OPINION OF THE EUROPEAN CENTRAL BANK

of 8 November 2018

on designation of essential services and operators of essential services for the purpose of network and information systems security

(CON/2018/47)

Introduction and legal basis

On 5 October 2018 the European Central Bank (ECB) received a request from the Slovenian Ministry of Public Administration for an opinion on a draft decree on the designation of essential services and a more detailed methodology for the designation of the operators of essential services (hereinafter the 'draft decree').

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[1], as the draft decree relates to Banka Slovenije, payment and settlement systems and rules applicable to financial institutions insofar as they materially influence the stability of financial institutions and markets, and the tasks conferred on 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 decree

1.1 The draft decree is to be adopted by the Government of the Republic of Slovenia as an implementing regulation under the Law on information security[2]. The latter transposed Directive (EU) 2016/1148 of the European Parliament and of the Council[3] into Slovenian legislation. It lays down a framework the aim of which is to ensure that appropriate information systems-related security measures are taken to prevent, notify and react to cyber incidents. The Law on information security designates the national security incident response teams and their tasks, and sets up the national competent authority for information security (hereinafter the 'national information security authority'), which also acts as a single point of contact on information security. It also lays down the competences and duties of the national information security authority and provides to it and its inspectors the powers and means to enforce compliance by the providers of relevant services.

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 *Zakon o informacijski varnosti (ZinfV)*(2018) (Official Gazette of the Republic of Slovenia, No 30/18).

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).

1.2 The Law on information security applies to the following service providers: (i) operators of essential services; (ii) digital service providers; and (iii) state administration authorities managing information systems and providing information services necessary for the smooth functioning of the State and for safeguarding national security. As regards the operators of essential services, it foresees that this will include entities operating in the relevant sectors as specified by the Law, including, *inter alia*, banking and financial market infrastructures. The Law empowers the Government to designate individual entities as operators of essential services. First, however, it requires the Government to draw up a more detailed list of essential services from the relevant sectors, and to specify in more detail the methodology for the designation of the operators of those services[4]. It is the purpose of the draft decree to address these elements.

1.3 As regards the detailed list of services, the draft decree lists individual services using the standard classification of activities. In the banking sector the draft decree specifies the following services[5]: (i) 'central banking' (acting as banker for the government sector, including with regard to sub-accounts for pension, health and social insurance); (ii) 'other monetary intermediation' (acceptance of deposits and granting of loans by banks, savings banks and credit unions); and (iii) 'other activities auxiliary to financial services, except insurance and pension funds' (the activity of processing financial transactions and settlement activity, including credit card transactions and payment transactions). In the financial market infrastructures sector the draft decree specifies the following: (i) 'administration of financial markets' (operating and supervising financial markets other than by State authorities: collective safekeeping of securities, determining and executing obligations arising from securities transactions and maintaining a central register of holders of book-entry securities); and (ii) 'securities brokerage' (trading in securities traded on a trading venue pursuant to the law governing the market in financial instruments and related activities, and securities brokerage).

1.4 The draft decree explicitly states that it (i) does not apply to services the provision of which depends on information systems operated by the European System of Central Banks (ESCB); (ii) does not apply to services the provision of which depends on information systems operated by Banka Slovenije which are supervised by the ESCB; and (iii) is without prejudice to the supervision of information systems falling within the competence of Banka Slovenije or the ESCB governed by laws of the European Union or by laws of the Republic of Slovenia adopted on the basis of Union laws[6]. Further, the draft decree provides that the designation of individual entities as operators of essential services in the banking sector requires the prior consent of Banka Slovenije if the provision of such services depends on information systems of Banka Slovenije which are not information systems excluded by the draft decree as described in points (i) and (ii) above and which are used by Banka Slovenije for the performance of its tasks pursuant to the Law on Banka

4 See Articles 5, 6(1) and (2) and 7(4) of the Law on information security.
5 See the Annex to the draft decree and Articles 13 and 14 of the draft decree.
6 See Article 2 of the draft decree.

Slovenije[7], the Statute of the European System of Central Banks and of the European Central Bank (hereinafter the 'Statute of the ESCB') and Union laws[8].

1.5 In addition to any designation of operators of essential services on the basis of the draft decree as described above, the Law on information security also requires the Government to designate as operators of essential services the operators of critical infrastructures designated pursuant to the Law on critical infrastructures[9],[10].

2 General observations

2.1 As previously noted[11], the ECB supports the aim of Directive (EU) 2016/1148 of ensuring a high common level of network and information security across the Union and of achieving a consistent 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[12].

