Katarzyna Chałubińska-Jentkiewicz*
Monika Nowikowska**

Entities Involved in the Policy of Ensuring the Security of Network and Information Systems in the Light of the NIS 2 Directive (Part 1)

Abstract

The number, magnitude, sophistication, frequency and impact of incidents are increasing and present a major threat to the functioning of network and information systems. As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss and cause significant damage to the Union's economy and society. Therefore, effectiveness in cybersecurity is becoming increasingly vital for the proper functioning of the internal market. On December 14, 2022, the EU legislator adopted a directive on measures for a high common level of cybersecurity across the Union, called the NIS 2 Directive. The new NIS 2 directive aimed to lay down mechanisms for effective cooperation among the responsible authorities in each Member State and to update the list of sectors and activities subject to cybersecurity obligations. The article reviews the entities involved in the policy of ensuring the security of network and information systems in the light of the NIS 2 directive.

Key words: cybersecurity, incident, ENISA, essential entities, important entities

* Assoc. Prof. Katarzyna Chałubińska-Jentkiewicz, PhD, War Studies University, Faculty of Law and Administration, e-mail: kasiachalubinska@gmail.com, ORCID:0000-0003-0188-5704.
** Monika Nowikowska, PhD, War Studies University, Faculty of Law and Administration, e-mail: monika.nowikowska@gmail.com, ORCID:0000-0001-5166-8375.

Introduction

On December 14, 2022, the EU legislator adopted a Directive on measures for a high common level of cybersecurity across the Union called the NIS 2 Directive[1] and repealing Directive (EU) 2016/1148[2]. Recital 1 of the preamble indicates that Directive 2016/1148 aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security. As a result of adopting the Directive, significant progress has been made in increasing the Union's level of cyber resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mindset. That Directive has ensured the completion of national frameworks on the security of network and information systems by establishing national strategies on the security of network and information systems. Directive 2016/1148 has also contributed to cooperation at Union level through the establishment of the Cooperation Group and the network of national computer security incident response teams. Notwithstanding those achievements, the review of Directive 2016/1148 has revealed inherent shortcomings. These prevent it from addressing effectively current and emerging cybersecurity challenges. This necessitated the enactment and adoption of a new directive.

The EU legislator concluded that the identified divergences lead *de facto* to the fragmentation of the internal market, which may have a prejudicial effect on the cross-border provision of services and level of cyber resilience due to the application of different measures. Eventually, these divergences may even lead to a greater vulnerability of some Member States to cyberthreats. The new Directive aimed to remove such wide divergences among Member States. In particular, by laying down mechanisms for effective cooperation among the responsible authorities in each Member State and updating the list of sectors

1 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Official Journal of the European Union 2022, L 333/80) – hereinafter referred to as: Directive (EU) 2022/2555 or NIS 2 Directive.

2 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security for network and information systems across the Union (NIS Directive) (ibidem 2016, L 194/1).

and activities subject to cybersecurity obligations. With the repeal of Directive 2016/1148, the decision was taken to extend the scope of application by sectors to a larger part of the economy to provide comprehensive coverage of sectors and services of vital importance to key societal and economic activities in the internal market. One of the main changes was eliminating the distinction used in Directive 2016/1148 between operators of essential services and digital service providers. This division did not reflect the importance of particular sectors or services for social and economic activities in the internal market. In addition, under Directive 2016/1148, Member States were responsible for identifying the entities which met the criteria to qualify as operators of essential services. To eliminate the identified discrepancies between Member States and to provide legal certainty to all regulated entities concerning measures for cybersecurity risk management and incident reporting obligations, the legislator introduced a uniform criterion for determining which entities fall within the scope of the new directive. It was decided to adopt a new division into essential entities and important entities. This depends on how fundamental they are to their sectors, the type of services they provide, and their size. These entities have been placed within the scope of the NIS 2 to ensure effective compliance with cybersecurity risk management measures and incident reporting obligations.

