NIS2 Directive implementation in Poland

Warsaw, 28 October 2024

KL&M LAW

Kobylańska · Lewoszewski · Mednis

IMPLEMENTATION OF THE NIS2 TO THE POLISH LEGAL FRAMEWORK

This publication is intended solely for informational and educational purposes and should not be considered legal advice.

This paper outlines changes in the Polish legal system regarding the implementation of the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (hereinafter: the **"NIS 2 Directive"** or "**NIS2**"). The text focuses on emphasizing potential new obligations for undertakings and new competencies of government bodies. The new laws are presented in summary form without additional analysis.

1. IMPLEMENTATION OF NIS2

The Directive on measures for a high common level of cybersecurity across the Union (NIS2 - 2022/2555) entered into force in January 2023. Member States were obligated to implement (adopt and promulgate) the provisions of the Directive into their legal systems by 17 October 2024. On 3 October 2024, Poland published a second version of the draft implementing act, which serves as an amendment to the existing law - the Act on the National Cybersecurity System of 5 July 2018 (hereinafter: the "**ANCS**"). This legislation currently enacts the first NIS directive, which the NIS 2 Directive superseded. We assume that the *Sejm* will agree to the proposed amendment by the end of the year, since the official implementation deadline has expired, and this is the second attempt to amend the ANCS.

We have analyzed the proposed amendment and summarized the most important changes. This guide is based on the draft amendment of 3 October 2024. The proposed law sets out mechanisms for effective cooperation between competent authorities in different sectors of the economy and defines new cybersecurity obligations as well as measures to enforce them.

Should you have any questions, please do not hesitate to contact me.

Marcin Lewoszewski

Partner

Marcin.Lewoszewski@KLMLAW.PL

2. EXPANSION OF THE SCOPE OF THE LAW

In its present wording the ANCS distinguishes among three categories of entities: key service providers (in the NIS directive: operators of essential services), digital service providers and public entities.

The proposed draft ANCS eliminates the previous terms and introduces two new categories of entities. These are: essential entities (*podmioty istotne*) and important entities (*podmioty ważne*).

The primary distinction between the two categories lies in the fact that, while both essential and important entities share identical obligations, the oversight of each category is conducted differently.[1] The existing ANCS separately regulates obligations imposed on specific category of entities.

2.1. RULES FOR CATEGORISATION

The entities will be classified into categories according to two criteria:

- the staff headcount ceilings for micro, small and medium enterprises set forth in Article 2(1) of Annex I to Commission Regulation (EU) No. 651/2014 of 17 June 2014 (hereinafter: "**Regulation 651/2014/EU**")[2]; and
- whether particular entity belongs to one of the entity types referred to in Annex I or II to the amended ANCS.

The classification will follow the general rule:

Essential entity

- exceeds the ceiling for medium enterprise; and

[1] Even though, as a rule, the obligations of both key and important entities will be the same, entities providing certain types of services will have special obligations. For example, an electronic communications service provider has less time to report an incident. Such special regulations however do not impact the general rule, because an electronic communications service provider can be both a key and an important entity.

[2] Interestingly, the NIS2 directive refers to Annex to Recommendation 2003/361/EC, Article 2(1). This however is not an error, because ceilings set in both of these Annexes are identical.

- is of the type referred to in Annex I or II to the amended ANCS;

Important entity:

- is not an essential entity;
- is of the type referred to in Annex I or II; and
- complies with the threshold for the medium-sized entrepreneurs.

In addition, there will be special categorization rules for certain types of entities.

The following entities will also be considered essential under the amended ANCS.:

1) An electronic communications entrepreneur who, at the minimum, meets the requirements for a medium-sized entrepreneur, as set forth in Regulation 651/2014/EU;
2) Regardless of the entity's size:

   - DNS service providers;
   - providers of managed cybersecurity services (in NIS2: "managed security service providers");
   - critical entities (it is to be understood as a critical entity within the meaning of the CER directive, which has not yet been incorporated into Polish law);
   - public entities;
   - entities identified as essential entity pursuant to Article 7(l)(2) point 1[3];
   - top-level domain name registries (TLD);
   - state legal persons identified as key entities under Article 7m;
   - entities that are nuclear power facility operators pursuant to Polish Bill on Developing and Implementing Nuclear Energy Projects and Related Facilities.

