Monetary Penalties in the National Cybersecurity System Act

Filip Radoniewicz

Abstract This chapter presents the provisions of Chapter 14 ("Provisions regarding monetary penalties") of NCSA containing provisions directed at implementing the provisions of Art. 21 of the NIS which obliging Member States to lay down sanctions applicable to infringements of the national provisions adopted pursuant to the NIS Directive and to take all necessary measures to ensure their implementation.

Pursuant to the above provision of the NIS Directive, the Polish legislator adopted an appropriate provisions providing for administrative liability for three groups of entities: operators of essential services, digital service providers and (additionally) managers of operators of essential services.

To the penalties imposed on the basis of the NCSA, the provisions of the Code of Administrative Procedure apply, which results directly from the content of art. 189a Code of Administrative Procedure.

In this case, provisions of NCSA are 'lex specialis' and take precedence over codex regulations. On the other hand, however, it is difficult to consider the statutory regulation as complete (in Chapter 14, in principle, only provisions regulating the types of violations and the amount of administrative penalties are provided), hence the need to apply the provisions of the Code of Administrative Procedure.

1 Introductory Remarks

The provisions of Chapter 14 of the NCSA ("Provisions regarding monetary penalties") reflect the provisions of Article 21 of the NIS Directive, under which Member States are obligated to penalise infringements of the national provisions adopted

F. Radoniewicz (✉)
Akademickie Centrum Polityki Cyberbezpieczeństwa/Academic Center for Cybersecurity Policy, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland
e-mail: filip.radoniewicz@radoniewicz.eu

K. Chałubińska-Jentkiewicz et al. (eds.), *Cybersecurity in Poland*,
https://doi.org/10.1007/978-3-030-78551-2_22

pursuant to this Directive, and to take all measures necessary to ensure that they are implemented.

In line with the said NIS Directive provision, the Polish legislator adopted an appropriate regulation to govern the administrative liability of three groups of entities:

(1) operators of essential services, entities whose organisational units are located within the territory of the Republic of Poland, which have been recognised by the authority competent for cybersecurity as operators of essential services (operators of services, which are essential for the maintenance of critical societal and economic activities included in the list of essential services). These include banks, energy-sector companies and healthcare entities. It is reasonable to assume that in addition to legal persons and organizational units not being legal persons which have been granted the legal capacity by virtue of statutory law (such as commercial partnerships); such operators might also be natural-person entrepreneurs;[1]
(2) digital-service providers, legal persons or organizational units not being legal persons which have been granted the legal capacity by virtue of statutory law (art, 33^1 of the CC) which have their head office or management office within the territory of Poland, or whose representative has an organisational unit in Poland, which provides digital services, i.e. services provided by electronic means as defined by the Act on the Provision of Services by Electronic Means (PSEMA), listed in Annex 2 to the NCSA, an online marketplace, cloud computing or online search services;

and more:

(3) managers of operators of essential services.

Article 21 of the NIS Directive requires Member States to impose effective, proportionate and dissuasive penalties for infringements of national provisions adopted pursuant to this Directive, and to take all measures necessary to ensure that they are implemented.

By using the word "penalties", the EU legislator refrained from specifying their nature, thus, they may include criminal, civil, as well as administrative sanctions, as in the case of Poland. Effective penalties should be understood as sanctions designed to enforce an objective enshrined in EU laws, which has not been met due to the infringement of the national provisions. Hence, the underlying purpose of administrative penalties is to enforce compliance with the law. Penalties should be proportionate to the type, nature and circumstances of the infringement. In other words, they should be strictly necessary (essential) for the achievement of the objectives enshrined in law. In this sense the principle of proportionality safeguards the rights of individuals. Dissuasive penalties are sanctions, which deter infringement and enforce future compliance.[2]

[1] Radoniewicz (2019), p. 343.

[2] Cf. Fajgielski (2018); Łacny (2011), pp. 477–489.

Notably, administrative liability is not based upon the principle of guilt. Instead, it has an objective nature. Accordingly, administrative penalties are adjudged regardless of the possible fault, since the very fact of infringement provides a basis for their imposition. This is confirmed by the rulings of the Polish Constitutional Tribunal. For example, in its rationale to the judgement of the 25th of March 2010 in case P 9/08 (Legalis) the Tribunal found that monetary penalties represent measures to mobilise entities to comply with their obligations towards the State in a timely and appropriate manner, and that they are used automatically, and legally, and serve preventive functions. By warning against the negative consequences of the infringement of the obligations set forth in law or administrative decision, they encourage statutory compliance. However, it is the objective infringement of the law, which alone provides the basis for imposing a monetary penalty. Not surprisingly, the same stance may be found in the rulings of the Supreme Administrative Court (SAC).[3]

