# Procedure for the Identification of an Operator of Essential Services under the Act on the National Cybersecurity System

DOROTA LEBOWA

**Abstract** The Polish Act on the National Cybersecurity System defines cybersecurity as "the resistance of information systems to activities that violate the confidentiality, integrity, availability and authenticity of the data processed or related services offered by these systems". The Act is designed to ensure an adequate level of protection for users of digital services, and one of the basic measures to achieve this is to impose numerous obligations on digital service operators. The Act on the National Cybersecurity System sets out a procedure for identifying an entity as providing essential services. Recognition of a specific entity as an operator of essential services takes place through a formalized procedure with specific guarantees, concluded with an administrative decision. The provisions of the Polish Code of Administrative Procedure apply to the procedure for identifying an operator of essential services.

**Keywords:** • cybersecurity • operator of essential services • administrative decision • essential service

CORRESPONDENCE ADDRESS: Dorota Lebowa, Ph.D., Assistant Professor, Maria Curie-Sklodowska University, Faculty of Law and Administration, Department of Administrative Law and Administrative Sciences, Plac Marii Curie-Sklodowskiej 5, 20-031 Lublin, Poland, e-mail: dorota.lebowa@mail.umcs.pl, ORCID: 0000-0003-3316-5541.

https://doi.org/10.4335/2022.1.10 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

## 1 Introduction

The ever-growing influence of information and communication technology (ICT) on the socio-economic development of the Member States of the European Union and the increased use of ICT results in the products and services offered being increasingly dependent on cybersecurity (Karpiuk, 2021a: 611). The extensive architecture of ICT systems, including big data operations, serves the development of communication, trade and transport, and provides a foundation for rendering essential, digital and public administration services. Unfortunately, the opportunities offered by modern digital technologies are also used for unfair competition practices, to interrupt the continuity of selected services (whether for hooliganism purposes or to undermine the competitive position of an entity), to commit crimes using the Internet, or to carry out terrorist activities (explanatory memorandum to the government-proposed draft Act on the National Cybersecurity System, Sejm Papers no. 2505).

The Act of 5 July 2018 on the National Cybersecurity System (consolidated text: Journal of Laws of 2020, item 1369), hereinafter referred to as ANCS, implements Directive 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. Pursuant to the principles of the so-called pro-EU interpretation of national law (see, for example, the CJEU judgment of 9 March 2004, in joined cases C 397/01 to C 403/-1, Pfeiffer, 2004, p. I-8835, paragraph 113), it is right and necessary to refer to the relevant provisions of the Directive when interpreting individual norms of the ANCS. Important guidelines on how to understand the objectives of the Directive are provided in its preamble, which points out that networks and information systems and services play an important role in society. Their reliability and security are essential for economic and social activities and especially for the functioning of the internal market. The scale, frequency and impact of security incidents are larger and larger and pose a serious threat to the functioning of networks and information systems (Hydzik, 2019: 84-87).

The definition of operator of essential services is contained in Article 4(4) and Article 5(2) of the NIS (Network and Information Security) Directive 2016/1148 of 6 July 2016, according to which ‘operator of essential services’ means a public or private entity of a type referred to in Annex II, which provides a service which is essential for the maintenance of critical societal and/or economic activities; the provision of that service depends on network and information systems; and an incident would have significant disruptive effects on the provision of that service (Karpiuk, 2021b: 238).

The *ratio legis* behind the ANCS is to protect users of digital services in a broad sense from negative exposure to risks associated with the lack of an adequate degree of cybersecurity (Wajda, 2020: 5). The correct implementation by operators of essential services of the obligations imposed on them by the Act should, as planned by the lawmakers, translate into an appropriate degree of protection in the space of digital

services. These obligations comprise a very broad and complex range of activities concerning, among other things, the obligation to implement systemic solutions for managing security in the information system, the obligation to designate appropriate structures responsible for cybersecurity, information obligations (in relation to users and relevant authorities), obligations to implement appropriate procedures in the area of cybersecurity, including in the area of incident response, and the obligation to conduct audits in the area of cybersecurity (Chałubińska-Jentkiewicz, Karpiuk & Kostrubiec, 2021: 16). The implementation of these obligations is secured by the mechanism provided for in the ANCS for the supervision of their implementation, as well as administrative liability, i.e. the power to impose administrative penalties by competent authorities.