As regards engagement in assuring a high level of cybersecurity, an analysis of the provisions of the NIS 2 Directive allows the following categories of entities to be distinguished: „essential entities, important entities, critical entities, domain name registries, competent authorities, cyber crisis management authority, single point of contact on cybersecurity, computer security incident response teams (CSIRTs), ENISA, the Cooperation Group”[3]. Further discussion should begin with a detailed analysis of the individual entities and their structuring. Due to the comprehensiveness of the subject matter addressed, the Authors decided to divide the article into two parts. The first part analyses such concepts as essential entities, important entities, critical entities and domain name registries.

3 C. Banasiński, W. Nowak, *Europejski i krajowy system cyberbezpieczeństwa* [in:] *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018 p. 161–162; M. Nowikowska, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, ed. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, Art. 26.

Essential entities

Article 3 NIS 2 identifies the entities the Directive applies to, dividing them into essential and important entities. Essential entities are those referred to in Annex I exceeding the ceilings for medium-sized enterprises provided for in Art. 2(1) of the Annex to Recommendation 2003/361/EC. Annex I indicates the types of essential entities by sector and subsector. Eleven sectors are listed, including: a) energy (subsector: electricity, oil, gas, hydrogen, district heating or cooling), b) transport (subsector: air, rail, water, road), c) banking, d) financial markets infrastructure, e) health, f) drinking water, g) wastewater, h) digital infrastructure, i) ICT service management (business-to-business), j) public administration, k) space.

As a condition for being considered an essential entity, in addition to being classified in one of the sectors, there is a requirement to exceed the ceilings for medium-sized enterprises provided for in Art. 2(1) of the Annex to Recommendation 2003/361/EC[4]. Article 2 of the Annex defines the staff headcount and financial ceilings determining enterprise categories. The category of micro, small and medium-sized enterprises (SMEs) is made up of those which employ fewer than 250 persons. They have an annual turnover not exceeding EUR 50 million and/or an annual balance sheet total not exceeding EUR 43 million. NIS 2 Directive has, therefore, introduced the „size-cap" rule (recital 7). This means all companies complying with Commission Recommendation 2003/361 requirements fall within the scope of the Directive. This means that authorities competent for security will not determine, by administrative decision, the entities that fall under the Directive. All entities that are large and medium-sized enterprises will automatically be within the scope of application of the NIS 2[5].

Article 3(1)(b–g) lists the entities given the status of essential entities by the legislator. These include: 1) qualified trust service providers and top-level domain name registries and DNS service providers, regardless of their size, 2) providers of public electronic communications networks or publicly

4 Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422) (Official Journal of the European Union 2003, L 124).

5 M. Wrzosek, *Dyrektywa w sprawie odporności podmiotów krytycznych i Dyrektywa NIS 2 – nowe wyzwania dla operatorów w zakresie cyberbezpieczeństwa*, „Nowa Energia" 2021, no. 5–6, p. 66.

available electronic communications services which qualify as SMEs, 3) public administration defined by the Member State at the central government level which, according to a risk-based assessment, provides services where the disruption could have a significant impact on critical societal or economic activities, 4) any other entities qualified in one of the sectors identified by a Member State as essential, 5) entities identified as critical entities under Directive 2022/2557[6] (the RCE Directive), regardless of size, 6) if the Member State so provides, entities that the Member State identified before 16 January 2023 as operators of essential services under the former Directive 2016/1148.

Within the essential entities, two additional categories of entities are listed. These are critical entities and top-level domain name registries plus DNS service providers.

Critical entities

Critical entities, as providers of essential services, play a very important role in maintaining essential societal functions and vital economic activities in the internal market. In the opinion of the EU legislator, to achieve a high level of resilience, Member States should identify critical entities which will be subject to specific requirements and supervision and which will receive specific support and guidance when all relevant risks occur. Article 2(1) of the NIS 2 defines the term „critical entity". A critical entity is defined as a public or private entity identified by a Member State. The procedure for qualifying an entity as a critical entity is set out in Art. 6 of Directive 2022/2557. Each Member State is required to identify critical actors for the sectors and subsectors identified in the Annex. Sectors and subsectors include: 1) energy (sub-sector: electricity, oil, gas, hydrogen, district heating or cooling), 2) transport (sub-sector: air, rail, water, road, public), 3) banking, 4) financial markets infrastructure, 5) health, 6) drinking water, 7) wastewater, 8) digital infrastructure, 9) public administration, 10) space, 11) food production, processing and distribution.

