# The Authorities Competent for Cybersecurity


**Agnieszka Brzostek**

**Abstract** Authorities competent for cybersecurity matters are indicated in Article 41 of the NCSA. The legislator created a catalogue of organs, at the same time specifying the scope of their properties. The legislator, while creating the catalogue of competent authorities, indicated among them ministers managing government administration departments. The Polish Financial Supervision Authority is an exception.

Various legal doubts arise in analysing the legal status of authorities and the scope of their tasks. First of all, the authorities competent for cybersecurity were explicitly indicated as an element of the National Cybersecurity System, but their exact indication as public entities was missing.

Secondly, attention should be paid to the overlapping of competences of authorities competent for cybersecurity with the competent authorities in the field of crisis management.

The specified catalogue of the scope of tasks of the organs was limited to listing their individual tasks. In the implementation of tasks, public administration bodies use their imperious forms of activity.

It is also worth noting that the competent authorities consult and cooperate with relevant national law enforcement and national data protection authorities. The presence of various legal problems and issues was the motivation behind this article.

According to Article 8 of the NIS Directive, each Member State shall designate one or more national authorities competent for the security of network and information systems, covering at least one sector. Member States may assign this role to an existing authority or authorities. Their task is to monitor the application of the Directive at the national level. The Polish legislators have named a list of these

A. Brzostek (✉)
Instytut Prawa/Institute of Law, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland
e-mail: a.brzostek@akademia.mil.pl



K. Chałubińska-Jentkiewicz et al. (eds.), *Cybersecurity in Poland*,
https://doi.org/10.1007/978-3-030-78551-2_14

authorities.[1] By identifying successively the sectors related to cybersecurity, their responsibility has been defined and assigned to successive Ministers.

The position of a Minister as a member of the Council of Ministers is emphasised in Article 149 of the Constitution of the Republic of Poland. It has been specified that the tasks of Ministers in charge of departments of government administration are defined by the appropriate Acts.[2] As P. Czarny stressed, the Constitution does not explicitly state that a given department should cover similar or related matters, which constitute a certain part of the government administration's activities under the authority of a single Minister.[3] However, Article 149(1) provides for the principle of one-person management by a Minister within the department entrusted to him or her. This is combined at the constitutional level with individual responsibility before the Sejm for matters falling within its ambit, pursuant to Article 157(2) of the Constitution of the Republic of Poland.[4] It should be stressed that a department is managed in accordance with the provisions of the Acts governing the activities of individual government administration institutions, which define more precisely the specific powers of a Minister towards them. Due to the general nature of the concept of management, it may also be of a controlling, supervisory (both in substantive and personal terms), and coordinating nature. However, such provisions cannot be interpreted restrictively. The concept of management implies a general power to influence the activities of subsidiary institutions, except for the use of instruments prohibited by law. The law should also provide for the possibility of assigning certain powers, within the scope of the broadly understood management of organisational units subsidiary to a Minister, to the Council of Ministers or the Prime Minister. The independence of a Minister in managing a department is limited not only by the provisions of the Acts, but also by Article 146(1) and (3) and Article 148(4) of the Constitution. A Minister is also bound by the "political line" established by the Council of Ministers, and the methods of its implementation specified by the Prime Minister.[5] It should be stressed that management is a standard administrative-law scenario of an administrative authority. As part of it, a Minister may apply numerous and various authoritative means of influence on the managed entities, which do not benefit from legally guaranteed independence. These means do not have to be laid down by law, although they must not conflict with the law. The choice of these means depends on the will of the managing authority. Open means can also be applied.[6] The essence of management is that it exists only in a centralised system, in which, as part of management, a superior authority may use all means of influence, e.g. an official order, by which it determines the substance of the action to

[1] Article 41 of the NCSA.

[2] Act of 4 September 1997 on Government Administration Departments (consolidated text, Polish Journal of Laws of 2020, item 1220, as amended).

[3] Czarny (2019).

[4] Czarny (2019).

[5] Czarny (2019).

[6] Góralczyk Jr (2016), pp. 126–132.

be taken by a managed entity, but it is the superior authority which bears full legal responsibility for its implementation. The absence of legal indications as to the scope of management and the means of its implementation could give rise to a presumption of unlimited action affecting a subsidiary authority. This perception is limited by virtue of the powers which only the law may confer on individual authorities. A managing authority does not have the right to withdraw or take over these powers, but can only determine the manner in which they are to be exercised.[7]

The Act on Government Administration Departments, by identifying public administration departments, also defined their scope of action. This indication is reiterated in the National Cybersecurity System Act, except that this specification points to the authorities competent for cybersecurity.[8] The following sectors and authorities were identified.