Indeed, the monetary penalties imposed under the are governed by the provisions of the Code of Administrative Procedure[4] (CAP), as explicitly stipulated by Article 189a of the CAP, which requires the provisions of Section IVa of the CAP to be applied in cases involving the imposition or determination of administrative monetary penalties, or the granting of relief in their enforcement, subject to § 2 and § 3, which provide for partial or full derogations from the application of the provisions of this section. The first derogation applies to cases, in which a particular Act governs specific subject matters (preconditions for the determination of administrative monetary penalties, abstaining from the imposition of such penalties, prescription periods for their imposition or enforcement, interest on overdue administrative monetary penalties, and granting relief from their enforcement), thus constituting a *lex specialis*. The other derogation explicitly excludes the application of the CAP in cases involving the imposition or determination of penalties by public administration authorities based on the provisions governing petty offences, disciplinary liability and employees' liability for maintenance of order, and liability for public-finance discipline.

Here, NCSA provisions represent a *lex specialis* and take precedence over CAP regulations. On the other hand, it is difficult to consider the statutory regulation as complete (Chapter 14 essentially governs only the types of infringements and the amounts of administrative penalties). Hence the need to apply CAP provisions (not only those mentioned in Section IVa).

In accordance with Article 189b CAP, an administrative monetary penalty is a statutorily defined financial penalty imposed through an administrative decision issued by a public administration authority for an infringement of the law involving non-compliance or infringement by a natural person, legal person or organizational units not being legal persons which have been granted the legal capacity by virtue of statutory law.

[3] See e.g. SAC Judgement of 27 January 2016, II GSK, 694/14, Legalis.

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

The straightforward expressions used by the legislator in the provisions of Article 73 (1) ("a monetary penalty shall be imposed on operators of essential services") and Article 73 (2) ("a monetary penalty shall be imposed on digital-service providers") of the NCSA make it clear that the penalties provided for operators of essential services and digital-service providers (in contrast to natural persons, managers of operators of essential services, on whom "may be imposed a monetary penalty" by the authorities competent for cybersecurity, see below) are mandatory in nature, resulting in the competent authority being obliged to determine a financial penalty where it has found an infringement of the said provision (unless Article 189f CAP applies). However, the authority has the freedom to decide on the amount of the penalty, as such, the penalty is relative. In one instance the legislator provided for an absolute penalty, the infringement defined in Article 73 (1) (10) of the NCSA, which involves the neglect of a duty, as referred to in Article 14 (1) of the NCSA (i.e. failure to establish internal structures responsible for cybersecurity, or, alternatively, to enter into an appropriate agreement with a provider of cybersecurity services), is subject to a fixed monetary penalty of 100,000 PLN. As a side note, it is worth pointing out that the legislator was "careless" in setting the fixed amount of the penalty while also stipulating that such an amount may not be lower than 15,000 PLN (Article 73 (4) (3) of the NCSA).

2 Administrative Penalties Provided for in the NCSA

In addition to serving the retributive function (as particularly shown by the regulations of Article 73 (5) of the NCSA), administrative monetary penalties are intended primarily as preventive and admonitory measures, both generally (especially with regard to the negative aspect, by dissuading the addressees of the Act from infringing its provisions) and specifically (acting as a deterrent for the penalised operator). Moreover, they are usually designed to force the penalised operator to comply with the obligation set forth in the provisions of the said Act.[5] As mentioned above, almost all monetary penalties defined in the Act are relative. The Act sets the upper limit of the amount of the penalty, which may be determined for an infringement, as well as, for operators of essential services, its lower limit. The legislator has not defined the lower limit of the penalties imposed on digital-service providers. This might pose problems with their determination. In the existing situation this limit should be 1PLN.[6]

In its comments on the draft of NCSA, the Polish Entrepreneurs' Association noted that financial penalties would be imposed on institutions and not on the natural persons who serve managerial functions at them, postulating the introduction of

[5]Cf. Banasiński and Nowak (2018), pp. 170–171.

[6]Radoniewicz (2019), p. 346.

criminal penalties "which would provide the motivation to comply with the Act". In their opinion the PEA proposed the following types of prohibited acts:

(1) failing to ensure adequate data security, especially by operators of essential services, or putting data processed in information systems at risk of being disclosed or lost;
(2) intentionally (on purpose or through gross negligence) disclosing data processed in information systems.

The Council of Digital Affairs issued an opinion proposing that criminal liability be introduced, applicable only to managers of local government units, with the possible penalty being limited to 100,000 PLN per infringement. However, the legislator did not go so far as to introduce criminal liability for members of governing bodies at entities, which commit infringements, instead providing only for the possibility of imposing monetary penalties on managers of operators of essential services (Article 75 of the NCSA).