In identifying critical entities, the Member State shall take into account the results of its Member State risk assessment and strategy and shall apply all of the following criteria together: a) the entity provides one or more essential

6 Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Official Journal of the European Union 2022, L 333/164).

services, b) the entity operates, and its critical infrastructure is located, on the territory of that Member State, and c) an incident would have significant disruptive effects on the provision by the entity of one or more essential services or on the provision of other essential services. This means that identifying critical entities must be preceded by a risk assessment carried out separately by each Member State[7]. Each Member State shall establish a list of identified critical entities and notify within one month of classifying the entity as critical. In addition, Member States shall inform these entities of their obligations.

Similar to the NIS 2 Directive, the RCE Directive uses new terms, i.e., critical entities, departing from the previously used term „operators of critical infrastructure". In addition, the procedure for classifying an entity as a critical entity includes the same subsectors as the NIS 2 proposal, broadening and unifying the scope of the RCE[8].

Top-level domain name registries and DNS service providers

Recital 32 of the NIS 2 Directive states that „Upholding and preserving a reliable, resilient and secure domain name system (DNS) are key factors in maintaining the integrity of the internet and are essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to top-level-domain (TLD) name registries, and DNS service providers that are to be understood as entities providing publicly available recursive domain name resolution services for internet end-users or authoritative domain name resolution services for third-party usage". Analysing this recital, it can be pointed out that the EU legislator sees the need to regulate domain registration. Given their cross-border nature, DNS service providers and TLD name registries should be subject to a high degree of harmonisation at the EU level. Recital 109 further states that „Maintaining accurate and complete databases of domain name registration data (WHOIS data) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common

7 R. Wróbel, *Budowa i wzmacnianie odporności podmiotów krytycznych w Polsce*, „Zeszyty Naukowe Pro Publico Bono" 2022, no. 1, p. 168.
8 M. Wrzosek, op. cit., p. 66.

level of cybersecurity across the Union. For that specific purpose, TLD name registries and entities providing domain name registration services should be required to process certain data necessary to achieve that purpose. Such processing should constitute a legal obligation within the meaning of Article 6(1)(c) of Regulation (EU) 2016/679[9]". That obligation is without prejudice to the possibility to collect domain name registration data for other purposes, for example, on the basis of contractual arrangements or legal requirements established in other Union or national law. That obligation aims to achieve a complete and accurate set of registration data and should not result in collecting the same data multiple times. The TLD name registries and the entities providing domain name registration services should cooperate with each other in order to avoid the duplication of that task[10].

In addition, the Union legislature points out in recital 110 that „The availability and timely accessibility of domain name registration data to legitimate access seekers is essential for the prevention and combating of DNS abuse, and for the prevention and detection of and response to incidents"[11].

According to these principles, legitimate access seekers are to be understood as 1) any natural or legal person making a request pursuant to Union or national law, 2) any authorities that are competent under this Directive and those that are competent under Union or national law for the prevention, investigation, detection or prosecution of criminal offences, and CERTs or CSIRTs. TLD name registries and entities providing domain name registration services should be required to enable lawful access to specific domain name registration data, which are necessary for the purposes of the access request, to legitimate access seekers in accordance with Union and national law. The request of legitimate access seekers should be accompanied by a statement of reasons permitting the assessment of the necessity of access

9 Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the European Union 2016, L 119/6).