1. The energy sector—the Minister competent for energy.
2. The transport sector, excluding the water transport subsector—the Minister competent for transport.
3. The water transport subsector—the Minister competent for the maritime economy and the Minister competent for inland navigation.
4. The banking sector and financial-markets infrastructure sector—the Polish Financial Supervision Authority (KNF).
5. The healthcare sector—the Minister competent for health.
6. The healthcare sector[9]—the Minister for National Defence.
7. The drinking water supply and distribution sector—the Minister competent for water management.
8. The digital infrastructure sector—the Minister competent for computerisation.
9. The digital infrastructure sector—the Minister for National Defence.
10. For digital service providers—the Minister competent for computerisation.
11. For digital service providers—the Minister for National Defence.

Each of the entities indicated (apart from KNF) is a Minister managing a department of government administration, with a strictly defined material brief and position within the structure of public administration. It is not specified what is meant by the indicated responsibility of these authorities as authorities accountable

[7] Zimmermann (2016), p. 227.

[8] Article 41 of the NCSA.

[9] In points 5, 6, 8, 9, 10, 11, only in respect of the entities specified in Article 26(5) of the National Cybersecurity System Act. The tasks of the CSIRT MON include the coordination of handling incidents reported by: entities subordinate to or supervised by the Minister of National Defence, including entities whose communication and information systems or networks are covered by the uniform list of facilities, installations, devices, and services comprising the critical infrastructure referred to in Article 5b(7)(1) of the Act of 26 April 2007 on Crisis Management; enterprises of particular economic and defence importance in respect of whom the authority organising and supervising the performance of tasks for the defence of the state within the meaning of Article5 (3) of the Act of 23 August 2001 on the Organisation of Tasks for State Defence Performed by Enterprises (consolidated text, Polish Journal of Laws of 2020, item 1669) is the Minister for National Defence.

for cybersecurity. According to the theory of administrative law, it can be assumed that this is a material competence. Pursuant to Article 20 of the Code of Administrative Procedure (CAP)[10] the material competence of a public administration authority shall be defined by the regulations on the sphere of its activities. The legal provisions on the sphere of activities to which the National Cybersecurity System Act refers are provisions belonging to substantive administrative law, authorising or obligating public administration authorities to resolve individual matters cited in these provisions by way of decisions.[11]

According to the Constitution, Ministers manage specific departments of government administration, or carry out the tasks assigned to them by the Prime Minister.[12] Pursuant to Article 34(1) of the Act on Government Administration Departments, a Minister is obliged to initiate and prepare the policy of the Council of Ministers relating to the department which is headed by the Minister, as well as to submit draft laws and normative acts to the meetings of the Council of Ministers in this respect in accordance with the Rules of Procedure of the Council of Ministers. Within the department headed, the Minister implements the policy of the Council of Ministers and coordinates its implementation by the authorities, institutions, and organisational units subsidiary to or supervised by the Minister.[13] As part of their powers, any Minister heading an administrative department may issue regulations and orders. A regulation of a Minister, issued pursuant to Article 149(2) of the Constitution, as well as regulations of the Council of Ministers and the Prime Minister, is used as an act of management only in exceptional circumstances. Much more often such a role is played by an order of a Minister issued pursuant to Article 93(1) of the Constitution of the Republic of Poland. The difference between the orders of the Prime Minister and those of Ministers is that the binding force of the orders of the Prime Minister is greater than that of a Minister's, and that the scope of the potential addressees of the orders of a Minister is much narrower. It covers only those entities falling under the management of a given Minister, whereas orders of the Prime Minister could concern the entire government administration.[14]

The fact that the Polish Financial Supervision Authority (KNF) is included in the list of competent authorities indicated in the National Cybersecurity System Act requires clarification. Pursuant to Article 3 of the Act on Financial Supervision,[15] the Polish Financial Supervision Authority is the supervisory authority responsible for the capital market, and the market for financial instruments which are the subject of

[10]Act of 14 June 1960—the Code of Administrative Procedure, consolidated text, Polish Journal of Laws of 2020, item 256, as amended.

[11]Wróbel (2020b).

