EUROPEAN CENTRAL BANK

EUROSYSTEM

EN ECB-PUBLIC

OPINION OF THE EUROPEAN CENTRAL BANK

of 9 July 2024

on national cybersecurity

(CON/2024/24)

Introduction and legal basis

On 12 June 2024 the European Central Bank (ECB) received a request from the Ministry of Finance of the Republic of Lithuania for an opinion on a draft law on national cybersecurity (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 third and fifth indents of Article 2(1) of Council Decision 98/415/EC[1], as the draft law relates to Lietuvos bankas and to payment and settlement systems. 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 draft law replaces the Law on cyber security currently in force, which implements Directive (EU) 2016/1148 of the European Parliament and of the Council[2]. The main purpose of the draft law is to improve cybersecurity in Lithuania by strengthening and enhancing the existing measures and procedures to bolster the security of network and information systems of essential and important entities, as set out in Directive (EU) 2022/2555 of the European Parliament and of the Council[3].

1.2 More specifically, the draft law lays down provisions on the principles of cybersecurity, the institutions developing and implementing cybersecurity policy, their functions and powers, the principles for the identification of cybersecurity entities and their responsibilities, exchange of information and interinstitutional cooperation, compliance verification checks and enforcement measures, the powers of the national cybersecurity certification authority and the framework for the use of the Secure State Data Transfer Network[4].

1.3 The draft law applies to Lietuvos bankas in its entirety. The consultation request explains that although the total number of registered all-category cyber incidents decreased in 2023, compared with 2022, the number of dangerous medium-category incidents grew by 12 %. Therefore, the

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

2 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 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

4 See Article 1(1) of the draft law.

consulting authority believes that the cybersecurity of all Lithuanian public institutions, including Lietuvos bankas, should be strengthened, and that excluding Lietuvos bankas from the scope of the draft law would pose a major risk to Lithuanian national security and to the security of the Eurosystem as a whole.

1.4 The draft law provides that cybersecurity policy is set, organised, controlled and coordinated by the Ministry of Defence of the Republic of Lithuania. A cybersecurity policy is to be set taking into account the priorities and objectives of the long-term national security policy set out in the National Security Strategy approved by the Seimas (Parliament), the strategic objectives and other objectives set out in the National Progress Plan approved by the Government, the priorities and orientation for the strengthening and development of the national defence system approved by the Seimas and the National Cyber Security Development Programme approved by the Government. The cybersecurity policy is implemented by the National Cyber Security Centre (NCSC), the State Data Protection Inspectorate and the Lithuanian police[5].

1.5 As part of its cybersecurity-related tasks, the NCSC has, among other powers envisaged in the draft law, the power to (1) use cyber threat search tools in cyberspace, (2) monitor, collect and analyse information on cyber threats, (3) manage cyber incidents, warn cybersecurity entities about cyber threats and provide them with relevant information, (4) issue orders and instructions to limit the provision of public electronic communications networks and/or public electronic communications services, (5) inspect network and information systems operated by cybersecurity entities and (6) apply the necessary cybersecurity measures in the event of a cyber incident[6].

1.6 The State Data Protection Inspectorate implements a cybersecurity policy in the field of personal data protection and performs the tasks of the supervisory authority set out in Regulation (EU) 2016/679[7].

1.7 The Lithuanian police, as part of its cybersecurity-related tasks, receives and processes data and/or information on cyber incidents for the purpose of preventing, analysing, investigating or detecting criminal offences. In this respect, the Lithuanian police has the power to (1) request from cybersecurity entities the information necessary to analyse whether a cyber incident is potentially of a criminal nature, (2) require providers of public electronic communications networks, publicly available electronic communications services, electronic information hosting services, online marketplaces, online search engines and cloud computing services to preserve information relating to the services they provide and (3) where there is a reasoned court order, receive the user's traffic data and control the content of the information transmitted[8].

1.8 Supervision of the cybersecurity of Lietuvos bankas will entail remote monitoring of information and technologies, checking that Lietuvos bankas is in compliance with the cybersecurity requirements

5 See Article 4 of the draft law.

6 See Article 7 of the draft law.

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1). See also Article 9 of the draft law.

8 See Article 10 of the draft law.

determined by the draft law and on-site inspections[9]. The inspections of essential and important entities, including Lietuvos bankas, are to be carried out by the NCSC only on receipt of information indicating that the entity has infringed the requirements of the draft law[10].

1.9 Where the NCSC identifies a breach of the draft law during the inspection, it might apply one or more enforcement measures envisaged by the law[11], e.g. (1) issue warnings or instructions to implement measures necessary to prevent or contain the cyber incident, (2) issue an instruction to cease actions that infringe the requirements of the draft law, (3) appoint a monitoring officer, (4) impose a fine, (5) initiate the temporary suspension of the right to carry out part of or all of the activities of an essential entity, including Lietuvos bankas, or (6) initiate the temporary removal of the head of an essential entity from office, except where the head of a public administration entity has been appointed by a decision of the Seimas, the Government or the President of the Republic of Lithuania[12]. The draft law envisages that the temporary suspension of the right to carry out part of or all of the activities of an essential entity is to be exercised only by court order and where other enforcement measures were ineffective[13].