Ultimately, the legislator provided only for financial penalties in relation to operators of essential services and digital-service providers (the Polish Bank Association criticised this in its opinion), and they have increased them compared to the ones provided in the draft Act, although not going beyond setting the rates. I believe that the comments to the draft NCSA were right to note the need to introduce rates with the amount determined as a percentage of the revenue of the infringing entity. It seems worth considering other measures, which are equally harsh or even harsher than financial penalties, the same as those provided in the Act on the liability of collective entities[7] (LCEA), under which the catalogue of available penalties against collective entities (i.e. legal persons or organizational units not being legal persons which have been granted the legal capacity by virtue of statutory law (excluding the State Treasury, local government units and their associations), commercial companies with a State Treasury holding, local government units or their associations, companies under formation, entities in liquidation, entrepreneurs, who are not natural persons, foreign organisational units (Article 2 (1) and (2) of the LCEA) includes such measures as the prohibition of promotion and advertising, using grants, subsidies or other forms of public financial support, and the prohibition of entering public procurement procedures).

3 Catalogue of Penalties

Almost all infringements penalised under the NCSA involve non-performance or improper performance (failure to notify the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV about a serious incident within twenty four hours from its

[7]The Act of 28 October 2002 on Liability of Collective Entities for Prohibited Acts Punishable by Sanction, consolidated text, Polish Journal of Laws of 2020 item 358, as amended.

identification; hence, an untimely notification might represent an infringement) by operators of essential services of their obligations imposed under the NCSA. The other two instances relate to infringements of procedural rules provided for in the NCSA and involve obstructing inspection and failure to comply with post-inspection recommendations.[8] Provided below are infringements defined in Article 73 (1) the NCSA, including the penalties to which, operators of essential services are subject for such infringements:

(1) failure to perform incident risk assessment on a regular basis or to manage incident risk (negligence of the duty defined in Article 8 (1) of the NCSA) is subject to a monetary penalty of up to 150,000 PLN, but not less than 5000 PLN;
(2) monetary penalties of up to 100,000 PLN (but not less than 5000 PLN) may be imposed for failure to implement technical and organisational measures, which are appropriate for, and proportionate to, the assessed risk, taking into account the requirements referred to in Article 8 (2) (a–e), such as in particular:
    (a) the maintenance and safe operation of the information system;
    (b) physical and environmental security, including access control;
    (c) the security and continuity of services essential for the provision of critical services;
    (d) implementing, documenting, and maintaining action plans to enable the continued and uninterrupted provision of critical services, and to ensure the confidentiality, integrity, availability and authenticity of information;
    (e) establishing a system for the continuous monitoring of the information system used to provide an essential service;
(3) monetary penalties of up to 50,000 PLN (but not less than 5000 PLN) may be imposed for failing to implement the measures referred to in Article 8 (5) (a–d) of the NCSA, i.e. measures to prevent and mitigate the impact of incidents on the security of the information system used to provide an essential service, including the following measures:
    (a) using mechanisms to ensure the confidentiality, integrity, availability and authenticity of data processed in the information system;
    (b) keeping software up-to-date
    (c) providing protection against unauthorised modifications in the information system;
    (d) responding promptly to any identified cybersecurity vulnerabilities or threats;
(4) failure to appoint a contact person to communicate with entities within the national cybersecurity system (Article 9 (1) (1) of the NCSA) is subject to a monetary penalty of up to 15,000 PLN, but not less than 1000 PLN;
(5) failure to perform the duties referred to in Article 10 (1) of the NCSA, i.e. failure to draft documentation on the cybersecurity of the information

[8] Banasiński and Nowak (2018), pp. 170–171.

system used to provide an essential service, or failing to apply or update such documentation despite its being in place is subject to a monetary penalty of 50,000 PLN;

(6) failure to perform the duty referred to in Article 11 (1) (1) of the NCSA, i.e. failure to handle an incident, is subject to a monetary penalty of up to 15,000 PLN (but not less than 5000 PLN) for each identified negligence of such a duty;

(7) failure to perform the duty referred to in Article 11 (1) (4) of the NCSA, i.e. failure to notify the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV about a serious incident within twenty four hours from its identification (under this provision the monetary penalty is also imposed when the operator of essential services reported the incident after twenty four hours from its identification; this should be taken into account when determining the amount of the monetary penalty) is subject to a monetary penalty of 20,000 PLN (but not less than 5000 PLN) for each identified failure to notify an incident;

(8) failure to perform the duty referred to in Article 11 (1) (5) of the NCSA, i.e. failure to provide CSIRT MON, CSIRT NASK or CSIRT GOV with the data necessary to handle a serious incident, or personal data, is subject to a monetary penalty of 5000 PLN to 20,000 PLN;

(9) a monetary penalty of up to 20,000 PLN (but not less than 5000 PLN) is imposed for failure to resolve in a timely manner the vulnerabilities referred to in Article 32 (2) of the NCSA, i.e. ones, which have caused or could cause a serious, significant or critical incident, and the resolution of which has been demanded by the competent authority at the request of CSIRT MON, CSIRT NASK or CSIRT GOV, which coordinate the handling of such an incident;

(10) negligence of the duty referred to in Article 14 (1) of the NCSA, which involves establishing internal structures responsible for cybersecurity, or, alternatively, entering into an agreement with a provider of cybersecurity services, is subject to a monetary penalty of PLN 100,000 (but not less than PLN 15,000);

(11) failure to have an audit is subject to a monetary penalty of PLN 200,000 (but not less than PLN 15,000);

(12) monetary penalties of up to PLN 50,000 (but not less than PLN 5000) are imposed for obstructing inspections by the authority competent for cybersecurity or the minister competent for computerization, as defined in Article 53 (2) (1) of the NCSA, i.e.