10 See K. Chałubińska-Jentkiewicz, M. Nowikowska, *Ochrona danych osobowych w cyberprzestrzeni*, Warszawa 2021, p. 55; J. Taczkowska-Olszewska, K. Chałubińska-Jentkiewicz, M. Nowikowska, *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019, p. 146; J. Taczkowska-Olszewska, *Ogólne rozporządzenie o ochronie danych osobowych RODO* [in:] eadem, M. Nowikowska, *Informacja publiczne. Informacje niejawne. Ochrona danych osobowych*, Warszawa 2019, p. 241.

11 Directive (EU) 2022/2557 of 14 December 2022...

to the data. It seems that the three above-mentioned issues determined the need to regulate domain registration in the NIS-2 Directive. These include a) upholding and preserving a reliable, resilient and secure domain name system (DNS), b) accurate and complete databases of domain name registration data, and c) availability and timely accessibility of domain name registration data.

Recital 18 in the preamble to the Directive NIS-2 states that „in order to ensure a clear overview of the entities falling within the scope of this Directive, Member States should establish a list of essential and important entities as well as entities providing domain name registration services"[12]. For that purpose, Member States should require entities to submit at least the following information to the competent authorities, namely, the name, address and up-to-date contact details, including the email addresses, IP ranges and telephone numbers of the entity and, where applicable, the relevant sector and subsector referred to in the annexes, as well as, where applicable, a list of the Member States where they provide services falling within the scope of this directive. To that end, the Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA)[13], should, without undue delay, provide guidelines and templates regarding the obligation to submit information. To facilitate the establishing and updating of the list of essential and important entities as well as entities providing domain name registration services, Member States should be able to establish national mechanisms for entities to register themselves. Where registers exist at the national level, Member States can decide on the appropriate mechanisms that allow for the identification of entities falling within the scope of this Directive[14].

An analysis of the provisions of the NIS 2 Directive makes it possible to identify the entities in the domain name registration system. The registration of domain names involves the registrants, the registrars, the registries and other companies and organisations that provide infrastructure to the public DNS. However, the DNS ecosystem is not limited to these organisations. Other entities also have a stake in domain name registration, including intellectual

12 Ibidem.

13 For more details see: M. Nowikowska, *Cooperation Mechanisms to Ensure the Security of Network and Information Systems in the Light of the NIS Directive* [in:] *The Role of Cybersecurity in the Public Sphere – The European Dimension*, eds. K. Chałubińska-Jentkiewicz, I. Hoffman, Maribor 2022, p. 90.

14 K. Chałubińska-Jentkiewicz, M. Nowikowska, *Entities in the Domain Name Registration System in Poland in the Light of the Provision of the NIS 2 Directive*, „Cybersecurity and Law" 2023, no. 2, p. 10–11.

property holders, researchers, practitioners, law enforcement authorities or brand protection companies. The DNS ecosystem in Poland consists of various stakeholders in several different roles[15].

Those registrants of domain names may include individuals, businesses, public sector entities or other organisations. The registration process involves a business relationship between registrants and registrars. These are accredited organisations acting as the retail channel for domain name registration. In Art. 6, the EU legislator adopted the basic definitions: domain name system, DNS service provider, top-level domain name registry, entity providing domain name registration services, and representative.

Domain name system or DNS means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and online connectivity services to get access to those services and resources.

A DNS service provider is an entity that provides a) publicly available recursive domain name resolution services for internet end-users or b) authoritative domain name resolution services for third-party use, except for root name servers.

Top-level domain name registry or TLD name registry means an entity which has been delegated a specific TLD and is responsible for administering the TLD, including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use.

An entity providing domain name registration services means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller.

Representative means a natural or legal person established in the Union explicitly designated to act on behalf of a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service

15 M. McFadden, E. Kantas, *DNS Identity Verification and Authentication of Domain Name Owners*, Athens 2023, p. 49.

provider, or a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the Union, which may be addressed by a competent authority or a CSIRT in the place of the entity itself with regard to the obligations of that entity under this Directive.

The primary entity in the registration system is the registrant. A domain name registrar is an individual or entity that registers a domain name. When the registrant registers a domain name, they enter into a contractual relationship with a registrar. The contract describes the terms under which the registrar agrees to register and maintain the requested domain name. Once the domain name is initially registered, registrants manage their domain name and its configuration through tools provided by the registrar.