The following entities will also be considered as **important entities** for the purposes of the amended ANCS:

[3] Relevant authorities can identify essential and important entities on their own, if given entities meet certain requirements – see Points 3.1., 3.3. of this guide.

- non-qualified trust service providers falling into one of the categories of a micro, small or medium-sized enterprises referred to in Article 2(1) of Annex I to Regulation 651/2014/EU;

- electronic communication entrepreneurs being one of the micro-, small or medium-sized enterprises referred to in Article 2(1) of Annex I to Regulation 651/2014/EU,

- an entity identified as an important entity pursuant to Article 7l (2)(2),[4]
- an entity being an investor in a nuclear power project under Polish Bill on Developing and Implementing Nuclear Energy Projects and Related Facilities.

If an entity meets both the criteria for an essential entity and an important entity, it is classified as an essential entity.

Entities providing services essential to the functioning of the modern information society operate across borders. Consequently, it was essential to preemptively assess their national jurisdiction in compliance with the NIS2 Directive. The entities fall under Polish jurisdiction if the head of the entity who is the entity's decision-maker regarding its information security management system is based, or tasks related to the entity's information security management system are carried out, or the largest number of the entity's employees as compared to other European Union Member States is in the territory of the Republic of Poland (Article 5a ANCS).

Furthermore, authorities will be able to categorize essential and important entities on their own, even if a specific entity does not meet the requirements set out in points 2.1 and 2.2 above. The amended ANCS will set out the conditions that will make it possible (which are discussed in Points 3.1., 3.3. below).

[4] Relevant authorities can identify essential and important entities on their own, if given entities meet certain requirements – see Points 3.1., 3.3. of this guide.

2.2. OBLIGATIONS IMPOSED ON THE ESSENTIAL AND IMPORTANT ENTITIES

2.2.1. GENERAL OBLIGATIONS

NIS2 requires non-EU businesses operating in the European Union to appoint representatives, who will be contacted by the National cybersecurity system institutions, such as CSIRT, regarding their obligations. This is reflected in Article 5a (5-6) ANCS.

In order to facilitate identification of an entity as an essential or important one, it is obliged to register itself, as required under Articles 7-7b ANCS. The registration will take place within the list of key and important entities, which will be maintained by the Minister of Digitization (see Point 3.1. below). This regulation will replace the existing regulations on the list of key service operators.

Entities that meet the requirements for an essential or important entity will be required to be registered within two months after they have met the relevant criteria (Article 7b (1) ANCS). The list will provide all information necessary to effectively exercise supervision of such entities: the data identifying the entity - name (business name), economy sector, subsector and type of entity, in accordance with the annexes to the laws, registered office and mailing address, (if assigned) electronic delivery address, e-mail address, tax identification number, REGON number and the code number in the relevant register of regulated activities (article 7 (3) ANCS)

Once it is entered in the register, an entity will be required to connect to an ICT system through which it will carry out risk estimations and report incidents (Article 46 (1a) and (4) ANCS). The system is already in place, supporting the exchange of information among the entities of the national cybersecurity system. Ultimately, the system will consolidate all communications regarding cybersecurity issues and furnish tools to assist the interconnected entities in doing risk assessments, among other functions.

An entity may request delisting if it no longer meets the criteria of an essential or important entity, which will be confirmed by the cybersecurity authority (Article 7f ANCS).

Article 53c has been introduced in order to ensure that the supervisory authority can properly exercise its powers. It provides that, upon request, essential and important entities provide cybersecurity authority with all data, information and documents the authority needs to exercise its powers and obligations provided by law.

2.2.2. OBLIGATIONS UNDER ARTICLE 21 NIS 2

Following the implementation of Article 21 of the NIS 2, Article 8 of the ANSC imposes a new obligation on the essential and important entities to deploy an information security management system that will guarantee:

- regular incident risk estimation and management;
- implementation of the technical and organizational measures appropriate and proportionate to the estimated risk, considering the state of the art, cost of implementation, entity's size, likelihood of the incidents, entity's exposure to various risks;
- collecting information on cyberthreats and vulnerabilities of the information system by which the service is provided;
- incident management;
- application of measures to prevent and reduce the impact of incidents on the security of the information system by which the service is provided;
- use of secure means of electronic communication as part of the national cybersecurity system, considering multi-factor authentication.