[12]Zimmermann (2016), p. 242.

[13]More on the political position of a Minister heading a department of government administration—Opaliński (2013), pp. 26–27.

[14]Góralczyk Jr (2016), pp. 126–132.

[15]Act of 29 July 2005 on Capital Market Supervision, Polish Journal of Laws of 2020, item 1400, consolidated text.

requests for admission to trading on the market.[16] The Chair of the KNF manages the operations of the KNF. There is no uniform view in the literature on the subject assessing the legal status of the KNF. As noted by L. Góra, some of the authors rank the KNF as a central-government administration authority, while others indicate that the KNF does not have the status of a government administration authority.[17] Also, the case law of the administrative courts remains inconsistent. The view that the Polish Financial Supervision Authority has the status of a state administration authority prevails, although

> the Act does not explicitly state that the Polish Financial Supervision Authority is a central authority (headed by a Minister within the meaning of the provisions of the CAP), such a conclusion should be drawn from a comprehensive analysis of the provisions of the Act on Financial Supervision.

At the same time, the Supreme Administrative Court noted

> no other state authority has been designated which would be responsible for matters falling within the scope of the Polish Financial Supervision Authority, and, in particular, no other authority has been designated which would be a higher-instance authority, superior to the Polish Financial Supervision Authority, with a power to decide on the validity of KNF's decisions.[18]

The legal assessment of the KNF in the literature has been significantly influenced by the judgment of the Constitutional Tribunal, in which it stated that

> the specific links with other state authorities resulting from the legal provisions which could determine whether that authority is subject to the jurisdiction of the Council of Ministers, the Prime Minister, or a responsible Minister heading a department of government administration, are essential for determining the position of the Polish Financial Supervision Authority within the structure of state authorities[19].

According to the analysis made by the Tribunal as regards the statutory tasks of the KNF, and of the legal forms of action the KNF may use, it can be concluded that the authority is part of the executive. The Constitutional Tribunal noted

> in the light of the provisions of the Constitution, the Act on Financial Market Supervision, and other Acts, it should be stated that the Polish Financial Supervision Authority is a special public state-administration authority, but located outside the government administration structure.[20]

In the case of the KNF, with the existence of certain statutory links, the status of the KNF is characterised by a considerable degree of autonomy and independence, greater than that of the regulatory authorities defined by law as central-government administration authorities.[21] The argument by P. Wajda that the Polish Financial

[16] Article 3(1) of the Act on Capital Market Supervision.

[17] Góral (2012).

[18] The Supreme Administrative Court in its judgment of 21 February 2012, II GSK 67/11.

[19] The judgment of the Constitutional Tribunal of 15 June 2001, K 2/09, OTK-A 2011/5/42.

[20] The judgment of the Constitutional Tribunal of 15 June 2001, K 2/09, OTK-A 2011/5/42.

[21] Góral (2012).

Supervision Authority, due to its appointment to perform the tasks of public administration specified in legal acts, within its territorial responsibility covering the whole country, should be included in a collective group of administrative entities, which form the so-called central administration, may be accepted. Within this broad category, the KNF, due to the fact that it has not been granted the position of supreme authority, should be classified in a subcategory of central offices.[22] It should also be emphasised that to decisions by the *Polish Financial Supervision Authority* on the basis of Article 11(6) of the Act on Financial Market Supervision, Article 127§3 of the CAP should be applied accordingly, which results in the KNF's being considered a Minister within the meaning of Article 5§2(4) of the CAP, as such a legal measure is available in respect of decisions by a Minister or a local government appeal court issued in the first instance.[23]

In the Cybersecurity System Act, the legislators have created a list of tasks for cybersecurity authorities.[24] This fragmented list can be divided into several aspects of the operation of the authorities.

The first of these concerns the situation in which a Minister, as a public administration authority, conducts administrative proceedings in accordance with the CAP, and issues administrative decisions on recognising an entity as an operator of essential services, or decisions stating that rulings on recognising entities as operators of essential services have expired.

The second group comprises the authorities' powers to supervise and monitor the activities of the operators of essential services.

The third group entails the authorities' tasks regarding the formulation of conclusions and recommendations.

The next group of actions includes cooperation with EU bodies.

The last group comprises the powers to process information, including personal data, concerning the provision of essential and digital services, and operators of essential services or digital service providers.