   (a) for the minister competent for computerization, inspections on compliance by the internal structures responsible for cybersecurity and the cybersecurity service providers referred to in Article 14 (2) of the NCSA with the requirements referred to in Article 14 (2) of the NCSA, i.e.:

      – meeting the organisational and technical requirements to ensure cybersecurity for the operator of essential services;
      – the availability of incident-response rooms protected against physical and environmental threats; having safeguards in place to ensure the

confidentiality, integrity, availability and authenticity of processed information, taking into account personal safety and the operation and architecture of the systems;

(b) for the authority competent for cybersecurity:

– the fulfilment by operators of essential services of their statutory obligations related to counteracting cybersecurity threats and reporting serious incidents;
– the fulfilment by digital-service providers of the safety requirements related to the digital services provided by them, as laid down by Implementing Regulation 2018/151, and their statutory obligations related to reporting significant incidents;

(13) failure to comply with post-inspection recommendations on resolving irregularities, as referred to in Article 59 (1) of the NCSA (i.e. possible irregularities found by the authority competent for cybersecurity or the minister competent for computerisation based on the information contained in the inspection report) is subject to a monetary penalty of up to 200,000 PLN, but not lower than 15,000 PLN.

As emphasised in the rationale to the draft Act, in accordance with the NIS Directive digital-service providers may be subject to sanctions in the form of monetary penalties only when such providers have infringed the national provisions, which implement the NIS Directive. It is not an option to impose monetary penalties for the infringement of the provisions of the EU legislation, which supplements the NIS Directive (including provisions governing the protection of the information systems designed to provide digital services, as defined in Implementing Regulation 2018/151).

Of course, the catalogue of infringements for which digital-service providers are subject to monetary penalties is much smaller than that applicable to operators of essential services, since they have fewer duties under the Act. Accordingly, monetary penalties apply only to matters associated with the reporting and handling of significant incidents, resolving vulnerabilities, which have or could have led to significant incidents, or which have or could have harmed national defence and state security, public order or the safety, health and lives of people. Digital-service providers are liable for failure to promptly (i.e. within twenty hours from identification) notify a significant incident to the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV (the obligation referred to in Article 18 (1) (4) of the NCSA). Such providers are subject to monetary penalties of up to 20,000 PLN for each failure to report such an incident. Digital-service providers, who fail to provide the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV with the necessary data, including personal data, when handling a significant or critical incident, are subject to a monetary penalty of up to 20,000 PLN. Providers who have failed to resolve the vulnerabilities referred to in Article 32 (2) of the NCSA (i.e. vulnerabilities that have or could have caused a serious, significant or critical incident) despite being ordered to do so by the authority competent for cybersecurity at the request of CSIRT MON,

CSIRT NASK or CSIRT GOV, depending on which one is handling the given incident, may be imposed a monetary penalty of up to 20,000 PLN by such an authority.

4 Penalty Increase

Article 73 (5) of the NCSA provides the authority competent for cybersecurity with the option of imposing an increased monetary penalty of up to 1,000,000 PLN (as already mentioned, the amount was 200,000 PLN in the initial version of the draft), should an inspection find that the operator of essential services or digital-service provider repeatedly infringes the NCSA, causing the consequences listed in the said provision, i.e.:

(1) a direct and serious cybersecurity threat to national defence and state security, public order and the safety, health and lives of people;
(2) the threat of serious damage to property, or serious essential-service disruptions.

Marked by many ambiguous expressions, this provision affords considerable freedom to the authority competent for cybersecurity. In order for the penalty to be imposed, two objective preconditions must be met, the provisions of the Act have been infringed ("repeatedly" suggests that there must be more than one infringement) and such infringements have caused a threat (as stipulated in Article 73 (5) (1) or (2) of the NCSA). However, it is at the discretion of the authority competent for cybersecurity to decide whether the infringements have been committed repeatedly, and also whether their consequences meet the preconditions specified in the said provision (i.e. whether the cybersecurity threat for national defence, state security, public order and the safety, health and lives of people caused by such infringements has been "direct and serious", or whether the potential property damage as a result of such infringements may be described as serious, or whether essential-service disruptions caused by such infringements were serious in nature), and whether to impose a monetary penalty, accordingly.