It is worth noting that pursuant to Article 8 ANCS, information security management systems need not be certified for any of the technical standards. It is sufficient to implement the system in compliance with the law and to document it accordingly.

2.2.3. OBLIGATIONS OF THE HEADS OF THE ESSENTIAL AND IMPORTANT ENTITIES

Articles 8c-8e of the ANCS impose several obligations on the heads of the essential and important entities.

The head of an essential or important entity is responsible for the entity's performance of its duties in the area of cybersecurity. If the head is a multi-member body, then all members of the body are responsible. The head will also be responsible in cases that were consensually entrusted to another person.

Article 8d-8e ANCS provides for some of the other obligations and competencies of the entity's head, including specifically:

- making decisions on the preparation, implementation, application and review of the entity's information security management system;
- planning adequate financial resources for the implementation of the cybersecurity obligations;
- undergoing the cybersecurity training every year;
- making the basic information on the entity's head activity available on a designated webpage.

Provisions under which the key service operators have performed their duties through internal structures or through cybersecurity service providers are repealed in the amended ANCS. Now, such entities will be directly obliged to implement information security management systems.

Article 8h ANCS sets a framework for the exchange of critical cybersecurity information among the essential and important entities; sharing information about threats and attacks allows other entities to secure their systems and protect themselves against the threat. The entities grouped in the national cybersecurity system may also enter into agreements for mutual exchange of information. Each of the essential and important

entities must also designate two contact persons to maintain relations with such other entities (Article 9 (1) Point 1 ANCS). The entities are also required to provide to service users knowledge to understand cyberthreats and apply effective ways to protect against them to the extent related to the service provided (Article 9 (1) Point 2 ANCS).

2.2.4. REPORTING INCIDENTS

Article 11 of the amended ANCS follows incident-reporting standards provided in NIS2. According to the proposed solutions, significant incidents will be reported to the sectoral CSIRT to the extent necessary for the performance of its tasks.

First, the affected entity, whether it is an essential or important one, will be required, without undue delay, but no later than within 24 hours of becoming aware of a significant incident, to send an early warning notice. In the warning, the entity, where applicable, will indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact (Article 11 (1) (4) ANCS).

The early warning notice may include a request for guidance on implementable mitigation measures for a significant incident or for technical support in handling the incident. If the significant incident bears the attributes of a crime, the sectoral CSIRT will provide information on how to report it to the prosecuting authorities. The sectoral CSIRT is obliged to provide the requested support within 24 hours.

Within 72 hours of becoming aware of a significant incident, the affected entity will send an update notice to the respective sectoral CSIRT to update the information provided in the early warning any event (Article 11 (1) (4a) ANCS). Furthermore, the affected entity will also be obliged to submit periodic incident handling reports upon request from the sectoral CSIRT.

2.2.5. AUDITS

Essential and important entities are required to ensure, at their own expense, the running of security audits of their information systems (Article 15 (1) ANCS) at least once in three years, which will run from the preparation and signing of the previous audit. Within three

days of receiving the report, the entity will submit it in the electronic form to the competent cybersecurity authority

The competent cybersecurity authority will have the power to have the essential and important entities undergo *ad hoc* external audits, especially in the event of occurrence of a significant incident or other violation of the cybersecurity law.

The audit of the information security management system must be conducted by independent without a bias regarding the audited entity; the audit may not be performed by individuals who, up to one year prior to the audit have worked or still work for the audited entity while executing tasks concerning the information security system management, incident reporting and response.

2.2.6. IMPLEMENTATION DEADLINES

Currently, the moment from which the deadlines for the implementation of obligations by key service operators (*operator usług kluczowych*) run, is the delivery of the decision recognizing a key service operator.

The proposed regulations (Article 16 ANCS) indicate that essential and important entities must carry out their obligations within six months from the date they have fulfilled the conditions to recognize them as such, and the system audit will be implemented for the first time within 24 months from the date of fulfilment of the said prerequisites.

2.2.7. OBLIGATIONS FOR TOP LEVEL DOMAIN NAME REGISTRIES

New obligations have also been imposed on the top-level domain name registries (hereinafter: "**TLDs**") and the entities providing domain name registration services, especially regarding the due diligence collection, preservation, completeness, and accuracy of the domain name registration data (Article 16a (1) ANCS).