To sum up, it can be stated that the legislature has set very strict requirements for operators of essential services, which may entail the need to rebuild the company structure and a new division of powers and responsibilities in order to ensure an appropriate degree of cybersecurity (Sawicki, 2019: 13-20). Hence, the procedure established in the ANCS for identifying an entity as a provider of essential service is so important.

## 2 Procedure for the identification of operator of essential service

Recognition of a specific entity as an operator of essential services takes place through a formalized procedure with specific guarantees, concluded with an administrative decision. The procedure for identifying an operator of essential services is generally governed in Poland by the provisions of the Act of 14 June 1960 the Code of Administrative Procedure (consolidated text: Journal of Laws of 2021, item 735, as amended), hereinafter referred to as CAP. The Act on the National Cybersecurity System does not contain a direct reference to the provisions of the CAP. It seems that such a reference is not necessary in the light of the principles of correct lawmaking, On the other hand, the application of the provisions of the CAP is indicated by the reference to the detailed regulation concerning the time limits for settling administrative matters contained in Article 5(5) ANCS (the period for consultation referred to in paragraph 4 shall not be included in the time limits referred to in Article 35 of the Act of 14 June 1960 - Code of Administrative Procedure). Moreover, the requirements for the application of the provisions of the CAP on jurisdictional proceedings set out in Article 1(1) CAP (the Code of Administrative Procedure governs proceedings before public administration bodies in individual matters falling within the jurisdiction of these bodies, resolved through administrative decisions or settled on a tacit basis) must be met, and proceedings in this matter have also not been explicitly excluded from the application of the Code in Articles 3 and 4 CAP or in specific provisions of the Code.

The Act provides for a specific procedure for the competent authority to determine whether the entity concerned meets the conditions to be considered an operator of essential services. The authority may request a specific entity to provide information allowing for a preliminary assessment of whether the entity meets the conditions to be

considered as an operator of essential service (Article 43ANCS). Such a solution stems from a very large number of entities that need to be verified. The procedure is deformalised and shall take place without initiating administrative proceedings. This is an exception to the fundamental principle of administrative law, namely the running of jurisdictional proceedings to concretise the legal norm and to determine the rights and obligations of supervised entities. Such a basic procedure in the Polish legal system is the administrative procedure carried out on the basis of the Code of Administrative Procedure. The competent authority requests the entity by way of a simple official letter containing the questions which will allow an initial assessment whether it would be appropriate to initiate the formal procedure. The request should specify a time limit to provide the requested information, which must not be less than 14 days. The addressee of the letter is not obliged to provide information. However, it should be pointed out that the entity concerned may be interested in providing that information to avoid the initiation of an administrative procedure, if the preliminary proceeding demonstrates that the statutory conditions for considering the entity as an operator of essential service are not met. The information provided by the entity will be able to be used as evidence in future administrative proceedings.

As a rule, the administrative procedure for identification is initiated *ex officio*. However, the provisions of the Code of Administrative Procedure do not prevent another authority whose competence includes cybersecurity issues from drawing the competent authority's attention to the need to initiate such proceedings. As part of its business, an important piece of information for the entity running such business is the possibility of excluding it from the requirements of the ANCS. It is therefore possible that an entity not recognised as an operator of essential services may apply for such proceedings. The ANCS also does not exclude the possibility of initiating such proceedings at the request of an NGO or allowing this organization to participate in ongoing proceedings with the rights of a party, if it is justified by the statutory objectives of this organization and if there is a public interest in doing so (Article 31 §1(1) CAP).

The public administration body is not obliged to issue a separate decision on the initiation of proceedings. The initiation of proceedings *ex officio* entails, in the light of Article 61 § 4 CAP, the obligation to notify all the parties of this initiation. The case-law stresses that the notification of the initiation of proceedings served to a party is not a value in itself, but has a specific purpose, namely primarily to inform the parties that an administrative procedure has begun in which they may need to defend their rights (Judgment of the Supreme Administrative Court of 18 April 2008, case ref. no. II OSK 429/07, LEX no. 469206). On the other hand, when a party is served the notice of initiation of proceedings, the Code requirements for the public administration body to conduct proceedings under and within the limits of law are applicable, taking into account the constitutional principles and general administrative procedural principles.