The administrative penalties referred to in Article 73 of the NCSA are imposed by the authority competent for cybersecurity (i.e. respective ministers, depending on the sector in which the given operator of essential services or digital-service provider operates, as defined in Annex I to the NCSA to ministers competent for energy, transport, maritime economy, inland navigation, health, national defence, computerisation and the Financial Supervision Authority, see Article 41 (4)) by an administrative decision.

Since the administrative penalties set forth in the said provision are subject to administrative discretion (being obligatory but falling within a specified bracket of amounts), and since the legislator has not defined the factors, which should guide the authority's determination of the penalty, the decisions in this regard are governed by the degree-of-penalty directives ("general requirements for the determination of administrative penalties) defined in Article 189d CAP, namely:

(1) the gravity and circumstances of the infringement, including in particular with regard to the protection of life or health, the protection of assets of substantial value, or the safeguarding of an important public interest, or a particularly important interest of a party, and the duration of such an infringement;
(2) past recurring events of non-compliance or infringements of the same type as that which is subject to the penalty;
(3) a record of penalties imposed for the same behaviour, offence, fiscal offence, petty offence and fiscal petty offence;
(4) the degree to which the party to be penalised has contributed to the infringement of the law;
(5) the actions taken voluntarily by the party to be penalised to avoid the consequences of the infringement of the law;
(6) the size of the benefit gained, or the loss avoided, by the party to be penalised; this will be taken into consideration only when the determination alone of the infringement is contingent upon whether the party to be penalised has gained a benefit or avoided a loss through that infringement;
(7) in the case of a natural person, the personal circumstances of the party to be penalised.

In the case of digital-service providers, as legal persons and organizational units not being legal persons which have been granted the legal capacity by virtue of statutory law, it is clear that the last precondition mentioned in the said provision shall not apply, as opposed to operators of essential services, who (at least theoretically) may be natural persons, and their managers. An analogous situation applies to the precondition described in item 4 (it is difficult to accuse a legal person or organisational unit of "contributing" to an infringement of the law).

Since the competent authorities are either supreme authorities (ministers) or central authorities (the Financial Supervision Authority), administrative procedures concerning the imposition of monetary penalties pursuant to provisions of the NCSA are single-instance procedures (i.e. the decisions may not be appealed against). Accordingly, under Article 127 § 3 of the CAP the penalised entity may (in the case of a decision issued by the Financial Supervision Authority, under Article 127 § 3 of the CAP in conjunction with Article 11 (5) of the Financial-Market Supervision Act) lodge a motion for reconsideration. This motion may, however, be relinquished in accordance with Article 127a § 1 of the CAP, resulting in the decision becoming final and irrevocable as of the date on which the public administration authority is served the declaration on the relinquishment of the right to appeal made by the last party to the proceedings.

Since, as already mentioned, under Article 127 § 3 of the CAP motions for reconsideration are governed by the provisions on appeals, under Article 128 CAP there is no requirement to substantiate such motions. It is sufficient that the motion expresses the party's discontent with the decision; unless specific provisions lay down other requirements as to the contents of such motions (no such provisions exist in this case). The time limit for lodging the motion is fourteen days from the service of the decision, and if the decision has been announced orally, from the date of such

an announcement. The decision may not be enforced before this time limit has lapsed, and the lodging of the motion suspends the enforcement of the decision, unless an order of immediate enforceability has been issued by a court (Article 108 of the CAP), or the decision is immediately enforceable by statute (Article 130 § 1, 2 and 3 of the CAP). If the decision satisfies the demands of all the parties, or if all the parties have relinquished their right to appeal (Article 130 § 4 of the CAP), the decision becomes enforceable before the said time limit expires.

A complaint may be filed with the appropriate administrative court against the decision issued after the examination of the motion for reconsideration, in which case general rules for such complaints apply (Article 3 § 2 (1) of the Law on proceedings before administrative courts[9] [LPACA]).

Due to the nature of the operations conducted by operators of essential services and digital-service providers, involving personal-data processing and cross-border ICT networks, a considerable role is played by Article 189f § 1 of the CAP, which provides public administration authorities with the option to refrain, through a decision, from imposing a monetary penalty, and instead only issue a warning. This is the case where the gravity of the infringement is negligible and the party has remedied such an infringement, or where an administrative penalty has been previously imposed by an appropriate public administration authority under a final and irrevocable decision for the same infringement, or where the party has been penalised under a final and irrevocable decision for a petty offence or fiscal petty offence, or where the party has been sentenced under a final and irrevocable judgement for a fiscal offence and the previous penalty serves the purpose underlying the possible administrative penalty. This provision makes it possible to avoid a double penalty for the same infringement as a result of the concurrence of legal rules prescribed in the NCSA, such as with GDPR or cybersecurity regulations applicable in other EU Member States, as might be the case with cross-border incidents.