These entities should now introduce policies and procedures, including verification procedures, to ensure that the data in the domain registration databases are accurate and complete; the policies will be made available publicly, and the data from the

databases will only be shared with law enforcement agencies and judicial authorities upon valid request.

2.2.8. FINES

Amendments to the law regarding fines include the adjusting of the catalogue of fines for failure to breach the new obligations imposed on the essential entities or important entities, as provided in Articles 73 – 76e ANCS.

An essential or important entity may be fined for failures to:

- fulfil its obligations regarding the register of essential and important entities;
- introduce an information security management system;
- conduct regular risk assessment or to manage the risk of an incident;
- run an audit to the deadline;
- appoint a person for contacts with such other entities;
- provide service users with access to knowledge to understand cyberthreats and apply effective ways to protect against them to the extent related to the services provided;

and more.

Fines may be imposed when justified by the gravity and importance of the violated regulations. An essential or important entity may even be fined when its action or failure to act is a one-time occurrence.

The minimum penalty for essential entities is PLN 20,000. The penalty shall not surpass the greater of the following two amounts: the PLN equivalent of EUR 10,000,000, calculated using the average exchange rate published by the National Bank of Poland on the date of the penalty decision, or 2% of the revenue accrued by the essential entity from its business operations in the fiscal year prior to the penalty's imposition.

For the important entities, the minimum fine level has been set at PLN 15,000. In principle, the fine may not exceed the higher of the PLN equivalent of EUR 7,000,000 as determined using the average exchange rate announced by the National Bank of Poland

in effect on the date of the decision to impose the penalty, or 1.4 of the revenue generated by the essential entity from its business activities in the fiscal year preceding the imposition of the penalty.

However, if the action or omission poses an imminent serious cybersecurity threat to the national defense, state security, public safety and order, or human life and health, or may cause serious property damage or serious obstruction of services, the fine imposed by the competent authority may amount up to PLN 100,000,000.00.

The Head of an essential or important entity may also be fined for a failure to fulfil the obligations set forth in ANCS (Article 73a (2 and 3) ANCS), and the fine may be imposed regardless of whether the entity itself was also fined or not.

The potential implementation of a recurring fine on an entity is a significant modification to the law. This will be feasible under certain conditions, including delays in implementing measures to prevent or halt violations of the ANCS[5].

In order to compel an entity to comply with obligations set on it, the cybersecurity authority may impose on the entity, by decision, a periodic fine ranging from PLN 500.00 to PLN 100,000.00. It should be noted that the periodic fine differs from the fine envisaged in the preceding articles of the law, since it is not the violation of the ANCS itself that is punished but rather the delay in executing the steps ordered by the authority, often in connection with the violation.

3. IMPLICATIONS FOR GOVERNMENTAL AUTHORITIES

3.1. THE MINISTER FOR DIGITIZATION

The Minister for Digitization maintains a list of essential and important entities. Importantly, the Minister will acquire the following additional powers as a result of the changes made to the list itself (Article 7 ANCS):

- supplementing the data provided by the self-registering entities (Article 7 (5) ANCS), including the competent cybersecurity authority, the competent

[5] The periodic fine may be imposed in the situations listed in Articles 53 (4); 53 (5) (2-7) ANCS.

sectoral and national CSIRTs, the legal reason for the entity registering itself on the list (Article 7 (2) (19-20, 24) ANCS;

- if possible, *ex officio* registering entities from among the groups that will be included in the list in their entirety anyway, e.g., telecommunications entrepreneurs, critical entities, trust service providers or public entities using data that is already collected in other public registers (Article 7 (6) ANCS)[6];
- when suitable, *ex officio* de-listing of the entities that have lost the relevant status or have been wrongfully registered (Article 7 (18, 20);

The Minister is also given new obligations, i.e., disclosing data from the list to various CSIRT bodies and other authorities competent for cybersecurity and to an essential or important entity from the list (Article 7 (21) ANCS);

The Minister will also have another obligation, which is preparing and monitoring the implementation of the National Plan for Large-Scale Cybersecurity Incident and Crisis Response and Monitoring (Article 72d ANCS). Here, the Minister will serve as the civilian body responsible for large-scale cybersecurity incident and crisis management.

