the financial system in the Union. In this regard, the SWIFT Cooperative Oversight Group has developed a specific set of principles and high level expectations that apply to SWIFT, such as risk identification and management, information security, reliability and resilience, technology planning and communication with users. The G10 overseers subject SWIFT to an intense form of oversight, and expect that SWIFT specifically adheres to the CPMI-IOSCO Guidance on cyber resilience and other international standards on IT Security, which exceed the requirements set out in Directive (EU) 2016/1148.

---

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 and paragraph 3.2.3 of Opinion CON/2018/22.

30 Ο περί της Κεντρικής Τράπεζας της Κύπρου Νόμος του 2002 (N. 138(I)/2002).

31 See also paragraph 2.4.4 of Opinion CON/2017/31 and paragraph 4.2 of Opinion CON/2018/47.

32 See paragraph 3.4.2 of Opinion CON/2018/22 and paragraph 4.3 of Opinion CON/2018/47.

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

3.3.2 Similar to the case of non-SIPS, the possibility cannot be excluded that the draft law and the supervisory powers of the DSA could cover critical service providers for which there are applicable oversight measures. It is therefore suggested that the Cypriot authorities take existing oversight arrangements into consideration in their application of the draft law, if the application affects critical service providers[34]. In the particular case of SWIFT, it is proposed that the draft law excludes SWIFT from its scope considering that SWIFT is established in and operated from Belgium with infrastructure hubs that are not located within Cyprus, and that SWIFT simply supplies secure messaging services in Cyprus, as well as in a vast number of other countries.

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

3.4.1 The Eurosystem oversight policy framework identifies payment instruments, such as cards, credit transfers, direct debit and electronic 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 role. Payment service providers (PSPs), including credit institutions, payment institutions and electronic money institutions, are subject to Directive (EU) 2015/2366 of the European Parliament and of the Council[35], which is applicable as of January 2018, as implemented into national law. The legal and regulatory framework set out requirements pertaining to operational and security risks and incident reporting. Nevertheless, prudential supervisors need to exercise careful judgment when deciding whether to publish information concerning individual cybersecurity incidents, to ensure public confidence in the affected institutions is not undermined. Furthermore, the European Banking Authority (EBA) has produced draft guidelines on information and communication technology (ICT) and security risk management[36] which are intended to harmonise standards required from payment service providers as regards ICT security, incident reporting, project management and business continuity. While PSPs are therefore subject to Union and Cypriot legislation, and regulations based on Union legislation, the oversight of international and domestic card schemes is not subject to Union legislation as such[37].

3.4.2 The ECB understands that the various payment schemes and instruments and PSPs may potentially fall within the scope of the draft law. It is thus suggested that the same clarifications and effective information-sharing and cooperation framework as mentioned in paragraph 3.1.6 are established in relation to and between the authorities responsible for the oversight of payment schemes, instruments and services and for the supervision of PSPs and the DSA[38]. The draft law

34 See paragraph 3.3.1 of Opinion CON/2018/22 and paragraph 5 of Opinion CON/2018/47.

35 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).

36 See EBA Guidelines on internal governance under Directive 2013/36/EU of 26 September 2017 (EBA/GL/2017/11) and EBA draft Guidelines on ICT and security risk management of 13 December 2018 (EBA/CP/2018/15) available on the EBA's website at www.eba.europa.eu.

37 See paragraph 2.4.3 of Opinion CON/2017/31 and paragraph 3.4.2 of Opinion CON/2018/22.

38 See also paragraph 3.4.3 of Opinion CON/2018/22 and paragraph 6.2 of Opinion CON/2018/47.

could also clarify that as regards the supervision of PSPs, the DSA's responsibilities are without prejudice to and are aligned with the tasks of the CBC.

3.5 *Impact of the draft law on central securities depositories (CSDs)*

3.5.1 CSDs are strictly regulated and supervised by different authorities pursuant to Regulation (EU) No 909/2014 of the European Parliament and of the Council[39], which sets out requirements pertaining to operational risk. Furthermore, CSDs should take note of the CPMI-IOSCO Cyber Guidance, which is applicable to all financial market infrastructures.