While analysing the separate first group of tasks, it should be noted that each designated authority may conduct administrative proceedings in the field of the recognition of an entity as an operator of essential services. According to Article 1 (1) of the CAP, proceedings before public administration authorities in individual cases falling within the responsibility of these bodies shall be settled by means of administrative decisions, or settled tacitly. A legal definition of an administrative authority classifies, in Article 5§2 of the CAP, a Minister as a public-administration authority within the meaning of the CAP. Pursuant to the provisions of the National Cybersecurity System Act, the authority carries out an ongoing analysis of entities in a given sector or subsector, in terms of their recognition as an operator of essential services, or failure to meet the conditions classifying an entity as an operator of

[22]Wajda (2009), p. 139.

[23]Chrościelewski (2015), p. 13.

[24]More on the public administration authorities responsible for cybersecurity in Chałubińska-Jentkiewicz (2019), pp. 360–375.

essential services, and issues decisions on the recognition of an entity as an operator of essential services, or decisions stating that the ruling on recognising an entity as an operator of essential services has expired. Such an indication precludes tacit decisions. The authority carrying out the aforementioned analysis conducts administrative proceedings, as evidenced by the fact that the proceedings are terminated with the issue of an administrative decision. When applying the CAP to the issue of this decision, the operators of essential services become parties to the proceedings, using all the statutory rights of such parties. A Minister as a public-administration authority issues a decision, and, pursuant to Article 127§3 of the CAP, no appeal may be brought against this decision.[25] However, any party dissatisfied with the decision may ask the authority to re-examine the case, and the regulations regarding appeals against decisions apply in such a case. A request for re-examination of the case as regards a first-instance decision issued by a Minister is treated in the literature on the subject as a form of a standard appeal, although it serves as a final decision. A request for the re-examination of a case differs from an appeal in that it does not have a devolutive effect, i.e. it does not refer the case to a higher authority.[26] It should be noted that a request for the re-examination of a case will also be admissible when specific provisions introduce the possibility of bringing an action before a court in respect of a particular type of decision.[27]

Immediately after issuing a decision on recognising an operator of essential services, or a ruling stating the expiry of a decision on recognising an operator of essential services, the competent authority forwards requests to the Minister competent for digital affairs for inclusion in the list of operators of essential services, or removal from that list.[28]

It was further stated that authorities competent for cybersecurity should monitor the application of the provisions of the Act by operators of essential services, and digital service providers.[29] The use of the verb "monitor" ("monitoruje") by the legislators creates some ambiguity in its interpretation. The use of this term results from a direct translation of the terminology of the NIS Directive. It would be more appropriate to use the term "nadzór" ("supervision"). This provision would then correlate with the next task, namely that the competent authority, at the request of CSIRT NASK, CSIRT GOV, or CSIRT MON, calls on the operators of essential services or digital service providers to remove, within a specified time frame, the vulnerabilities which have led or could lead to a serious, significant, or critical

[25] According to B. Adamiak, an appeal against a decision is one of the legal remedies, which should be understood as "procedural institutions standardize which authorised entities may request the verification of administrative decisions with a view to their cassation or amendment". Adamiak (1996), p. 544. For more information on a request for re-examination of the case, cf. Piszczek and Piszczek (2008), pp. 62–77.

[26] Wróbel (2020a). More on the devolutive effect of a request for the re-examination of the Z. Kmieciak case, Kmieciak (2008), pp. 19–35.

[27] Przybysz (2019).

[28] Article 42(1) (3) of the NCSA.

[29] Article 42(1) (6) of the NCSA.

incident.[30] The literature indicates that supervision occurs in a centralised and decentralised authority structure. The concept of supervision is connected with subsidiarity, in which a supervisory authority has overseeing powers, and the essence of supervision is the ability to draw consequences from the behaviour of a subsidiary authority, observed by the supervisory authority from the point of view of a specific, selected criterion.[31] The literal use of the concept of supervision in this form is justified in the later part of the list of tasks assigned to the authorities compe for cybersecurity, in which the authorities submit requests for a change to the data in the list of operators of essential services, no later than 6 months after the change of such data, and monitor the application of the provisions of the Act by the operators of essential services and digital service providers.[32] In Chapter 11 of the Act, the Polish legislators indicated the principles and manner of exercising supervision over the operators of essential services and digital service providers.