Pursuant to Article 67g, in the event of a critical incident, the Minister for Digitization, may issue a security command – to the extent necessary and proportionate – to businesses providing essential services to the information society, to adopt a conduct that will protect, among others, the information systems and telecommunications networks of multiple entities against the consequences of a critical incident. The procedure will be preceded by an analysis conducted jointly with the Team for Critical Incidents Affairs[7]. The command may consist of imposing the adoption of a specific security patch, specific configuration of hardware or software or prohibiting the use of specific hardware or software. However, it should also be noted that the ban on the use of specific services and software will only apply to solutions that are relevant to the ongoing critical incident no longer than two years (Article 67g (10-12) ANCS).

---

[6] It is worth noting, that other authorities competent for cybersecurity (see: Articles 41-41a ANCS; Point 3.3 hereof) hold similar competencies with regard to the entities meeting the prerequisites to recognize them as an essential or important entity that have not submitted an application (Article 7a of ANCS).

[7] It is an expert team designed to facilitate the response to a critical incident, consisting of some key government institutions providing cyber security in the country (Article 36 ANCS).

The Minister will *ex officio* conduct proceedings to recognize a hardware or software supplier as a high-risk supplier (Article 67b ANCS). The proceedings may involve suppliers of ICT products, services and processes – notably of 5G networks – if the premise of ensuring the protection of the state security is met. The proceedings will not cover all products, services and processes of a particular hardware or software supplier, but only to those used by essential and important entities, with the exception of those from the electronic communications subsector or telecommunications undertakings whose annual revenues from the telecommunications activities exceeded PLN 10,000,000.00 in the previous fiscal year. The proceedings may also be conducted at the request of the Chairman of the College for Cybersecurity Affairs (*Przewodniczący Kolegium ds. Cyberbezpieczeństwa*) (see: Point 3.6. hereof).

Identification of a high-risk supplier should result in the risk being mitigated as a legal consequence. A high-risk supplier could be either international or based in the Republic of Poland.

Under Article 70a ANCS, the Minister for Digitization become the body responsible for the implementation of the Cybersecurity Strategy for the Republic of Poland and may obtain information on the implementation of the strategy from other entities involved. As described in Article 69 ANCS, the strategy outlines the strategic goals and relevant policy and regulatory measures to achieve and maintain a high level of cybersecurity.

The national strategy for handling major cybersecurity emergencies and events will be introduced by a number of new laws (Articles 72a-72f ANCS). In order to maximize the effectiveness of cybersecurity assurance and crisis management efforts, this policy document outlines the authorities' responsibility as well as the measures and procedures to be taken in the event of a cybersecurity emergency. The plan will be adopted by a resolution of the Polish government (the Council of Ministers) and drafted by the Minister for Digitization, who (like in the case of the aforementioned Strategy) may obtain information on the implementation of the strategy from other involved entities.

3.2. THE MINISTER FOR NATIONAL DEFENSE

The catalogue of the tasks of the Minister of Defense has been adapted to the new structure of the national cybersecurity system. The new tasks will include:

- directing, through the Ministry of National Defense's CSIRT MON, incident handling activities, as well as coordinating the activities of the CSIRT NASK and CSIRT GOV during martial law and during wartime (Article 2a ANCS);
- assessing cyberthreats at each stage of the state defense readiness and making proposals to the relevant authorities on the defense measures (Article 51 (1) (7) ANCS);
- coordinating, in cooperation with the minister in charge of the internal affairs and the minister in charge of information technologies, the implementation of the tasks of the government administration bodies and local government units during martial law and in wartime concerning the defense measures in the event of a cyberthreat (Article 51 (1) (8) ANCS);
- coordinating the activities of the government bodies in the event of cybersecurity crisis situations with regard to the defense of the State and the Armed Forces of the Republic of Poland (Article 51 (1) (9) ANCS);
- Upon appointment of the Commander-in-Chief of the Armed Forces and his assumption of the command of the Armed Forces, supervising selected specialist teams and equipment resources of Cyberspace Defense Forces (Article 52a ANCS);
- coordinating incidents handling with the entities performing the tasks for the Polish Armed Forces.

3.3. SUPERVISORY AUTHORITIES

The obligation to implement Articles 31-32 NIS 2 must be performed taking into account the amendments to Article 53 of ANCS. The authorities competent for cybersecurity will oversee the performance of obligations by the essential and important entities arising under the law (Article 53 (1) ANCS).