2.2 As regards specific provisions of the draft decree concerning information systems operated or 'supervised' by Banka Slovenije and/or the ESCB as described in paragraph 1.5, the ECB understands that the term 'supervision' (Slovene: *nadzor*) as used in the draft decree includes both 'supervision' and 'oversight'. Under Slovenian law the term 'supervision' may be understood as referring to the concepts of both 'supervision' and 'oversight', as those terms are understood in, for example, the English language.

3 Impact of the draft decree on systemically important payment systems (SIPS) and TARGET2-Securities

3.1 The ECB 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. This Regulation 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)[13] in a legally binding manner. It recently introduced a number of new requirements for SIPS operators addressing new risks, including those related to operational and security risks

7 *Zakon o Banki Slovenije (ZBS-1)* (2002) (Official Gazette of the Republic of Slovenia, No 72/06 – official consolidated text, 59/11 and 55/17).

8 See Article 6(4) of the draft decree.

9 *Zakon o kritični infrastrukturi (ZKI)* (2017) (Official Gazette of the Republic of Slovenia, No 75/17). The ECB was consulted on that Law and issued Opinion CON/2017/31.

10 See Article 6(3) of the Law on information security.

11 See e.g. paragraph 2.1 of Opinion CON/2014/58, paragraph 2.1 of Opinion CON/2017/10, paragraph 2.2 of Opinion CON/2018/22, paragraph 2.2 of Opinion CON/2018/27 and paragraph 3.1 of Opinion CON/2018/39. All ECB opinions are published on the ECB's website at www.ecb.europa.eu.

12 See e.g. Article 15(4a) 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).

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

(such as cyber resilience)[14], taking into account, *inter alia*, the Committee on Payments and Market Infrastructures (CPMI)-IOSCO Guidance on cyber resilience for financial market infrastructures which was published in 2016[15]. Among listed SIPS, TARGET2 plays a distinct role, as it is owned and operated by the Eurosystem and subject to strict regulation and oversight.

3.2 The ECB understands, on the basis of Article 2(1) and (2) of the draft decree, which exempts services provided using information systems operated by the ESCB or operated by Banka Slovenije and supervised or overseen by the ESCB from the scope of the draft decree, that such services are, consequently, also exempt from the scope of the Law on information security. The ECB welcomes this, as it should help to ensure that the Slovenian legislation on information security does not encroach on the ESCB's competences, consistent with the principles of the primacy of Union law and of central bank independence pursuant to Article 130 of the Treaty[16].

3.3 In particular, the ECB understands that, on the basis of Article 2(1) of the draft decree, TARGET2-Securities (T2S) services would be exempt from the scope of the relevant legislation, since pursuant to Article 6 of Guideline ECB/2012/13 of the European Central Bank[17] and Article 7 of the T2S Framework Agreement[18], T2S is operated by the ESCB. Further, in line with the Governing Council's decision in its Eurosystem oversight policy framework (revised version of July 2016)[19], T2S falls under Eurosystem oversight competences under Articles 127(2) of the Treaty and Articles 3(1) and 22 of the Statute of the ESCB.

3.4 The ECB also understands that, on the basis of Article 2(2) of the draft decree, the Slovenian component of TARGET2 is exempt from the scope of the draft decree and the Law on information security, since Banka Slovenije acts as the operator of that component. TARGET2 has been identified, pursuant to Decision ECB/2014/35 of the European Central Bank[20], as a SIPS and is overseen by the ECB as competent authority under Regulation (EU) No 795/2014.

3.5 The ECB understands that Article 2(3) of the draft decree aims to limit the impact of the draft decree on supervision or oversight which is performed by Banka Slovenije or ESCB central banks on the basis of Union law[21] such that any designation of operators of essential services pursuant

---

14 See Article 15, 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.

15 Available on the Bank for International Settlements' website.

16 See e.g. paragraph 2.2 of Opinion CON/2014/58, paragraph 2.2 of Opinion CON/2017/10, paragraph 3.1.1 of Opinion CON/2018/22 and paragraph 3.2.1 of Opinion CON/2018/39.

17 Guideline ECB/2012/13 of the European Central Bank of 18 July 2012 on TARGET2-Securities (OJ L 215, 11.8.2012, p. 19).

18 Available on the ECB's website.

19 Available on the ECB's website.

20 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).