The Act does not provide for a time limit to conclude the administrative procedure for the adoption of an identification decision. Therefore, in this respect, reference should be made to the time limits contained in the CAP. The handling of a case requiring clarification proceeding should take place no later than one month and for a particularly complex case no later than two months after the initiation of the proceedings (Article 35 § 3 CAP).

The procedure for identifying an operator of essential services may be concluded with a decision to recognise it an operator of essential services only if the competent authority has determined that the entity meets the conditions for obtaining this status (of a systemic and substantive nature). If, on the other hand, following clarification proceeding, the authority finds that the conditions for considering an entity to be an operator of essential services are not met, the procedure should also end with an administrative decision. The provisions of the ANCS do not contain a separate regulation in this matter, so the authority in such a situation should issue a decision to discontinue the proceedings pursuant to Article 105 § 1 CAP.

According to Article 7 CAP, in the course of the proceedings, public authorities must safeguard the rule of law, take all necessary steps, either *ex officio* or at the request of the parties, to examine the facts thoroughly and to settle the case having regard to the public interest and the legitimate interests of citizens. This provision expresses the principle of objective truth, according to which a public authority is required to study thoroughly all the facts in order to examine the case correctly, which is a necessary element in the proper application of a norm of substantive law. This principle is mainly guaranteed by the rules governing evidence taking. The authority is required to collect thorough evidence and therefore to take a series of procedural steps to gather and consider all the evidence (Article 77 § 1 CAP). In the course of the proceedings, it is also necessary to take account of the principle of active participation of the parties in the proceedings by providing the parties with access to the file of the case and by notifying them of the opportunity to comment on the evidence collected and the service of the decision.

## 3 Conditions for considering an entity as an operator of essential services

The following entities shall be deemed operators of essential services: 1) those which are listed in the annex to the ANCS and have an organisational unit in the territory of the Republic of Poland; 2) which provide an essential service specified in the list of essential services; 3) the provision of this service depends on information systems; 4) an incident would have a significant disruptive effect on the provision of the essential service by this operator (Article 5(1) and (2) ANCS).

Specific categories of entities are described in the annex to the ANCS to indicate potential entities for which a decision to recognise them as operators of essential services may be issued now or in the future, but this does not mean that such an entity will be automatically

recognised as an operator of essential services. Essential service within the meaning of Article 2(16) of the Act under is a service which is of key importance for maintaining a critical social or economic activity, specified in the list of essential services. The list is contained in the Ordinance of the Council of Ministers of 11 September 2018 on the list of essential services and the thresholds of significance of the disruptive effect of an incident on the provision of essential services (Journal of Laws of 2018, item 1806). For an entity to be qualified as an operator of essential service, it is necessary that the provision of the essential service is dependent on information systems. Information system is defined in Article 2(14) ANCS as an ICT system referred to in Article 3(3) of the Act of 17 February 2005 on computerisation of the activities of public task-performing entities (consolidated text Journal of Laws of 2021, item 670) together with data in electronic form processed in it. The case law points out that information system is a set of cooperating IT devices and software ensuring the data processing (including storage, as well as sending and receiving) by telecommunication networks by means of a telecommunications device appropriate for a given type of network and designed to be connected directly or indirectly to network terminals, together with the data processed in it in electronic form (Judgment of the Regional Administrative Court of 5 August 2020, VI SA/Wa 2667/19, LEX No. 3068097). In general, therefore, the dependence of the provision of an essential service on information systems should be referred to such circumstances in which the use of information systems is necessary for the continuous and effective provision of the service in question.