The supervisory authorities include the President of the Office of Electronic Communications, the competent ministers or the Head of the Internal Security Agency (Articles 41-41b ANCS). The supervisory authorities are each appointed for the relevant

sectors and entity types. For example, the Minister of Digitization is the supervisory authority for the important entities in the sector of digital service providers.

The competencies that the supervisory authorities have with regard to the essential and important entities are listed as oversight measures in Article 53 (2) ANCS:

- on-site or remote inspections, requesting information, access to data, documents and information;
- making specific entity obliged to run a security audit.

Oversight may be exercised by ordering CSIRT MON, CSIRT NASK, CSIRT GOV or sector CSIRTs to perform a security assessment of a specific entity (Article 53 (3) ANCS).

In the event of reasonable suspicion that an essential entity, by its actions or omissions, may violate ANCS, the competent authority may issue a warning specifying such actions or omissions and the measures that the entity shall take to prevent or cease the violation (Article 53 (4) ANCS).

Under Article 53 (5) (7) ANCS, the supervisory authority may also appoint a monitoring officer to supervise the performance of the obligations provided for in Chapter 3 ANCS (Obligations of the essential entities) from among the employees of its office for a specific time. The competencies of the officer are described in the new Article 53d of the amended ANCS.

It should also be noted that the essential entities are subject to a comprehensive system of ex ante (preventive) and ex post (follow-up) supervisions to ensure that they themselves and the services they provide meet the requirements provided for in the ANCS. The important entities are subject to a simplified system of supervision, which involves ex post supervision only, mainly because of the different role this group of entities plays in the cybersecurity system. The ex-post supervision is based on a reactive approach and may be triggered when there is a suspicion of a possible violation of ANCS. It should be noted that while important entities are subject to the same enforcement and supervision procedures that govern essential entities, these measures only apply ex post.

If, following a probe, a suspicion of a breach of personal data protection emerges, the supervisory authority must notify the President of the Office for Personal Data Protection of such suspicion. (Article 59a ANCS).

A regulation has also been introduced on cooperation of the supervisory authorities for cybersecurity with the authorities of other EU Member States in the scope of supervision of the entities that provide services in the territory of the Republic of Poland that have their headquarters in other countries or the other way around (Article 59b ANCS).

Moreover, the cybersecurity authorities may request the entities grouped in the national cybersecurity system to provide information on the ICT products, ICT services or ICT processes recalled thereby (Article 67d (2) ANCS).

3.4. GOVERNMENT REPRESENTATIVE FOR CYBERSECURITY

In accordance with the new regulations the Government Representative for Cybersecurity may be the Minister of Digitization, the Secretary of State or the Undersecretary of State at the Office of the Minister of Digitization (amended Article 61 (3) ANCS).

The competencies of the Representative will include the issuing of the recommendations specifying the technical and organizational measures applied to enhance the security of the information systems of the entities grouped in the national cybersecurity system. Th recommendations will be published on the sub-page of the Representative in the Public Information Bulletin (Article 67a (1-2) ANCS).

3.5. COMBINED CYBERSECURITY OPERATIONS CENTER

The Government Representative for Cybersecurity will set up a Combined Cybersecurity Operations Center (Polish acronym: "**PCOC**"), which will be an auxiliary body that will coordinate activities and implement the government policy to ensure cybersecurity (Article 62a ANCS). The PCOC will include representatives of certain key government institutions providing cybersecurity in Poland (which are listed under Article 62a (2) ANCS). Pursuant to Article 62a (6) (1-6), the PCOC's tasks will include:

- exchange of information on cyberthreats, incidents and vulnerabilities at the national level;

- exchange of information on the results of risk assessments of the revealed cyberthreats and incidents that have occurred;

- exchange of information on investigations regarding computer devices or software (run under Article 33 (1) ANCS)

- unanimous designation of the role of the CSIRT for incidents the handling of which requires the actions of several CSIRT teams, except in cases of critical incidents;

- exchange of information on cyber emergencies;

- preparation of up-to-date information on the situation in cyberspace for the Government Representative for Cybersecurity.

3.6. COUNCIL FOR CYBERSECURITY AFFAIRS

The draft amended ANCS expands the composition of the Council for Cybersecurity Affairs, the scope of its tasks and clarifies certain issues related to its operation.

