Paweł Pelc*

The Polish Financial Supervision Authority in the national cybersecurity system

Abstract

The Polish Financial Supervision Authority is the authority competent for cybersecurity for the banking sector and financial market infrastructure. It is the only cybersecurity authority that does not have the status of a minister managing a government administration department as well as being the only authority competent for cybersecurity outside the structure of the government administration and not operating within the legal personality of the State Treasury. Only some entities supervised by the Polish Financial Supervision Authority under the regulations on supervision over the financial market are subject to its supervision as the authority competent for cybersecurity. Regulatory differences lead to the necessity to apply different rules when the Polish Financial Supervision Authority carries out controls under the regulations on financial market supervision and controls under the National Cybersecurity System Act.

Key words: The Polish Financial Supervision Authority, supervisory authority, administrative authority, national cybersecurity network

* Paweł Pelc, War Studies University in Warsaw, Academic Centre for Cyber Security Policy, e-mail: pawel.pelc@gmail.com, ORCID: 0000-0002-5007-568X.

Existing since 2006, the Polish Financial Supervision Authority – an integrated financial market regulator[1] – upon the entry into force on 28 August 2018 of the National Cybersecurity System Act of 5 July 2018[2] – became the authority competent for cybersecurity for the banking sector and financial market infrastructure, in accordance with Art. 41(4) thereof. None of these terms are defined in the glossary to the National Security System Act contained in Art. 2 Annex 1, describing sectors and subsectors and types of entities, defines the „Banking and Financial Market Infrastructure" sector, which includes credit institutions, domestic banks, branches of foreign banks, branches of credit institutions, credit unions, a regulated market operator, a CCP (a legal person that interposes itself between the counterparties to the contracts traded on one or more financial markets, becoming the buyer to every seller and the seller to every buyer), and a joint stock company that is a subsidiary of the National Securities Depository, to which the National Securities Depository has delegated by written agreement the performance of its statutory tasks. Despite the use of the term „banking sector and financial market infrastructure sector" in Art. 41(4) of the National Cybersecurity System Act, and the definition of the sector in Annex 1 thereto, referred to as „Banking and financial market infrastructure" which would lead to the conclusion that these are not the same concepts, the only rational interpretation is to determine that in both cases the scope of regulation is the same. Indeed, it should be pointed out that neither the term 'banking sector' nor the term „financial market" are explicitly defined in the Act of 21 July 2006 on financial market supervision[3]. This Act only defines, in Art. 1(2)(1), banking supervision by referring to the regulations of the Banking Law[4], the Act of 29 August 1997 on the National Bank of Poland[5], the Act of 29 August 1997 on Mortgage Bonds and Mortgage Banks[6], the Act of 7 December 2000 on the Operation of Cooperative Banks[7]

1 P. Pelc, *The Polish Financial Supervision Authority in the Polish administrative system*, „Cybersecurity and Law" 2022, no. 2.

2 Consolidated text, Journal of Laws 2022, item 1863.

3 Consolidated text, Journal of Laws 2022, item 660. Cf. P. Pelc, *Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa*, „Cybersecurity and Law" 2019, no. 2, p. 152–153.

4 The Act of 29 August 1997 – the Banking Law, consolidated text, Journal of Laws 2021, item 2439.

5 Consolidated text, Journal of Laws 2022, item 2025.

6 Consolidated text, Journal of Laws 2022, item 581.

7 Consolidated text, Journal of Laws 2022, item 1595.

and the EU Regulation on Prudential Requirements for Credit Institutions[8]. The reference to the scope of banking supervision contained in the Act on Financial Market Supervision is additionally flawed in that there is no separate supervision over financial market infrastructure. Under the Act on Financial Market Supervision, the entities listed in Annex 1 to the National Cybersecurity System Act are subject not only to banking supervision but also to capital market supervision and supervision over credit unions. If the reference to the regulations of the Act on Financial Market Supervision does not allow proper reconstruction of the scope of the term 'banking and financial market infrastructure sector', and this term is not separately defined in Article 2 of the National Cybersecurity System Act, as well as the meaning of this term cannot be clearly determined using the linguistic meaning of this term, the only reasonable possibility to determine the meaning of the provision set out in Art. 41(4) of the National Cybersecurity System Act is to interpret it following the wording of Annex 1 thereto and assume that the term „banking sector and financial market infrastructure" should be construed as the Banking and Financial Market Infrastructure sector. This leads to the conclusion that the Polish Financial Supervision Authority is the authority competent for cybersecurity not for all entities that are subject to its supervision under the Act on Financial Market Supervision, but only for entities that are part of the Banking and Financial Market Infrastructure Sector, pursuant to Annex 1 to the National Cybersecurity System Act. According to the Report on the activities of the UKNF (Polish Financial Supervision Authority) and the KNF Board (Board of the Polish Financial Supervision Authority) in 2018[9] in accordance with Art. 86 of the National Cybersecurity System Act, „the KNF Board identified, by 9 November 2018, 19 entities representing the banking sector and financial market infrastructure which met the criteria for recognition as operators of essential services, and issued the related decisions"[10]. In the following years, the KNF Board issued decisions regarding further two entities, as well as two decisions on the expiration of the decision to recognise an entity as an