The concept of supervision is connected with the notion of control. Control should be understood as the examination of the compliance of the existing state with the requested state, the determination of the scope and causes of discrepancies, the communication of the results of this determination, and sometimes the resulting instructions to both the controlled entity and the superior entity.[33] Control is a basic element of supervision, and also an element of management. According to J. Zimmermann, supervision is, precisely, control carried out within the administrative system, enhanced by an element of administrative power, which makes it possible to derive consequences from the deficiencies in the activities of an administrative authority or other entity identified during the control. This means that control occurs as a stage in the supervisory procedure, or as a stage in the management procedure, and can occur as independent control.[34] The legislators specified in Article 42(1)(8) that the authorities carry out the control of the operators of essential services and digital service providers. In accordance with Article 15(1) of the NIS Directive, Member States shall ensure that the competent authorities have the necessary powers and means to assess the compliance of the operators of essential services with their obligations. Article 17(1) of the NIS Directive stipulates that Member States shall ensure that the competent authorities take action, if necessary, through *ex post* supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in Article 16. Such evidence may be submitted by a competent authority of another Member State in

[30]Article 42(1) (7) of the NCSA.

[31]Zimmermann (2016), p. 228. The most common supervision measures used include legality, i.e. compliance with the law, expediency, cost-effectiveness, reliability, and validity. These are repressive supervision measures. Preventive supervision, carried out before the supervised authority takes action, i.e. agreement or opinion on an act. Zimmermann (2016), p. 228.

[32]Article 42(1) (4) of the NCSA.

[33]Boć (2003), p. 327.

[34]Zimmermann (2016), p. 229.

which the service is being provided.[35] The detailed scope of control is set out in Chapter 11 of the National Cybersecurity System Act.

The competent authorities, using their powers, in cooperation with CSIRT NASK, CSIRT GOV, CSIRT MON, and sectoral cybersecurity teams, prepare recommendations for action to strengthen cybersecurity, including sector-specific guidelines on incident reporting.[36] Recommendations for action to strengthen cybersecurity, including sector-specific guidelines on incident reporting, referred to in paragraph 1(5), are prepared, taking into account, in particular, Polish standards transposing European standards, common technical specifications, understood as ICT technical specifications defined in accordance with Articles 13 and 14 of the Regulation of the European Parliament and of the Council (EU).[37]

As part of their powers, the competent authorities may cooperate with the authorities of the Member States of the European Union, and a Single Point of Contact.[38] As a general rule, cooperation between authorities should take place through a single point of contact. However, it cannot be excluded that a Polish competent authority might establish direct contact with its counterpart in another Member State. A Single Point of Contact should, however, be informed of such cooperation on a case-by-case basis, so that it is fully informed of the consultations which are taking place, and which will facilitate the proper coordination of activities.[39]

When a legal person or an organisational unit without legal personality providing digital services does not have its registered office or management board on the territory of the Republic of Poland, or has not appointed a representative on the territory of the Republic of Poland, but its information systems are located on the territory of the Republic of Poland and does not comply with the requirements set out in Implementing Regulation 2018/151, the authority competent for cybersecurity for digital service providers may transmit information and request action to the competent authority in another Member State of the European Union on the territory in which it has its registered office or management board, or has appointed a representative.[40]

The legislators have allowed the authorities competent for cybersecurity to delegate their tasks. This means that the authority may entrust the performance, on

[35]Prusak-Górniak and Silicki (2019a).

[36]Article 42(1)(5) of the NCSA.

[37]Articles 13 and 14 of Regulation (EU) No. 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC, and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No. 1673/2006/EC of the European Parliament. and of the Council (OJ EU 2012 L 316/12). and the guidelines of the European Commission and the European Network and the Information Security Agency (ENISA).

[38]Article 42(1)(9) of the NCSA.

[39]Prusak-Górniak and Silicki (2019b).