The second key entity is the registrar. A registrar is an organisation that allows individuals and entities (registrants) to register domain names. During the registration process, the registrar verifies whether the requested domain name meets the policy of the registry operator and then submits the name and other required information to the registry operator. Registrars also are required to collect information from registrants and make that information public. After registration, registrants can update their domain name configuration through tools provided by the registrar. Registrars can sell domain names for many TLDs and have contractual arrangements with each TLD[16].

Finally, the registration process consists of a registry operator (TLD name registry). A registry operator is a company that keeps an authoritative database of the domain names registered in a TLD. Each TLD in the DNS is associated with a registry that contains a record for every domain name that exists in its domain. The DNS uses the TLD registry to obtain the names of the authoritative name servers for all the domain names registered in that TLD.

The relationship between the registrant and the registrar is a contractual offer of services by the registrar to the registrant. The business process that makes those services work includes using an account created at initial domain name registration. The account is a service provided by the register for ongoing management of the domain name and its associated records[17].

16 S. Krasuski, A. Wolska-Bagińska, O. Zinkiewicz-Będźmirowska, *Działania naruszające prawa do domen internetowych*, Warszawa 2021, p. 36.

17 K. Chałubińska-Jentkiewicz, M. Nowikowska, *Entities in the Domain…*, p. 14; J. Ożegalska-Trybalska, *Znaki towarowe a domeny internetowe* [in:] *System Prawa Prywatnego*, vol. 14C, *Prawo własności przemysłowej*, ed. R. Skubisz, Warszawa 2017, p. 698; A. Piechocki, *Wielostronne relacje prawne związane z rejestracją i utrzymywaniem nazwy domeny internetowej* [in:] *Domeny internetowe. Teoria i praktyka*, ed. I. Matusiak, Warszawa 2020, p. 57.

The entire domain registration process is based on mutual trust. A trust framework is a set of rules and policies that govern the relationships between the key participants in domain name registration. Those rules and policies include: 1) conducting identity management responsibilities, 2) sharing identity information, 3) using identity information that has been shared with them, 4) protecting and securing identity information, 5) performing specific roles within the federation, 6) managing liability and legal issues.

In the trust model: a) registrants entrust registrars with personal details, including personal, technical, billing, and payment information. Registrants trust that needed and appropriate information will be forwarded to registries to complete the domain name registration process, b) registrants trust and verify registration data needed for both use by the registrar and the data to complete the domain name registration with the registry. Registries verify and then trust payment information from the registrant, c) registrants trust registries to accurately publish information needed for a chosen domain name to appear active in the DNS with appropriate configuration and security information, as supplied by both the registrant and registrar[18].

In the process of trust, the most critical link is to receive accurate data. It is, therefore, important to introduce registrant verification mechanisms. Verification is the process of establishing an initial digital identity to register a domain name. For several countries in Europe, a system of national digital identities is in place. In some cases, that identity is a natural, verified one, meeting the needs of the registration ecosystem and also addressing requirements laid down in NIS-2. In Estonia, local registrants use national eIDs to carry out registration at the ccTLD21. Third-party identity assessment can be based on a large variety of documentation, including government ID, driving licence, passport, credit card, and company ID[19].

Domain name registration results in the creation of databases. The rules concerning the database of domain name registration data are set out in Art. 28 of the NIS 2 Directive. According to that provision, for the purpose of contributing to the security, stability and resilience of the DNS, Member States shall require TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in

18 *DNS Identity Verification and Authentication*..., p. 13.
19 Ibidem, p. 30.

accordance with Union data protection law as regards data which are personal data. Member States shall require the database of domain name registration data to contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. Such information shall include: a) the domain name, b) the date of registration, c) the registrant's name, contact email address and telephone number, d) the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.