The last condition for an entity to be considered an operator of essential services is related to the fact that a cybersecurity incident, if any, has a significant disruptive effect on the provision of the essential service by the entity. Cybersecurity is understood as the resistance of information systems to activities that compromise the confidentiality, integrity, availability and authenticity of the data processed or related services offered by these systems (Article 2 (4) ANCS). According to Article 2(5) ANCS, incident is an event that has or may have an adverse impact on cybersecurity. It is not sufficient for an entity to provide an essential service in a manner that is dependent on information systems, but it is further required that a possible incident affects (or could affect) the confidentiality, integrity, availability and authenticity of the data processed for the provision of the service or affects the provision of that service (e.g. interferes with its proper provision or even prevents its performance).

What is legally relevant is not any impact of an incident on the provision of a service, but rather causing an effect of a material nature that disrupts the provision of this service by a given operator, e.g. one that affects continuity of provision of the service, quality of the service, security of users, protection of users' data, etc. The degree of significance of the incident is of a highly arbitrary nature. Possible effects of such an incident may depend on many variables, such as the scale of provision of a given type of service, or the scale of impact of the incident on economic or social activity. That is why it was necessary to establish thresholds of significance of the disruptive effect, on the basis of which the

competent authorities assess, in the course of the procedures for identification of operators of essential services, the significance of the disruptive effect for a given service provided by a particular operator. These thresholds are set out in the aforementioned Ordinance of the Council of Ministers of 11 September 2018 on the list of essential services and the thresholds of significance of the disruptive effect of an incident on the provision of essential services.

The disruptive effect significance thresholds are set out in the Annex to the Ordinance for each essential service sector. In general, these thresholds correspond to the cross-sectoral factors set out in the provisions of 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. As follows from Article 6(1) of the Directive, when determining the significance of a disruptive effect, Member States must take into account at least the following cross-sectoral factors: 1) the number of users relying on the service provided by the entity concerned; 2) the dependency of other sectors referred to in Annex II on the service provided by that entity; 3) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; 4) the market share of that entity; 5) the geographic spread with regard to the area that could be affected by an incident; 6) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

## 4 Decision on recognising an entity as an operator of essential service

The recognition as an operator of essential service is to be done by way of an administrative decision. Administrative decision means a specific administrative act, which is a manifestation of the will of public authorities administering the State, issued under generally applicable administrative law of a sovereign and external nature, resolving a specific case of a specific natural or legal person, in proceedings governed by procedural rules (Judgment of the Supreme Court of 3 April 2000, I CKN 582/98, LEX No. 50843; Zdyb, Stelmasiak 2020: 220-224). The constituent elements of administrative decision are listed in Article 107 CAP. This provision obliges the authority to clarify all relevant factual and legal circumstances and to explain to the party the reasons behind the decision on handling the party's request. The statement of reasons for the decision must be drafted in such a way as to make it possible to understand the body’s reasoning and to review correctness of the decision. A precondition for the recognition as an operator of essential services is that all the above-mentioned conditions must be met cumulatively, which should be reflected in the factual and legal substantiation for the decision. The legal basis for the decision in question should be the following provisions: Article 5 1 ANCS (systemic condition), Article 5 (2) ANCS (substantive condition) and Article 41(1) and Article 42 (1) item 2 ANCS (competent authority).

Factual findings should concern all the conditions for the recognition as an operator of essential service. The competent authority may not confine itself to identifying the evidence gathered in the case and referring to the content of the provisions applicable to the case. It is also necessary to establish and demonstrate a link between various conditions, in particular regarding the provision of a particular service, with the fact that it depends on the functioning of the information system, or to analyse the significance of the disruptive effect.