[40]Article 42(2) of the NCSA.

its behalf, of certain tasks to entities which are subsidiary to, or supervised by, the authority.[41] Tasks are entrusted on the basis of an agreement between the competent authority for cybersecurity and the entities. This agreement sets out the rules for the exercise of control by the competent authority for cybersecurity over the proper performance of the tasks entrusted. The communication on the conclusion of the agreement is published in the official journal of the competent authority for cybersecurity. The Act specifies what information such a communication should contain.[42]

Each competent authority processes information, including personal data concerning the provision of key and digital services and digital service operators or providers, to the extent necessary to carry out its statutory tasks. The right to process information, including personal data, should be derived from provisions indicating the specific tasks for which such processing is required. As noted by K. Prusak-Górniak and K. Silicki, the processing of information may take place only to the extent justified by the performance of a specific task, hence it seems excessive to include provisions indicating the general right to process information, including personal data.[43]

The legislators have provided the possibility of requesting information by creating a simplified procedure.[44] As a result, the authority competent for cybersecurity may, without initiating proceedings for recognising an entity as an operator of essential services, request information to enable a preliminary assessment of whether the entity meets the conditions to be recognised as an operator of essential services.[45] The same applies to procedures to carry out an inspection. The competent authority may, without initiating an inspection, request information from an operator of essential services which will make it possible to determine the need for an inspection, and may, without initiating proceedings, request information from an operator of essential services which will make it possible to make a preliminary assessment of whether the entity no longer meets the conditions to be recognised as an operator of essential services.[46]

The authority competent for cybersecurity, when making a request for information to the appropriate entity or operator of essential services, indicates when the information is to be provided. The deadline set may not be less than 14 days from the date of the receipt of the request by the entity or the operator of essential services.[47] The competent authority addresses the entity in the form of a simple letter containing

[41] Article 42(3) of the NCSA.

[42] Article 42(4)-(6) of the NCSA. The information refers to the address of the website on which the agreement will be published, together with its integral annexes, and the date from which the agreement will be effective.

[43] Prusak-Górniak and Silicki (2019a).

[44] Walczuk (2019), pp. 274–275.

[45] Article 43(1) of the NCSA.

[46] Article 43(2) of the NCSA.

[47] Article 43(3) of the NCSA.

questions which will allow a preliminary assessment of the legitimacy of initiating a formal procedure based on the provisions of the Code of Administrative Procedure.[48] The entity requested by the authorities may provide information on the matter to which the request relates, or decline to provide information.[49] A request for information followed by the failure to provide information does not affect the possibility of initiating administrative proceedings or inspections, but might constitute evidence in administrative proceedings or inspections initiated. The failure to provide information does not affect the procedural situation of the party or the inspected entity, nor does it affect the administrative proceedings or inspection initiated.[50]

The National Cybersecurity System Act also indicates the possibility of the competent authority's creating a sectoral cybersecurity team for specific sectors or subsectors. Such a team is responsible, in particular, for receiving reports of serious incidents and assisting in the handling of those incidents, supporting the operators of essential services in carrying out their duties, analysing serious incidents, finding links between incidents, preparing conclusions of incident handling, and cooperating with the appropriate CSIRT MON, CSIRT NASK, or CSIRT GOV in coordinating the handling of serious incidents.[51] It should be noted, as did K. Walczuk, that the tasks mentioned above do not form an exhaustive list; on the contrary—they rather constitute a sample task list.[52]

A sectoral cybersecurity team may transmit to, and receive from, other states, including Member States of the European Union, information on serious incidents, including those involving two or more Member States of the European Union. A sectoral cybersecurity team may receive reports of a serious incident from another Member State of the European Union involving two or more Member States of the European Union. A sectoral cybersecurity team forwards these reports to the appropriate CSIRT MON, CSIRT NASK, or CSIRT GOV, and a Single Point of Contact.[53] When a sectoral cybersecurity team is established, the authority competent for cybersecurity informs the operators of essential services in the appropriate sector, and CSIRT MON, CSIRT NASK, and CSIRT GOV, of the establishment of that team, and the scope of the tasks carried out.[54] Sectoral cybersecurity teams may operate in addition to CSIRTs which are mandatory at the national level.[55]

The legislators have defined the responsibility of the authorities in a fairly short and general chapter, while at the same time providing the opportunity to extend this responsibility in the other chapters discussed in this publication. The indicated list of

[48]Prusak-Górniak and Silicki (2019a).
[49]Article 43(4) of the NCSA.
[50]Article 43(6) of the NCSA.
[51]Article 44(1) of the NCSA.
[52]Walczuk (2019).
[53]Article 44(2) and (3) of the NCSA.
[54]Article 44(4) of the NCSA.
[55]Walczuk (2019).