8 Regulation (EU) 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, Official Journal of the European Union 2003, L 176.

9 *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2018 roku*, https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie%20z%20dzia%C5%82alno%C5%9Bci%20UKNF%20oraz%20KNF%20w%202018%20roku_66979.pdf [access: 4.10.2022].

10 Ibidem, p. 193.

operator of essential services, therefore, as of the end of 2021, there were 19 entities recognised as operators of essential services by the KNF Board as an authority competent for cybersecurity, with 15 entities belonging to the banking and credit union sector and 4 entities belonging to the financial market infrastructure sector[11].

Entrusting the Polish Financial Supervision Authority with the role of an authority competent for cybersecurity is an unusual solution on the grounds of Art. 41(1–3) and (5–11) of the National Cybersecurity System Act because it is the only authority competent for cybersecurity that does not have the status of minister (the other authorities competent for cybersecurity are the ministers competent for energy, transport, maritime economy, inland navigation, health, water management, computerisation and the Minister of National Defence)[12]. Thus, all other authorities competent for cybersecurity have the status of a constitutional minister heading a government department[13], are part of the Council of Ministers and form part of the government administration, and operate under the legal personality of the State Treasury. In the case of the Polish Financial Supervision Authority, the situation is different, it is admittedly a public administration body, but it is not a government administration body, it is not part of the Council of Ministers, nor does it head a government administration department. In addition, as of 1 January 2019, the UKNF became a state-owned legal person, and the KNF Board – its body, that is – began to function outside the scope of the legal personality of the State Treasury[14].

11 *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2020 r.*, Warszawa 2021, p. 136, https://www.knf.gov.pl/knf/pl/komponenty/img/SPRAWOZADANIE%202020_76375.pdf [access: 4.10.2022]; *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 r.*, p. 150–151, https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie_z_dzialalnosci_UKNF_oraz_KNF_w_2021_roku_78361.pdf [access: 4.10.2022].

12 More extensively on the tasks of the Minister of National Defence: K.A. Wąsowski, *Cognition of the Minister of National Defence in the scope of cybersecurity*, „Cybersecurity and Law" 2019, no. 1, p. 11–24; M. Karpiuk, *Tasks of the Minister of National Defence in the area of cybersecurity*, ibidem 2022, no. 1, p. 85–94.

13 Cf. A. Brzostek, *Organy właściwe do spraw cyberbezpieczeństwa* [in:] *System cyberbezpieczeństwa*, Warszawa 2021, p. 200–202.

14 P. Pelc, *The Polish…*; M. Torończak, *Kilka uwag na temat nowej konstrukcji nadzoru nad rynkiem finansowym*, „Monitor Prawniczy" 2019, no. 10, p. 537; A. Nadolska, *Soft law w regulacji rynku finansowego w Polsce: rekomendacje, wytyczne i lista ostrzeżeń publicznych KNF*, Warszawa 2021.