As a rule, a decision must not be enforced before the time limit for lodging an appeal against it, and lodging an appeal suspends its enforcement. However, the legislation provides for quite numerous exceptions to this rule. This is because a decision may be subject to the obligation of immediate enforceability by virtue of law or where the requirement of immediate enforceability is conferred on it by a public administration body pursuant to Article 108 CAP. "The state of immediate enforceability of a decision" consists in the possibility of immediate enforceability of the decision, which becomes an enforcement order, despite being not final (judgment of the Supreme Administrative Court of 7 December 2018, I OSK 3311/18, LEX No. 2628876). Article 5 (7) ANCS indicates that the decision on recognition of an entity as an operator of essential services is subject to immediate enforcement. Contrary to the literal wording of the Act, it should be assumed that the decision is not immediately enforceable by operation of law, but the competent authority is obliged to declare *ex officio* the decision on recognition as an operator of essential service immediately enforceable (Besiekierska, 2019). However, the immediate enforceability of a decision does not mean that the obligations imposed by the Act on the operator are promptly applicable. The individual obligations imposed by the law are to be fulfilled by the operator within the time limits set out in Article 16 ANCS: from 3 months to a year from the date of service of the decision. The essence of this solution is to oblige operators of essential services to undertake performing the obligations imposed by the ANCS as soon as possible (Wajda, 2020: 9). It is the right solution from the point of view of clients of these services since the operator, regardless of filing the appeal to the administrative court, will be required to ensure the provision of services with an appropriate degree of cybersecurity.

An entity recognised in the decision as an operator of essential services may appeal against the decision to an administrative court. A party dissatisfied with the decision of the body may also exercise the right provided for in Article 127 § 3 CAP, according to which a decision issued in the first instance by the Minister may not be appealed against, but a party dissatisfied with the decision may apply to this body for reconsideration of the case; the provisions on appeals against decisions shall apply accordingly to such an application. The relevant case law indicates that in the proceedings for reconsideration of the case, similarly as in appeal proceedings, the administrative body is obliged to reconsider the case in its entirety, including in particular to respond to the allegations and arguments contained in the request for reconsideration (judgment of the Supreme Administrative Court of 19 March 2019, II OSK 1132/17, LEX No. 2655883). In the

ANCS, the legislature also regulated a situation similar to the regulation contained in Article 162 CAP, i.e. declaring a decision expired due to its groundlessness. In relation to an entity which no longer meets the conditions for being recognised as an operator of essential services, the competent authority for cybersecurity makes a decision stating that the decision on recognition as an operator of essential services has expired (Article 5(6) ANCS). The proceedings in this matter may be initiated *ex officio*, but in practice this is most often done at the request of an interested entity.

## 5 Conclusion

The cybersecurity obligations contained in the Act on the National Cybersecurity System concern, *inter alia*, the implementation of an effective security management system, including risk management, procedures and mechanisms for reporting and handling incidents or organisation of structures at operator level. However, the annex to the Act lists potential categories of entities in particular sectors of the economy and government activities, from which operators of essential services may be selected through an administrative decision. The criteria for identifying operators of essential services set out in the Act on the National Cybersecurity System meet the requirements referred to in Directive 2016/1148. Recognition of a specific entity as an operator of essential services takes place through a formalized procedure with specific guarantees, based as a rule on the provisions of the Code of Administrative Procedure.

**References:**

Besiekierska, A. (ed.) (2019) *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (Warszawa: C.H. Beck).

Chałubińska-Jentkiewicz, K., Karpiuk, M. & Kostrubiec, J. (2021) *The Legal Status of Public Entities in the Field of Cybersecurity in Poland* (Maribor: Institute for Local Self-Government), https://doi.org/10.4335/2021.5.

Hydzik, W. (2019) Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych, *Przegląd Ustawodawstwa Gospodarczego*, 3, pp. 84-87.

Karpiuk, M. (2021a) The Local Government's Position in the Polish Cybersecurity System, *Lex Localis – Journal of Local Self-government*, 19(3), pp. 609-620, https://doi.org/10.4335/19.3.609-620(2021).

Karpiuk, M. (2021b) The organisation of the national system of cybersecurity. Selected issues, *Studia Iuridica Lublinensia*, 30(2), pp. 233-224, http://dx.doi.org/10.17951/sil.2021.30.2.233-244.

Sawicki, M. (2019) Kilka uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego, *Europejski Przegląd Sądowy*, 9, pp. 13-20.

Wajda, P. (2020) Cyberbezpieczeństwo – sektorowe aspekty regulacyjne, *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, 2, pp. 9-27.

Zdyb, M. & Stelmasiak, J. (eds.) (2020) *Prawo administracyjne. Część ogólna, ustrojowe prawo administracyjne, wybrane zagadnienia materialnego prawa administracyjnego* (Warszawa: Wolters Kluwer).