21 As described in paragraph 1.3, the draft decree includes in the list of essential services 'activity of processing financial transactions and settlement activity, including credit card transactions and payment transactions', and 'administration of financial markets' (operating and supervising financial markets other than by State authorities: collective safekeeping of securities, determining and executing obligations arising from securities transactions and maintaining a central register of holders of book-entry securities).

to the draft decree, and the consequential application of the Law on information security to such designated operators, will be without prejudice to the performance of that supervision or oversight. In addition to exempting the Slovenian component of TARGET2 from the scope of the Law on information security, the ECB understands that, on the basis of Article 2(3), the relevant Slovenian legislation will not encroach on the Eurosystem's competences in the field of SIPS, including through any supervisory powers of the national information security authority and its inspectors under the Law on information security.

4 Impact of the draft decree on non-SIPS

4.1 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[22] non-SIRPS have been divided into two distinct groups: prominently important retail payments systems (PIRPS) and other retail payments systems (ORPS). The Slovenian local retail clearing and payment systems have been classified as PIRPS or ORPS[23] and the ECB understands that in the present case, as their services are of the type included in the list of essential services pursuant to the draft decree, the operators of those systems or some of them might be designated as operators of essential services, thereby falling within the Law on information security and becoming subject to the supervisory measures of the national information security authority and its inspectors.

4.2 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)[24]. 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), however there is, strictly speaking, no Union legislation regulating the oversight or supervision of these systems[25]. Banka Slovenije is given supervisory and oversight competence over non-SIPS pursuant to the Law on payment services, services concerning issuing electronic money and payment systems[26], which in this particular matter does not implement Union 'laws' as described in this paragraph 4.2 above[27].

4.3 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 network and information

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

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

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

25 See paragraph 2.4.4 of ECB Opinion CON/2017/31 and paragraph 3.2.3 of Opinion CON/2018/22.

26 *Zakon o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (ZPlaSSIED)* (2018) (Official Gazette of the Republic of Slovenia No 7/18 and 9/18 – corr.).

27 See also paragraph 2.4.4 of Opinion CON/2017/31.

security-related laws[28].

4.4 If it is intended that non-SIPS are excluded from the scope of the draft decree and the Law on information security, the ECB suggests that, in the interest of legal certainty, it is explicitly clarified that the relevant legislation does not encroach on the oversight of non-SIPS by Banka Slovenije or the ESCB that are subject to applicable oversight frameworks, guidelines and principles. If the Slovenian authorities, however, consider it necessary to include non-SIPS within the scope of the draft decree and the Law on information security, it notes that Article 27(2)(5) of the Law on information security foresees that the national information security authority cooperates with the regulators and supervisors of the sectors in which the respective essential services are provided. The ECB suggests that, in applying this, effective information-sharing and cooperation arrangements are put in place to ensure that the national information security authority shares information about actual and potential cyber incidents as well as measures planned or adopted by the national information security authority which affect non-SIPS with Banka Slovenije in a timely and efficient manner in order to enable Banka Slovenije to fulfil its tasks under the Treaty and Slovenian law. It would, in any case, be advisable to clarify the exact scope of the draft decree and the Law on information security and the supervisory powers of the national information security authority and its inspectors in relation to non-SIPS to avoid potential confusion on the applicable standards and the powers of the relevant authorities[29].

5 Impact of the draft decree on critical service providers

The revised Eurosystem oversight policy framework[30] covers critical service providers. Similar to the case of non-SIPS, it cannot be excluded that the draft decree and the supervisory powers of the national information security authority could cover critical service providers for which the applicable oversight measures, insofar as soft law instruments, would not be considered Union laws within the meaning of Article 2(3) of the draft decree. It is therefore suggested that the Slovenian authorities take existing oversight arrangements into consideration in their application of the Law on information security, if such application would affect critical service providers[31].

6 Impact of the draft decree on payment services and payment instruments and schemes

6.1 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 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) are subject

28 See paragraph 3.2.4 of Opinion CON/2018/22.
29 Ibid.
30 P. 9.
31 See paragraph 3.3.1 of Opinion CON/2018/22.

to Directive (EU) 2015/2366 of the European Parliament and of the Council[32], which is applicable as of January 2018, as implemented into national law. While PSPs are therefore subject to Union and Slovenian legislation (including regulations based on Union legislation), the oversight of international and domestic card schemes is not subject to Union legislation as such[33].

6.2 It is not fully clear to the ECB if various payment schemes and instruments are covered by the type of services listed in the draft decree as 'other activities auxiliary to financial services, except insurance and pension funds'. It is thus suggested that the same clarification, effective information-sharing and cooperation framework as mentioned in paragraph 4.4 are provided and put in place in relation to and between the authorities responsible for the oversight of payment schemes, instruments and services and the national information security authority[34].