Article 189f § 2 and 3 of the CAP provides for the possibility of waiving the penalty in cases other than those described in Article 189f § 1 of the CAP, should this serve the purposes of the possible administrative penalty. In this situation a public administration authority may issue a decision to set a time limit for the party to furnish evidence that the infringement of the law has been remedied, or that the appropriate entities have been notified of the infringement, prescribing the time limit for, and manner of, such a notification (Article 189f §2 of the CAP). Where the entity has furnished evidence that the requirements of the decision have been met, the public administration authority shall refrain from imposing an administrative penalty and instead only issues a warning to that entity. Adjudication with regard to refraining from imposing an administrative penalty, as a determination of the merits of the case (i.e. a subject-matter determination), should take the form of an administrative decision.[10]

[9]Act of 30 August 2002—the Law on proceedings before administrative courts, consolidated text, Polish Journal of Laws of 2019, item 2325, as amended.

[10]Stankiewicz (2020).

Article 76 of the NCSA ("the penalty referred to in Article 73 may also be imposed where the entity has remedied the infringement or the damage caused by such an infringement, provided that the authority competent for cybersecurity finds that this is justified due to the duration, scope and consequences of the infringement") seems to suggest *a contrario* that the administrative penalty prescribed in Article 73 may not be imposed where the entity concerned has remedied the infringement or damage caused by such an infringement, unless the authority competent for cybersecurity finds that this is justified due to the duration, scope or consequences of the infringement.[11] However, it seems that in reality this provision is somewhat amiss, modifying the general regulation applicable to refraining from a penalty, as stipulated by Article 189f § 2 and 3 of the CAP. Indeed, it enables the competent authority to impose a monetary penalty even in the circumstances described in Article 189f § 3 of the CAP (Article 189f § 3 of the CAP do not provide for options other than refraining from the penalty). Notably, the legislator has afforded the authority competent for cybersecurity considerable freedom in its decision-making. Hence, the exercise of the right to impose a monetary penalty is contingent here on the authority's finding that such a monetary penalty is justified by the vaguely described statutory preconditions, i.e. the duration, scope or consequences of the infringement.

The original version of the draft of NCSA (discussed as part of public consultations held before it being submitted for further Parliamentary processing) expected that before instigating penalty proceedings the authority competent for cybersecurity could request the operator of essential services (the original draft did not provide for digital-service provider's liability) to remedy the infringement within a specified time limit, provided that this is justified due to the nature of the infringement (Article 58 (2) of the original bill). This provision, however, was eventually removed from the final version of the Act. Possibly, it was considered redundant, since similar solutions are provided by the above-discussed provisions of Article 189f § 2 and 3 of the CAP. I believe this supports the above-presented interpretation.

An adjudication made pursuant to Article 76 of the NCSA should take the form of an administrative decision.

Since the NCSA does not address the prescription period for the ruling and the enforcement of the penalty, CAP provisions apply, stipulating that an administrative penalty may not be imposed once five years have lapsed after the infringement date or the date on which the consequences of the infringement occurred, unless separate laws prescribe a time limit after which administrative-penalty or infringement proceedings, involving a potential monetary penalty, may not be instigated. Such a penalty may not be enforced once five years have lapsed from the date on which the penalty should have been enforced. The prescription period for, as well as the enforcement of, the administrative penalty cease upon the declaration of bankruptcy by the party concerned (Article 189h and 189j CAP).

[11] Banasiński and Nowak (2018), pp. 170–171.

In accordance with Article 189 of the CAP, where justified due to an important public interest or an important interest of the party concerned, the public administration authority, which has imposed an administrative penalty at the request of the party may grant relief in the enforcement of the administrative penalty by:

(1) postponing the date by which the administrative penalty is to be enforced, or dividing the monetary penalty into instalments;
(2) postponing the date by which the outstanding administrative penalty is to be enforced, or dividing the monetary penalty into instalments;
(3) forgiving the administrative penalty in full or in part (where an outstanding administrative penalty is forgiven, this also includes late-payment interest in full or in part, to the extent that such an outstanding administrative penalty has been forgiven);
(4) forgiving, fully or partly, late-payment interest.

In proceedings concerning relief in an administrative-penalty enforcement a party to which is a business entity, the authority has the obligation to determine whether such a relief represents state aid as defined by EU law. No such relief may be granted where it represents *de minimis* aid or *de minimis* aid in agriculture or fisheries. Where the relief is found to be state aid other than *de minimis* aid, it may be granted, provided that:

(1) its purpose would be to redress/remedy any damages caused by natural disasters or other force majeure;
(2) it would help to address serious economic disturbances;
(3) it would be compatible with the internal EU market rules, and that it has been considered admissible by the appropriate EU authorities for purposes other than those mentioned in items (a) and (b) above.[12]