The proposed amendment provides for new types of analyses that may be commissioned to CSIRT MON, CSIRT NASK or CSIRT GOV, which will deal with the impact of specific ICT products, ICT services or ICT processes on the security of the services provided by specific entities, as well as the manner and extent to which the manufacturing and delivery procedures for the products, services and processes are supervised by the supplier. The analyses will be performed at the request of the Chairman of the College for Cybersecurity Affairs, and may be used as evidence in proceedings to recognize a supplier as a high-risk supplier, which may also be conducted *ex officio* by the Minister of Digitization (see: Point 3.1. hereof).

The catalogue of the tasks of the College for Cybersecurity Affairs has been expanded to include, among others, giving an opinion on the decision to recognize a hardware or software supplier as a high-risk supplier (Article 65 (8) ANCS).

3.7. COMPUTER SECURITY RESPONSE TEAMS (CSIRTs)

The tasks of CSIRTs were expanded and more precisely specified in NIS 2 Directive; this has been reflected in a new catalogue of the tasks in the amended ANCS. It should be noted that the CSIRT teams have already been performing some of these tasks, e.g., processing of forensic data under the existing regulations.

The proposed regulations give the Government Representative for Cybersecurity the right to request that a Polish CSIRT assists a cybersecurity authority of another national system.

CSIRT NASK will carry out the tasks of a coordinated disclosure of the vulnerabilities of ICT products or ICT services in the European Union (Article 26a (5) ANCS). To this end , it will receive reports of vulnerabilities, and then contact the manufacturers or suppliers of the products and services in question to determine the method and timetable to eliminate the vulnerability. It should be noted that the CSIRT will not have sovereign powers in this regard, and therefore the elimination of the vulnerability and the manner thereof will be up to the owner of the product or service in question, while the provisions of the law allow the CSIRT to issue a warning or request the Government Representative for Cybersecurity to issue recommendations not to use specific equipment (Article 32 (2) ANCS).

The issues related to the conduct of analyses by CSIRT have been clarified in the amended ANCS. In conducting the analysis, CSIRT MON, CSIRT NASK and CSIRT GOV, will not be bound by the provisions of the license agreements of the equipment and/or software at issue (Article 33 (1c) ANCS). CSIRT MON, CSIRT NASK, CSIRT GOV or sectoral CSIRTs may conduct security assessments of the information systems used by entities of the national cybersecurity system (Article 36a (1) ANCS). The assessment is to be agreed to by the relevant national-level CSIRTs.

A CSIRT team conducting a security assessment will receive two key competencies under Article 36b (4-5), which include:

- authorization to produce or obtain equipment or software adapted to commit specific criminal offences[8] in order to verify whether the assessed system is susceptible to this type of software;
- authorization to use the above-mentioned devices or programs, unlawfully access information by means of breaking or bypassing its electronic, magnetic, IT or other specific security – a CSIRT team will be able to access all or part of the assessed system.

A CSIRT team will not be allowed to use the information so obtained for the purpose of its other statutory tasks. In the event that during a security assessment the CSIRT discovers a vulnerability that may also appear in other information systems, it will be obliged, under Article 36c, to notify the Minister for Digitization and the Government Representative for Cybersecurity Affairs of such discovery.

[8] Those criminal offences include, among others, unlawful obtaining of information by means of surveillance devices; destroying or obstructing access to computer data. For a full list, see Articles 165 §1 (4), 267a §1 or §2 in conjunction with §1, 269§1 or §2, 269a of the Polish Criminal Code.

About us

We have set up a specialized law firm to help our clients protect their intangible assets and develop new business based on new technologies and data. Our goal is to provide complex, specialized support to our customers' key issues - we are constantly close to them, providing the most precise, clear, and business-oriented legal advice – always tailored to their business needs.

We rely on our many years of experience, gained in well recognized international law firms operating in Poland.

We offer legal support in adapting business practices to the requirements of data security, personal data protection regulations, in particular in the context of the General Data Protection Regulation (GDPR), NIS/NIS2, DSA, DA, CER and other regulations.

More information:

Marcin Lewoszewski – Partner

Marcin.Lewoszewski@KLMLAW.PL

WWW.KLMLAW.PL

Anna Kobylańska

Marcin Lewoszewski

Arwid Mednis