1.10 The draft law stipulates that prior to conducting inspections or implementing enforcement measures with regard to Lietuvos bankas, the NCSC must consult the ECB[14].

2. General observations

2.1 Directive (EU) 2022/2555 is a minimum-harmonisation directive. Article 5 of that Directive provides that it does not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law. The draft law goes beyond Directive (EU) 2022/2555, which excludes central banks (along with parliaments and the judiciary) from the definition of a 'public administration entity'[15]. This would have the consequence that the Lithuanian component of Eurosystem-owned and operated financial market infrastructures, such as TARGET, would not benefit from the exclusion of central banks from the application of Directive (EU) 2022/2555[16].

2.2 The ECB refers to its previous stance taken in the context of national measures implementing Directive (EU) 2016/1148, whereby the ECB supported the aim of Directive (EU) 2016/1148 of ensuring a high common level of network and information security across the Union and of achieving

9 See Articles 16, 26 and 27 of the draft law.

10 See Article 26(3) of the draft law.

11 See Article 28 of the draft law.

12 The ECB understands that the temporary removal from office of the head of an essential entity is not applicable to Lietuvos bankas since Lietuvos bankas qualifies as a public administration entity for this purpose, and the Governor of Lietuvos bankas is appointed by the Seimas on a proposal of the President of the Republic of Lithuania. See Article 10(4) of the Law on Lietuvos bankas.

13 See Article 32(1) of the draft law.

14 See Article 20(2)(8) of the draft law.

15 See Article 6(35) of Directive (EU) 2022/2555.

16 See paragraph 2.1 of Opinion CON/2024/14. All ECB opinions are published on EUR-Lex.

a consistency of approach in this field across business sectors and Member States[17]. The ECB strongly supports the objectives of Directive (EU) 2022/2555 to increase the level of cyber resilience across all relevant sectors, reduce inconsistencies across the internal market and improve the level of situational awareness and the collective capability to prepare and respond by ensuring efficient cooperation in the Union[18]. As already noted by the ECB, 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[19]. Directive (EU) 2022/2555 produces benefits from synergies and economies of scale. In particular, dedicated national cyber security authorities have the potential to become repositories of considerable resources and expertise which the Eurosystem may draw upon. Concurrently, it should be ensured that the provisions of the national legislation transposing Directive (EU) 2022/2555 are interpreted and applied consistently with the Eurosystem's competences, and respect the principle of central bank independence enshrined in Article 130 of the Treaty. Indeed, Lietuvos bankas' independent exercise of its tasks and responsibilities within the Eurosystem, for instance to implement monetary policy and for the smooth operation of payment and settlement systems, should not be affected. Central bank independence does not have the consequence of separating the Union's central banks entirely from the Union and exempting them from every rule of Union law[20]. This also applies to national legislative measures capable of applying to national central banks (NCBs). Furthermore, the exercise of the NCSC's powers is subject to various specific rules and guarantees, whilst the purpose for which they may be used is clearly delineated. In that respect, certain provisions of the draft law[21] provide for specifically listed powers of the NCSC to be exercised with a view to achieving the objectives set out in the draft law[22]. Therefore, national measures implementing Directive (EU) 2022/2555 that extend to NCBs, such as the draft law, are not per se precluded from applying to Eurosystem central banks[23].

3. Impact of the draft law on TARGET and on payment systems overseen by the ECB and the Eurosystem

3.1 In accordance with the fourth indent of Article 127(2) of the Treaty, 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 European System of Central Banks and of the European Central Bank (hereinafter the 'Statute of the ESCB'), the ECB and the NCBs may provide facilities, and the ECB may make regulations, to ensure efficient and sound clearing and payment systems

17 See paragraph 2.1 of Opinion CON/2014/58 of the European Central Bank of 25 July 2014 on a proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (OJ C 352, 7.10.2014, p. 4), 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 2.2 of Opinion CON/2019/17.

18 See Opinion CON/2022/14 of the European Central Bank of 11 April 2022 on the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (OJ C 233, 16.6.2022, p. 22), General observations.

19 See paragraph 2.2 of Opinion CON/2019/17.

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

21 See Chapter V of the draft law.

22 See Article 4 of the draft law.

23 See paragraph 2.2 of Opinion CON/2024/14.

within the Union and with other countries. Thus, the ECB and the Eurosystem as a whole have a particular interest in an enhanced level of network information security in respect of payment systems, as it fosters confidence in the euro and the smooth functioning of the economy in the euro area and beyond[24].

3.2 Systemically important payment systems (SIPS) such as, for example, EURO1, STEP2-T and TARGET are identified pursuant to ECB Decisions[25] and are thus overseen by the ECB as the competent authority under Regulation (EU) No 795/2014 of the European Central Bank (ECB/2014/28)[26]. SIPS are subject to regular assessment related to operational risk[27], which allows the competent Eurosystem central bank, as the 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[28].