7 Impact of draft decree on central securities depositories (CSDs)

7.1 CSDs are strictly regulated and supervised by different authorities pursuant to Regulation (EU) No 909/2014 of the European Parliament and of the Council[35], 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.

7.2 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 national central banks 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.

7.3 KDD d.d., the Slovenian CSD, is supervised by Banka Slovenije and the Slovenian Securities Market Agency and overseen by Banka Slovenije[36]. While KDD appears to be covered by the type of services listed in the draft decree, such as collective safekeeping of securities, determining and executing obligations arising from securities transactions and maintaining a central register of

---

32 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).

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

34 See paragraph 3.4.3 of Opinion CON/2018/22.

35 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).

36 Supervision of KDD is regulated in the Law on the financial instruments market (2007) (*Zakon o trgu finančnih instrumentov (ZTFI)* (Official Gazette of the Republic of Slovenia No 108/10 – official consolidated text, 78/11, 55/12, 105/12 – ZBan-1J, 63/13 – ZS-K, 30/16 and 9/17) and the Decree on the implementation of the EU Regulation on improving securities settlement in the European Union and on central securities depositories (2016) (*Uredba o izvajanju Uredbe (EU) o izboljšanju ureditve poravnav vrednostnih papirjev v Evropski uniji in o centralnih depotnih družbah* (Official Gazette of the Republic of Slovenia No 60/16). The Securities Market Agency issues authorisation to, and supervises, KDD in the provision of notary services and central maintenance services and other related non-banking-type ancillary services.

holders of book-entry securities, the ECB understands that the Law on information security should be without prejudice to the supervision and oversight of the KDD, given that such supervision and oversight is performed on the basis of Union legislation. The draft decree should, however, be amended to clarify that the national information security authority's responsibilities are without prejudice to and are aligned with the tasks not only of Banka Slovenije but also of the Securities Market Agency.

8 Impact of draft decree on credit institutions

8.1 Pursuant to Article 2(3) of the draft decree, the draft decree is without prejudice to the supervision of information systems falling within the competence of Banka Slovenije or of the ESCB. Thus, the ESCB's competence under Union law and the supervision of information systems under Banka Slovenije's competence should not be affected by the draft decree. However, the ECB understands that some credit institutions established in Slovenia can be designated as operators of essential services, and thus would need to comply with their obligations under the Law on information security. Against this background, the following points are noted.

8.2 Council Regulation (EU) No 1024/2013[37] 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 SSM's functioning, based on a distribution of responsibilities between the ECB and NCAs, including Banka Slovenije. In particular, the ECB carries out its task of authorising and withdrawing the authorisations of all credit institutions. For significant credit institutions the ECB also has the task, among others, of ensuring compliance with relevant Union law imposing prudential requirements on credit institutions, including the requirement to have in place robust governance arrangements, including sound risk management processes and internal control mechanisms[38]. 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[39].

8.3 The prudential supervision of credit institutions also covers topics related to cybersecurity and the protection of infrastructures relevant for the operation of credit institutions 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 events[40]. In this respect, the ECB has the power, among others, to restrict or limit the business, operations or network of an institution or to request the divestment of activities that pose excessive risks to the soundness of an institution[41]. Since the

37 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).

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

39 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 (OJ L 176, 27.6.2013, p.338), see also paragraph 4.1 of Opinion CON/2018/22 and paragraph 3.5.1 of Opinion CON/2018/39.

40 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).

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

assessment of the adequacy of the internal governance arrangements of credit institutions is one of the core competences of prudential supervisors, the draft decree and the requirements under the Law on information security should not interfere with the tasks that prudential supervisors carry out in this respect[42].

8.4 Under the Law on information security, the national information security authority has a range of powers to address cybersecurity incidents. In particular, it may, in the case of a major or critical cybersecurity incident and cyber attack or a threat thereof, impose such relevant and proportionate measures on the addressees of the Law as are deemed necessary and proportionate to prevent the continuation of an ongoing incident or the realisation of a threatening incident and to eliminate the consequences of incidents and to limit the expected consequences of a threat thereof[43]. The inspectors of the national information security authority, when enforcing compliance with the Law, may also impose measures to eliminate any identified shortcomings[44]. They may also prohibit providers of essential services from using their information system until established shortcomings have been eliminated, but only in extreme cases, and taking into account the significance of the sector in which they are operating and of their system and activities, if such a measure does not threaten supply in an individual sector or the provision of their services[45].