Pursuant to Article 189e CAP where the infringement was due to force majeure, operators of essential services and their managers, and digital-service providers are not subject to penalty (Article 189e of the CAP). A force majeure is an external event beyond the control of the affected entity, which has no influence on the occurrence and consequences of that event. Three categories of force majeure are distinguished: natural disasters, legislative and executive acts, and serious public disorders.[13] As noted by A. Wróbel, Article 189e of the CAP applies to situations where the affected entity failed to meet its obligation (through an infringement or non-compliance) as a result of a force majeure.[14]

The exclusion of penalty is a construct derived from criminal law. The Penal Code (PC) provides for such a solution where the perpetrator abandons the prohibited act or prevented its consequence (Article 15 § 1 of the PC), or where the co-perpetrator voluntarily prevents the prohibited act (Article 23 of the PC), or in

[12]For more on the subject, see Wróbel (2019a).
[13]Warkałło (1949), pp. 100–102.
[14]Wróbel (2019b).

the event that the limits of necessary defence have been exceeded due to fright or emotional distress, as justified by the circumstances of the attack.[15] It is a prerequisite for criminal proceedings, as defined in Article 17 § 4 of the CAP, representing a circumstance on which the admissibility of criminal proceedings is contingent (i.e. a circumstance which, if found to exist, result in the refusal to instigate proceedings or to discontinue pending proceedings), and which is substantive (meaning that it derives from, and causes consequences in, the substantive-law sphere), absolute (irresolvable), common (applicable always, regardless of the procedure) and negative (meaning that its occurrence shall preclude the instigation of the proceedings).[16] In the context of administrative proceedings, this means that an infringement of the law due to force majeure shall not result in the instigation of proceedings to impose a monetary penalty, and if the circumstance was found to exist in the course of the proceedings, such proceedings are discontinued.[17]

5 The Liability of Managers of Operators of Essential Services

The Act uses the term "managers of operators of essential services" (no liability is provided for "managers of digital-service providers") without providing any definition (e.g., in the "glossary" in Article 2) of what it means. Clearly, no such position exists in the organisational structures of organisational units, which operate, for instance, under the Code of Commercial Partnerships and Companies, and since operators of essential services (as well as digital-service providers) are usually entrepreneurs (see Annex 1 to the NCSA) within the meaning of Article 4 (1) and (2) in conjunction with Article 3 of the Entrepreneurs Law Act[18] (LEA) (i.e. natural persons, legal persons or organizational units not being legal persons which have been granted the legal capacity by virtue of statutory law which conduct business activities, i.e. organised for-profit activities carried out continuously and in their own name, and also partners in civil-law partnerships to the extent of their business activities), in legal transactions they usually operate as commercial entities, i.e. partnerships and, above all, companies. A similar problem is encountered in the Act on the protection of classified information[19] (PCIA), in which the term "manager" is used in relation to the so-called industrial-security proceedings (i.e. proceedings conducted by the Internal Security Agency or the Military

[15] Cf. Wróbel (2019b).

[16] Grzegorczyk (2014), pp. 108–109.

[17] Cf. Krawczyk (2018).

[18] Act of 6 March 2018—the Entrepreneurs Law, consolidated text, Polish Journal of Laws of 2019 item 1292, as amended.

[19] Act of 5 August 2010 on the Protection of Classified Information, consolidated text, Polish Journal of Laws of 2019, item 742, as amended.

Counterintelligence Service to establish whether an entrepreneur seeking, or planning to seek, to enter contracts associated with access to classified information, or an entrepreneur already bound by such contracts, or fulfilling statutory responsibilities associated with access to classified information provides the conditions required to protect classified information). However, the PCIA defines the term "entrepreneur's manager" as the sole Management Board member, or the member of a different single-member governing body, and if the governing body comprises multiple members, the entire body or the member or members of such a body appointed at least under a Management Board resolution to serve in the capacity of entrepreneur's manager, excluding any proxies appointed by such a body or unit; in the case of general partnerships and civil-law partnerships, entrepreneur's managers are the partners in charge of the partnership's affairs, and in the case of professional partnerships, the partners in charge of the partnership's affairs or the Management Board, and in relation to limited partnerships and limited joint-stock companies, the general partners in charge of the partnership's or company's affairs; in the case of natural-person entrepreneurs the entrepreneur's manager is the natural person concerned; liquidators, trustees in bankruptcy and receivers are also considered to be entrepreneur's managers; an entrepreneur's manager is an organisational-unit manager within the meaning of the Act (Article 2 (14) of the PCIA). The term manager, or unit manager, more specifically, is also used in the Accounting Act. For the purposes of this Act, Article 3 (1) (6) thereof stipulates that an organisational-unit manager is a member of the Management Board or other governing body, and if that body comprises multiple members, the members of that body, excluding any proxies appointed by the unit. In the case of general partnerships and civil-law partnerships, the role of unit manager is ascribed to the partners in charge of the partnership's affairs, and in the case of professional partnerships, the partners in charge of the partnership's affairs or the Management Board, and in relation to limited partnerships and limited joint-stock companies, the general partners in charge of the partnership's or company's affairs. In the case of natural-person entrepreneurs, unit managers are the natural persons concerned; and the same provision applies to individuals practising liberal professions, accordingly. Unit managers are also liquidators, trustees in bankruptcy and receivers appointed in reorganisation proceedings, as well as succession administrators, as referred to in the Act on succession administration (ASA), or the individuals referred to in Article 14 of the said Act, who performed the filing referred to in Article 12 (1c) of the Act on the registration and identification of taxpayers and taxable persons. The Accounting Act also provides the definition of the term "governing-body member" as a natural person serving in the capacity of member of the Management Board or other governing body, member of the Supervisory Board or other supervisory body, as well as member of other administrative body of the unit, appointed in accordance with the Articles of Association, Partnership Agreement or other laws applicable to the unit (Article 3 (1) (5a) of the Accounting Act). It seems that the definition provided in the Accounting Act is more appropriate for the purposes of interpreting the term "manager of an operator of essential services".