3.3 Regulation (EU) No 795/2014 (ECB/2014/28) inter alia contains provisions aimed at ensuring cyber resilience for financial market infrastructures. It provides that a SIPS operator is required to establish an effective cyber resilience framework with appropriate governance measures in place to manage cyber risk. The SIPS operator must identify its critical operations and supporting assets, and have appropriate measures in place to protect them from, detect, respond to and recover from cyberattacks. These measures are to be regularly tested. The SIPS operator is required to ensure that it has a sound level of situational awareness of cyber threats. The SIPS operator is required to ensure that there is a process of continuous learning and evolution to enable it to adapt its cyber resilience framework to the dynamic nature of cyber risks, in a timely manner, whenever needed[29].

3.4 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 issued on the basis of Article 3.1, Article 22 and the first indent of Article 34.1 of the Statute of the ESCB[30].

---

24 See paragraph 3.1 of Opinion CON/2024/14.

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); Decision ECB/2014/36 of the European Central Bank of 13 August 2014 on the identification of EURO1 AND STEP2-T as systemically important payment systems pursuant to Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems, available on EUR-Lex.

26 Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28) (OJ L 217, 23.7.2014, p. 16).

27 See Article 15 of Regulation (EU) No 795/2014 (ECB/2014/28).

28 See paragraph 3.4 of Opinion CON/2017/10, paragraph 3.1.2 of Opinion CON/2019/17 and paragraph 3.2 of Opinion CON/2024/14.

29 See paragraph 3.3 of Opinion CON/2024/14.

30 See paragraph 3.4 of Opinion CON/2024/14.

3.5 Among the listed SIPS, TARGET plays a distinct role, as it is the large value payment system for the euro, which is owned and operated by the Eurosystem and which serves as the channel for the implementation of the euro area's monetary policy. TARGET is subject to harmonised legal conditions defined in Guideline (EU) 2022/912 of the European Central Bank (ECB/2022/8)[31]. The Lithuanian component of TARGET, TARGET-Lietuvos bankas, for which Lietuvos bankas acts as the operator, would appear to fall within the scope of the draft law, as the draft law applies to Lietuvos bankas and no exemption with regard to infrastructures or payment systems operated by Lietuvos bankas is provided.

3.6 Against this background, the ECB would welcome the establishment under the draft law[32] of cooperation arrangements between the cybersecurity implementing bodies and Lietuvos bankas. The ECB suggests that, in the context of such cooperation, effective information-sharing and consultation mechanisms are put in place in order to prevent situations which could undermine the ability of Lietuvos bankas to perform its ESCB tasks independently or to preserve the confidentiality of ESCB information. In particular, Lietuvos bankas would need to be informed about actual and potential cyber incidents, as well as planned or adopted measures which may affect the TARGET-Lietuvos bankas component in a timely and efficient manner in order to enable Lietuvos bankas to fulfil its obligations under the Treaty and the Statute of the ESCB. Such arrangements would also ensure that the cybersecurity implementing bodies and Lietuvos bankas exchange information and consult on actual and potential cyber incidents or threats in the financial sector's systems, and in particular infrastructures operated by the Eurosystem, and on planned and adopted measures, in an effective and timely manner without the need to resort to the unilateral enforcement measures envisaged under the draft law.

3.7 In addition, the ECB stands ready to cooperate with cybersecurity implementing bodies, in particular the NCSC, with a view to ensuring that best practices with regard to Directive (EU) 2022/2555 are established and followed[33]. As noted above, the draft law stipulates that prior to conducting inspections or implementing enforcement measures with regard to Lietuvos bankas, the NCSC must consult the ECB[34]. The ECB understands that the purpose of this consultation would inter alia be to ensure that any supervisory or enforcement measures directed at Lietuvos bankas do not inadvertently disrupt the operations of other members of the Eurosystem and the Eurosystem as a whole, and to identify alternative measures that can achieve a comparable effect without compromising the integrity of TARGET, the confidentiality of ESCB information or the interests of other NCBs and the ECB. This consultative process would be crucial in safeguarding the collective interests of the Eurosystem and ensuring that all actions are harmoniously aligned with the broader objectives of the ECB's monetary policy. The ECB also suggests that the respective cooperation and information-sharing arrangements are established between the NCSC and the ECB, through Lietuvos bankas, to ensure that the overall functioning of TARGET is not undermined.

---

31 Guideline (EU) 2022/912 of the European Central Bank of 24 February 2022 on a new-generation Trans-European Automated Real-time Gross Settlement Express Transfer system (TARGET) and repealing Guideline ECB/2012/27(ECB/2022/8) (OJ L 163, 17.6.2022, p. 84); see also paragraph 3.5 of Opinion CON/2024/14.

32 See Article 20(1) of the draft law.

33 See paragraph 6.3 of Opinion CON/2018/22 and paragraph 2.4 of Opinion CON/2019/17.

34 See Article 20(2)(8) of the draft law.

This opinion will be published on EUR-Lex.

Done at Frankfurt am Main, 9 July 2024.

[signed]

The President of the ECB

Christine LAGARDE