8.5 It is acknowledged that the tasks of the ECB and Banka Slovenije as prudential supervisors are in a number of critical respects distinct from the tasks and competences of national security incident response teams and the national information security authority. Nevertheless, there could be an overlap where the actions of the latter could affect the prudential supervision of credit institutions under Union and Slovenian law. This would be most evident if the national information security authority and its inspectors chose, when using their powers under the Law on information security, to restrict the use of an information system. If the use of an information system used by a significant credit institution for the provision of payment services was restricted, this could significantly impact the continuous operation and financial standing of the institution. Additionally, informing the affected persons or the general public about cyber incidents[46] could have an impact on public confidence in the affected 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 Council[47]. Further, the primary responsibility for determining that a significant credit institution is failing or likely to fail as a condition for resolution lies with the ECB[48]. In the case of resolution, one of the resolution

42 See paragraph 2.12 of Opinion CON/2014/9, paragraph 3.5 of Opinion CON/2014/58, paragraph 4.3 of Opinion CON/2018/22 and paragraph 3.5.2 of Opinion CON/2018/39.

43 See Articles 21 and 22 of the Law on information security.

44 See Article 32 of the Law on information security.

45 See Article 35 of the Law on information security.

46 See Articles 13(9) and 23 of the Law on information security.

47 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).

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

objectives is to ensure the continuity of critical functions[49], which can include the continuing functioning of the credit institution's payment function[50].

8.6 Under the Law on information security administrative pecuniary sanctions may also be imposed where the relevant service providers do not comply with their obligations under the Law[51].

8.7 In the light of the above, and since Article 2(3) of the draft decree currently only refers to the ESCB's competences under Union law and to the supervision of information systems (and not the supervision of credit institutions), the ECB suggests clarifying that the scope of the Law on information security and any powers granted to the competent authorities thereunder are also without prejudice to the competences, tasks and powers of the ECB (and Banka Slovenije) under Regulation (EU) No 1024/2013 and Slovenian law[52]. To enable the ECB and Banka Slovenije to fulfil their tasks within the SSM, the ECB also recommends that an effective framework should be put in place to ensure that the national information security authority shares information about actual and potential cyber incidents affecting significant supervised entities, as well as measures planned or adopted by it. Where relevant, the national information security authority should share information with Banka Slovenije and, through Banka Slovenije, with the ECB in a timely and efficient manner. The Slovenian legislator may also wish to consider the interaction of the national information security authority's powers under the Law on information security with the resolution-related procedures and powers of the relevant authorities[53].

9 Other information systems of Banka Slovenije

Article 6(4) the draft decree relates to information systems of Banka Slovenije which are not operated by the ESCB, nor by Banka Slovenije under the supervision of the ESCB, but which are used by Banka Slovenije for the discharge of its duties pursuant to the Law on Banka Slovenije, the Statute of the ESCB or Union legislation. The ECB understands that an example of an information system that would fall within the scope of this provision is the infrastructure for the maintenance of the treasury account system, which Banka Slovenije uses to maintain the accounts of State bodies[54]. On the basis of the explanatory memorandum to the draft decree which clarifies that the relevant provision is similar in its purpose to the equivalent provision in the Law on critical infrastructures as regards Banka Slovenije's critical infrastructures, the ECB assumes that the intention of the legislator in drafting Article 6(4) was to require Banka Slovenije's consent before any relevant decisions can be adopted under the Law on information security relating to any information system that falls within the scope of this provision, in particular the system for the maintenance of the treasury account system. As Article 6(4) is drafted unclearly its wording should be reviewed in the interest of legal certainty.

---

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

50 See paragraphs 4.4 and 4.5 of Opinion CON/2018/22.

51 See Section XI of the Law on information security.

52 See also paragraph 4 of Opinion CON/2018/22 and paragraph 3.5 of Opinion CON/2018/39.

53 See paragraph 4.6 of Opinion CON/2018/22.54 See also the Annex to the draft decree which lists a central banking service 'acting as banker for the government sector, including with regard to sub-accounts for pension, health and social insurance' as an essential service.

54 See also the Annex to the draft decree which lists a central banking service 'acting as banker for the government sector, including with regard to sub-accounts for pension, health and social insurance' as an essential service.

10 Miscellaneous

For the sake of legal certainty it should be ensured that the exemptions and safeguards laid down in the draft decree also apply to operators of critical infrastructures in their capacity as operators of essential services.

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

Done at Frankfurt am Main, 8 November 2018.

[signed]

The President of the ECB

Mario DRAGHI