According to Art. 41 of the National Cybersecurity System Act, an authority competent for cybersecurity (which also means the Polish Financial Supervision Authority with respect to the banking and financial market infrastructure sector): 1) analyses, on an ongoing basis, entities in a given sector or sub-sector in terms of recognising them either as an operator of essential services or non-compliance with the conditions qualifying a given entity as an operator of essential services; 2) issues decisions recognising a given entity as an operator of essential services, or decisions confirming the expiration of the decision recognising a given entity as an operator of essential services; 3) immediately after issuing a decision recognising a given entity as an operator of essential services or a decision confirming the expiration of the decision recognising a given entity as an operator of essential services, submits applications to the minister competent for computerisation to enter that entity in the list of operators of essential services or to remove it from that list; 4) submits applications to change data in the list of operators of essential services, not later than within six months from the change of these data; 5) prepares, in cooperation with CSIRT NASK, CSIRT GOV, CSIRT MON and sectoral cybersecurity teams, recommendations on actions aimed at strengthening cybersecurity, including sectoral guidelines on incident notifications; 6) monitors the application of the provisions of the Act by operators of essential services and digital service providers; 7) requires operators of essential services or digital service providers, at the request of CSIRT NASK, CSIRT GOV or CSIRT MON, to remove, within the prescribed period, the vulnerabilities that have led or could lead to a serious, significant or critical incident; 8) conducts inspections of operators of essential services and digital service providers; 9) may cooperate with the competent authorities of EU Member States via the Single Point of Contact; 10) processes information, including personal data, about the essential and digital services being provided and the operators of essential services or digital service providers to the extent necessary to perform the tasks provided for in the Act; 11) participates in cybersecurity exercises organised in the Republic of Poland or in the European Union.

On the other hand, there are doubts about the possibility to apply to the Polish Financial Supervision Authority the powers under Art. 41(3) to (6) of the National Cybersecurity System Act to entrust, on its behalf, the performance of some of these tasks to units subordinate to or supervised by it, which results from the separateness of the Polish Financial Supervision Authority from the other authorities competent for cybersecurity. The Polish Financial

Supervision Authority has no subordinate units, and only supervises financial market entities. For these reasons, despite the absence of an explicit provision excluding the application of Art. 41(3) of the National Cybersecurity System Act to the Polish Financial Supervision Authority, it should be considered inapplicable to the Polish Financial Supervision Authority for the above reasons. The National Cybersecurity System Act provides that in justified cases the authorities competent for cybersecurity, and this means the Polish Financial Supervision Authority too, shall cooperate with law enforcement agencies and the authority competent for the protection of personal data. It should be pointed out that, according to Art. 16(5) of the Act on Financial Market Supervision, giving notice of a suspected criminal offence or providing further information in addition to this notice shall not violate the obligation of professional secrecy, while based on the regulation on professional secrecy, cooperation with law enforcement agencies may raise problems if this would require the provision of information covered by professional secrecy without giving notice of a suspected criminal offence as long as these would be other authorities than those specified in Art. 17ca of the Act on Financial Market Supervision. The authorities competent for cybersecurity, including the Polish Financial Supervision Authority, are authorised to obtain information under the rules laid down in Art. 43 of the National Cybersecurity System Act, as well as establish a sectoral cybersecurity team under Art. 44 of the National Cybersecurity System Act.

Pursuant to Art. 53 of the National Cybersecurity System Act, the authorities competent for cybersecurity, including the Polish Financial Supervision Authority, exercise supervision[15] within the scope of the compliance with the provisions of the National Cybersecurity System Act concerning the performance by operators of essential services of their obligations imposed under the National Cybersecurity System Act regarding counteracting cybersecurity threats and reporting serious incidents, as well as meeting by digital service providers the requirements regarding the security of the digital services they provide, as specified in Implementing Regulation 2018/151 and the performance of the obligations provided by the Act for reporting significant incidents. They may conduct inspections in this regard and impose fines on operators of essential services and digital service providers.

15 M. Nowikowska, *Nadzór i kontrola operatorów usług kluczowych, dostawców usług kluczowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa*, „Cybersecurity and Law" 2021, no. 1, p. 77–103.

Control in respect of entities that are enterprises is subject to the provisions of Chapter 5 the Act of 6 March 2018 – the Enterprise Law[16], whilst the National Cybersecurity System Act further specifies the obligations of controlled enterprises, the evidence procedure during the control which is carried out by persons performing inspection activities, and it also regulates issues related to control reports with post-control recommendations. In contrast, the National Cybersecurity System Act does not provide for the application of regulations regarding control carried out by the Polish Financial Supervision Authority of supervised entities in this regard. It should be recognised that the regulation in Art. 53–59 of the National Cybersecurity System Act is of a special nature in respect of the regulations regarding control carried out by the Polish Financial Supervision Authority in supervised entities contained in the regulations on particular types of entities supervised under the Act on Financial Market Supervision.

Under Art. 86 of the National Cybersecurity System Act, the authorities competent for cybersecurity, including the Polish Financial Supervision Authority, were required, by 9 November 2018, to issue a decision on recognising an operator of essential services and to submit to the Minister competent for computerisation applications to include operators of essential services in the list of operators of essential services. The Polish Financial Supervision Authority fulfilled this obligation on time[17].