The liability of managers of operators of essential services is limited to cases involving failure by such managers to exercise due care to fulfil the obligations laid down in the said provision, i.e. to perform incident risk assessment on a regular basis and to manage incident risk (Article 8 (1) of the NCSA), appoint a contact person to communicate with entities within the national cybersecurity system (Article 9 (1) (1) of the NCSA), and to have, at least every two years, a security audit of the information system used to provide the essential service (Article 15 (1) of the NCSA). Monetary penalties on managers of operators of essential services are optional (as opposed to operators of essential services and digital-service operators, where such monetary penalties are mandatory).

As already mentioned, during the public consultations on the NCSA a suggestion was put forward (in the comments made by the Polish Entrepreneurs' Association with regard to the draft of NCSA) to introduce criminal liability for individuals in managerial positions, the rationale being that ensuring cybersecurity was of considerable significance. However, the legislator chose not to implement this solution.

References

Banasiński C, Nowak W (2018) Europejski i krajowy system cyberbezpieczeństwa. In: Cyberbezpieczeństwo. Zarys wykładu, Warsaw

Fajgielski P (2018) In: Ogólne rozporzadzenie o ochronie danych, Commentary on Article 83 GDPR, section 8. LEX/el

Grzegorczyk T (2014) Kodeks postępowania karnego, Warsaw

Krawczyk A (2018) In: Chroscielewski W, Kmieciak Z (eds) Kodeks postepowania administracyjnego. Komentarz, Commentary on article. 189e CAP, Warsaw LEX/el

Łacny J (2011) Skuteczna, proporcjonalna i odstraszająca sankcja za naruszenie prawa UE. In: Wróbel A (ed) Zapewnienie efektywności orzeczeń sądów międzynarodowych w polskim porządku prawnym, Warsaw

Radoniewicz F (2019) In: Kitler W, Taczkowska-Olszewska J, Radoniewicz F (eds) Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Warsaw

Stankiewicz R (2020) In: Hauser R, Wierzbowski M (eds) Kodeks postępowania administracyjnego. Komentarz, Commentary on Article 189f CAP, Warsaw LEX/el

Warkałło W (1949) Siła wyższa jako zasada nieodpowiedzialności i domniemanie przypadkowości szkody, Państwo i Prawo 9–10

Wróbel A (2019a) Komentarz do art. 189e KPA. In: Jaśkowska M, Wilbrandt-Gotowicz M, Wróbel A (eds) Komentarz zaktualizowany do Kodeksu postępowania administracyjnego. Warsaw, LEX/el

Wróbel A (2019b) Komentarz do art. 189k KPA. In: Jaśkowska M, Wilbrandt-Gotowicz M, Wróbel A (eds) Komentarz zaktualizowany do Kodeksu postępowania administracyjnego. Warsaw, LEX/el

Filip Radoniewicz PhD; legal advisor; adjunct in the Department of Cybersecurity Law and New Technologies at the Institute of Law, War Studies University, Warsaw; expert at the Academic Centre for Cybersecurity Policy (War Studies University) and in the Ministry of Justice; he worked as an assistant judge (in the Fourth Criminal and Sixth Penitentiary Department of the Regional Court in Lublin); graduate of post-graduate studies: "European Union Law" at the Jagiellonian University, "Human Rights and Freedoms", co-organized by the Institute of Legal Sciences of the Polish Academy of Sciences and the Helsinki Foundation for Human Rights, and "Computer Network Administration" at the Lublin University of Technology; author or co-author of approximately fifty publications, mainly in the field of broadly understood criminal law, new technology law and human rights. Selected publications: F. Radoniewicz (2016) Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym / Criminal liability for hacking and other offences against computer data and information systems/, Wolters Kluwer, Warszawa; Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz /Act on the National Cybersecurity System. Commentary/ (2019) ed. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, CH. Beck, Warszawa.