tasks of the authorities competent for cybersecurity is limited to mentioning the individual tasks of these authorities. Public-administration authorities use their own authoritative forms of action to perform their tasks. What is important is that in the case of doubts as to the legitimacy of initiating proceedings, the competent authorities may use the measure provided for in Article 43 of the National Cybersecurity System Act to request information, without the need to formally initiate the procedure. It is also worth noting that the competent authorities, with regard to Article 8 (6) of the NIS Directive, consult and cooperate with the appropriate national law enforcement authorities and national data protection authorities. However, it should be stressed that the statutory assumptions will only be verified as time goes by. The presentation of the activities of the authorities competent for cybersecurity as outlined above follows from the recommendations set out in the NIS Directive, and from political considerations and consultations. It is intended to provide for the possibility of applying these provisions to the widest possible extent, but the period which has elapsed since the adoption of the Act (2 years) does not yet enable a full assessment of their application in practice. What remains is the practice of the authorities, which might resolve a number of interpretation doubts.

## References

Adamiak B (1996) Komentarz do Kodeksu postępowania administracyjnego, Warsaw

Boć J (2003) Administracja publiczna, Wrocław

Chałubińska-Jentkiewicz K (2019) Cyberodpowiedzialność, Toruń

Chrościelewski W (2015) Postępowanie administracyjne – Komisja Nadzoru Finansowego – wyłączenie od udziału w sprawie. Glosa to the Judgment of the Polish Supreme Administrative Court (NSA) of 29 April 2014 r., II GSK 320/13 – a partly critical gloss

Czarny P (2019) Commentary on Article 149 Konstytucji RP. In: Tuleja P (ed) Konstytucja Rzeczypospolitej Polskiej. Komentarz, Wolters Kluwer, Warsaw, LEX/el

Góral L (2012) Commentary on Article 3 w: Ustawa o nadzorze nad rynkiem finansowym. Komentarz, LEX/el

Góralczyk W Jr (2016) Kierownictwo w prawie administracyjnym, Warsaw

Kmieciak Z (2008) Wniosek o ponowne rozpatrzenie sprawy w KPA (Odwołanie czy remonstracja?), Państwo i Prawo 3

Opaliński B (2013) Prawnoustrojowe uwarunkowania struktury Rady Ministrów, Przegląd Legislacyjny 1

Piszczek K, Piszczek P (2008) Wniosek o ponowne rozpatrzenie sprawy – kontrowersje wokół jego istoty. Prokuratura i Prawo 11

Prusak-Górniak K, Silicki K (2019a) Commentary on Article 42. In: Czaplicki K, Gryszczyńska A, Szpor G (eds) Ustawa o Krajowym Systemie cyberbezpieczeństwa. Komentarz, Warsaw, LEX/el

Prusak-Górniak K, Silicki K (2019b) Commentary on Article 26. In: Czaplicki K, Gryszczyńska A, Szpor G (eds) Ustawa o Krajowym Systemie cyberbezpieczeństwa. Komentarz, Warsaw, LEX/el

Przybysz P (2019) Commentary on Article 127. In: Przybysz P (ed) Komentarz do kodeksu postępowania administracyjnego, Komentarz aktualizowany, LEX/el

Wajda P (2009) Pozycja prawnoustrojowa i skład Komisji Nadzoru Finansowego – kilka uwag krytycznych, Przegląd Prawa Publicznego 7–8

Walczuk K (2019) Commentary on Article 43. In: Kitler W, Taczkowska-Olszewska J, Radoniewicz F (eds) Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Warsaw
Wróbel A (2020a). Komentarz do art. 20 KPA. In: Jaśkowska M, Wilbrandt-Gotowicz M,Wróbel A (eds) Komentarz zaktualizowany do Kodeksu postępowania administracyjnego, Warsaw, LEX/el
Wróbel A (2020b). Komentarz do art. 127 KPA. In: Jaśkowska M, Wilbrandt-Gotowicz M,Wróbel A (eds) Komentarz zaktualizowany do Kodeksu postępowania administracyjnego, Warsaw, LEX/el
Zimmermann J (2016) Prawo administracyjne, Warsaw

**Agnieszka Brzostek** PhD, adjunct at the Institute of Law of the War Studies Academy. She is a lecturer of law and administrative procedure at studies in the field of law and administration. Scientific interests focus on administrative law and administrative procedure, as well as on the functioning of public administration, in particular on the activities of public administration bodies in the field of security and cybersecurity. Scientific interests focus on administrative law and administrative proceedings, as well as on the operation of public administration, in particular on the operation of public administration bodies in the field of security and cyber security. She is the author or co-author of numerous chapters in monographs and scientific articles.