3.5.2 In addition to the supervisory competences entrusted to national competent authorities (NCAs) under Regulation (EU) No 909/2014, it should be noted that national authorities, in particular the members of the ESCB, may be entrusted with oversight competences in relation to CSDs. In this regard, recital 8 of Regulation (EU) No 909/2014 states that the Regulation should be without prejudice to the responsibilities of the ECB and the NCBs to ensure efficient and sound clearing and payment systems within the Union and other countries and that the Regulation should not prevent the members of the ESCB from accessing information relevant for the performance of their duties, including the oversight of CSDs and other financial market infrastructures[40].

3.5.3 The Cyprus Central Securities Depository and Central Registry (CDCR) is operated by the Cyprus Stock Exchange (CSE)[41], is supervised by the Cyprus Securities and Exchange Commission (CySEC), and overseen by the CBC. While the CDCR may fall within the scope of the draft law, the ECB understands that the draft law should be without prejudice to the supervision and oversight of the CDCR given that such supervision and oversight is performed on the basis of Union legislation. The draft law could also clarify that the DSA's responsibilities are without prejudice to and are aligned with the tasks of the CBC and of the CySEC.

3.6 *Eurosystem cyber resilience strategy for Financial Market Infrastructures (FMIs)*

3.6.1 The Cypriot authorities may also wish to take note of the Eurosystem cyber resilience strategy for FMIs, which is intended to support the implementation of the CPMI-IOSCO guidance from an oversight perspective. The objective of this strategy is to (i) improve the cyber resilience of the euro area financial sector as a whole by enhancing the 'cyber readiness' of individual FMIs that are overseen by the Eurosystem central banks; and (ii) foster collaboration among FMIs, their critical service providers and the relevant authorities. As part of the strategy, the Eurosystem has developed a range of tools that can be used by FMIs to enhance their cyber resilience, such as a European red team testing framework[42] and other tools, such as cyber surveys and focused assessments to assess the level of cyber maturity of Eurosystem payment systems and to develop

39 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, 28.8.2014, p. 1).

40 See paragraph 7.2 of Opinion CON/2018/47 and paragraph 7.3 of Opinion CON/2017/10.

41 The Cyprus CSD is established in accordance with the provisions of the Law 27(I)/1996 on securities and the Cyprus Stock Exchange (Central Securities Depository and Central Registry) (Ο περί Αξιών και Χρηματιστηρίου Αξιών Κύπρου (Κεντρικό Αποθετήριο και Κεντρικό Μητρώο Αξιών) Νόμος του 1996 (Ν. 27(Ι)/1996)).

42 See the Eurosystem's Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU) (May 2018), available on the ECB's website.

cyber resilience oversight expectations[43] which will provide more detailed guidance to payment system operators.

4. Impact of the draft law on credit institutions

4.1 Recital 13 of Directive (EU) 2016/1148 states that requirements in respect of information systems, which often exceed the requirements provided for under Directive (EU) 2016/1148, are set out in a number of Union legal acts, including the rules on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms. Member States should consider those requirements in their application of provisions transposing Directive (EU) 2016/1148 as *lex specialis*. Indeed, the Union legal acts harmonising the area of supervision of credit institutions include Regulation (EU) No 575/2013 of the European Parliament and of the Council[44] and Directive 2013/36/EU of the European Parliament and of the Council[45], jointly establishing the CRR/CRDIV framework. Credit institutions established in Cyprus must also adhere to the Directive on governance and management arrangements[46], enacted by the CBC, which sets, inter alia, a framework of principles for a sound and effective operation of information technology systems in the context of managing operational risk.

4.2 The ECB and the CBC are the competent authorities exercising specified supervisory powers under the CRR/CRDIV framework, by virtue of Council Regulation (EU) No 1024/2013[47] which confers specific tasks on the ECB concerning the prudential supervision of credit institutions within the euro area and makes the ECB responsible for the effective and consistent functioning of the Single Supervisory Mechanism (SSM) within which specific supervisory responsibilities are distributed between the ECB and the participating NCAs, including the CBC. In particular, the ECB carries out the task to authorise and to 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 that imposes prudential requirements on credit institutions, including the requirement to have in place robust governance arrangements, such as sound risk management processes and internal control mechanisms[48]. To this end, the ECB is given all supervisory powers to intervene in the activity of credit institutions that are necessary for the exercise of its functions.