On 1 April 2019 the Cybersecurity Department was established within the UKNF's organisational structure „responsible for 1) the supervision of financial market entities in the area of ICT risk and cybersecurity in terms of financial market supervision; 2) the performance of tasks under the National Cybersecurity System Act of 5 July 2018 [...]; 3) undertaking measures to ensure a high level of cybersecurity at the UKNF"[18].

In addition, on 1 July 2020, the KNF Board as an authority competent for cybersecurity established the KNF CSIRT acting as the Sectoral Team for Cybersecurity to coordinate activities and support the management

16 Consolidated text, Journal of Laws 2021, item 162.

17 *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2018*..., p. 193.

18 *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2019 r*., Warszawa 2020, p. 140, https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie%202019.pdf [access: 4.10.2022].

of security incidents of financial market entities recognised as operators of essential services[19].

According to the information provided by the UKNF, the KNF Board has effectively stepped into the role of an authority competent for cybersecurity in accordance with the regulations of the National Cybersecurity System Act, whilst its different nature from other authorities competent for cybersecurity does not have an adverse impact on fulfilling this role. Given its role as a financial market regulator, the Polish Financial Supervision Authority should be considered a body well-prepared to carry out supervisory and control functions on the grounds of the National Cybersecurity System Act, irrespective of the regulatory differences between the regulations on financial market supervision and controls carried out within this supervision, and the supervision it exercises as the authority competent for cybersecurity and controls carried out under the National Cybersecurity System Act.

Bibliography

Brzostek A., *Organy właściwe do spraw cyberbezpieczeństwa* [in:] *System cyberbezpieczeństwa*, Warszawa 2021.

Karpiuk M., *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.

Nadolska A., *Soft law w regulacji rynku finansowego w Polsce: rekomendacje, wytyczne i lista ostrzeżeń publicznych KNF*, Warszawa 2021.

Nowikowska M., *Nadzór i kontrola operatorów usług kluczowych, dostawców usług kluczowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa*, „Cybersecurity and Law" 2021, no. 1.

Pelc P., *Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa*, „Cybersecurity and Law" 2019, no. 2.

Pelc P., *The Polish Financial Supervision Authority in the Polish administrative system*, „Cybersecurity and Law" 2022, no. 2.

Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2018 r., Warszawa 2019, https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie%20z%20dzia%C5%82alno%C5%9Bci%20UKNF%20oraz%20KNF%20w%202018%20roku_66979.pdf [access: 4.10.2022].

Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2020 r., Warszawa 2021, https://www.knf.gov.pl/knf/pl/komponenty/img/SPRAWOZADANIE%202020_76375.pdf [access: 4.10.2022].

Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie_z_dzialalnosci_UKNF_oraz_KNF_w_2021_roku_78361.pdf [access: 4.10.2022].

19 *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2020...*, p. 137; *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021...*, p. 151–154.

Torończak M., *Kilka uwag na temat nowej konstrukcji nadzoru nad rynkiem finansowym*, „Monitor Prawniczy" 2019, no. 10.
Wąsowski K.A., *Cognition of the Minister of National Defence in the scope of cybersecurity*, „Cybersecurity and Law" 2019, no. 1.

Komisja Nadzoru Finansowego w krajowym systemie cyberbezpieczeństwa

Streszczenie

Komisja Nadzoru Finansowego jest organem właściwym do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych. Jest to jedyny organ właściwy do spraw cyberbezpieczeństwa, który nie ma statusu ministra kierującego działem administracji rządowej i jednocześnie jest to to jedyny organ właściwy do spraw cyberbezpieczeństwa znajdujący się poza strukturą administracji rządowej i nie działający w ramach osobowości Skarbu Państwa. Jedynie część rodzajów podmiotów nadzorowanych przez Komisję Nadzoru Finansowego na gruncie regulacji o nadzorze nad rynkiem finansowym podlega jej nadzorowi jako organu właściwego do spraw cyberbezpieczeństwa. Odmienności regulacyjne prowadzą do konieczności stosowania odmiennych zasad w trakcie przeprowadzania przez Komisję Nadzoru Finansowego kontroli na podstawie regulacji dotyczących nadzoru na rynkiem finansowym i kontroli na podstawie ustawy o krajowym systemie cyberbezpieczeństwa.

Słowa kluczowe: Komisja Nadzoru Finansowego, organ nadzoru, organ administracji publicznej, krajowy system cyberbezpieczeństwa