4.3 The prudential supervision of credit institutions, as exercised by the ECB and the CBC within the SSM, covers several aspects related to cybersecurity as part of the prudential supervision of operational risk, which means the risk of loss resulting from inadequate or failed internal processes,

---

43 See the Cyber resilience oversight expectations for financial market infrastructures (CROE) (December 2018), available on the ECB's website.

44 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).

45 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).

46 Η περί Ρυθμίσεων Διακυβέρνησης και Διαχείρισης Οδηγία του 2014.

47 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).

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

people and systems or from external events[49]. In addition, the EBA has produced guidelines on internal governance, covering aspects of IT risks, and, as noted in paragraph 3.4.1, draft guidelines on ICT and security risk management[50] which are intended to harmonise requirements for credit institutions, investment firms and payment service providers as regards ICT security, incident reporting, project management and business continuity. Further EBA Guidelines are under development, concerning inclusion of cyber risk aspects in the Supervisory Review and Evaluation Process[51]. The ECB has developed comprehensive IT risk questionnaires for supervised credit institutions that are fed into their SREP outcomes and also uses insights on cyber-security issues that may be drawn from thematic reviews, on-site inspections and reports of cyber incidents[52]. Such insights may form the basis for ad hoc institution-specific recommendations and general sector-wide comparisons and policies. At the same time, prudential supervisors need to exercise careful judgment when deciding to publish information concerning individual cybersecurity incidents so as to not undermine public confidence in the affected credit institutions.

4.4 Moreover, 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 Council[53] (as transposed 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 ECB[54]. In the case of resolution, one of the resolution objectives is to ensure the continuity of critical functions[55], which can include the continuing functioning of the credit institution's payment and cash circulation systems.

4.5 Central banks are excluded from the scope of Directive 2013/36/EU and are thus not supervised institutions falling within the scope of Regulation (EU) No 575/2013. Therefore, neither the ECB nor the CBC falls within the scope of the 'banking sector' for the purposes of point (3) of Annex II to Directive (EU) 2016/1148[56].

4.6 It is understood that, during the exercise of its monitoring task, the DSA might request the assistance of both significant and less significant credit institutions established or operating in Cyprus, and of the CBC and the ECB as competent authorities exercising specific supervisory powers in relation to such credit institutions within the SSM[57]. It is also understood that credit institutions established in Cyprus can be designated as operators of essential services, and thus

49 See Article 4(1)(52) of Regulation (EU) No 575/2013.

50 See the EBA Guidelines on internal governance under Directive 2013/36/EU of 26 September 2017 (EBA/GL/2017/11) and the EBA draft Guidelines on ICT and security risk management of 13 December 2018 (EBA/CP/2018/15), available on the EBA's website.

51 See the EBA draft Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) of 6 October 2016 (EBA/CP/2016/14), available on the EBA's website.

52 See also the Newsletter article of 13 February 2019 on 'IT and cyber risk - the SSM perspective', available on the ECB's website.

53 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).

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

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

56 See paragraph 2.4 of Opinion CON/2017/10.

57 See Article 17(hh) of the draft legislative provisions.

would need to comply with their obligations under the draft law. Finally, it is understood that informing the general public about cyber incidents, as anticipated in the draft law[58], might include incidents originating from credit institutions.

4.7 In light of the above, the ECB recommends clarifying that the scope of the draft law and any powers granted to the DSA thereunder are without prejudice to the competences, tasks and powers of the ECB and the CBC under Regulation (EU) No 1024/2013 and relevant national law[59]. In addition, to enable the ECB and the CBC to fulfil their tasks within the SSM, the ECB recommends that, for the purposes of the draft law, cooperation and information-sharing arrangements are established not only between the DSA and the CBC, but also between the DSA and the ECB, through the CBC as referred to in paragraph 2.3[60]. Examples of areas which such cooperation and information-sharing arrangements may helpfully address include, but are not limited to, reporting requirements imposed on credit institutions, the process for deciding on publication of information concerning individual cybersecurity incidents, and the safeguarding of the continuity of critical functions of credit institutions.

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

Done at Frankfurt am Main, 2 May 2019.

[signed]

The President of the ECB

Mario DRAGHI

58 See Article 35 of the draft law.

59 See also paragraph 4 of Opinion CON/2018/22; paragraph 3.5 of Opinion CON/2018/39; and paragraph 8.7 of Opinion CON/2018/47.

60 See also paragraph 4.6 of Opinion CON/2018/22 and paragraph 8.7 of Opinion CON/2018/47.