Member States shall require the TLD name registries and the entities providing domain name registration services to have policies and procedures, including verification procedures, in place to ensure that the databases include accurate and complete information. Member States shall require such policies and procedures to be made publicly available. Member States shall require the TLD name registries and the entities providing domain name registration services to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.

A significant element is the sharing of data with authorised entities. Member States shall require the TLD name registries and the entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers in accordance with Union data protection law. Member States shall require the TLD name registries and the entities providing domain name registration services to reply without undue delay and, in any event, within 72 hours of receipt of any requests for access. Member States shall require policies and procedures regarding the disclosure of such data to be made publicly available.

To summarise the above, it can be noted that the registration of domain names involves the registrants, the registrars, the registries and other companies and organisations that provide infrastructure to the public DNS. These entities are defined by the EU legislator in the NIS Directive. Domain names and the Domain Name System are at the heart of the modern Internet. The ability to transform a human-readable string of characters into an Internet Protocol address is fundamental to services and applications that billions of people take for granted. The DNS is also an integral part of reducing spam and locating other services on the Internet. As part of this process, the domain name registrant enters into an agreement with the registrar,

which includes a requirement for accurate information. The registrar is responsible for establishing verification procedures, ensuring the information collected is accurate and complete, and implementing strong authentication controls to guarantee the protection of the accounts related to the domain names. Protecting the participants in that ecosystem starts with resilient authentication of potential registrants. Without strong authentication, there are risks to intellectual property, the ability of legitimate law enforcement authorities to investigate crimes, and an enterprise's identity and presence on the Internet. The EU legislator sees the need to regulate the registration process of domain names. Upholding and preserving a reliable, resilient and secure domain name system (DNS) are key factors in maintaining the integrity of the Internet and are essential for its continuous and stable operation, on which the digital economy and society depend[20].

Important entities

Pursuant to Art. 3(3) of the NIS 2, Member States are required, by 17 April 2025, to prepare a list of essential and important entities and entities providing domain name registration services. These lists shall include the following data: the name of the entity, the address and up-to-date contact details, including email addresses, IP ranges and telephone numbers, the name of the relevant sector and subsector, a list of the Member States where they provide services falling within the scope of NIS 2.

Depending on the size of the entity and the sector in which it operates, i.e., the importance of the sector in question for the smooth economic and social functioning of the Union, it will be classified either as an essential or important entity. The EU legislator has applied a new way of determining whether an entity is covered by the NIS 2 Directive and should comply with the obligations set out therein. This is because NIS 2 adopts the general principle of self-assessment. The entities will be responsible for assessing whether they are an essential or important entity based on the criteria indicated in the NIS 2 Directive.

It should be noted that important entities are a new category introduced in the NIS 2 Directive. The *ratio legis* of the introduction of this category

20 K. Chałubińska-Jentkiewicz, M. Nowikowska, *Entities in the Domain…*, p. 17.

stems from the need to consider entities that do not meet the strict criteria of essential entities but whose activities significantly impact the functioning of the Union society and economy. This is because these entities rely heavily on the security of networks and information systems. According to NIS 2, important entities are medium-sized entities operating in the indicated sectors of high criticality and medium-sized or large entities operating in other critical sectors, as defined in Annex II of NIS 2, i.e., postal and courier services, waste management, manufacture, production and distribution of chemicals, production, processing and distribution of food (broadly-defined) manufacturing, digital service providers and research.

It should be highlighted that the sectors indicated in the Annex are listed very broadly. The division into essential and important entities may seem unintuitive. After all, important entities do not only operate in „other critical sectors" but also in „sectors of high criticality". The source literature points out that this linguistic inconsistency is due to the Polish translation of the NIS 2, where the two categories of sectors („kluczowe" – essential, and „ważne" – important) have names identical to the two categories of entities (essential and important entities). In the English version of the NIS 2, sectors are respectively named „sectors of high criticality and other critical sectors, while entities are divided into essential entities and important entities"[21].

Conclusion

One of the main reasons justifying the need for the new NIS 2 Directive – which significantly modifies the existing solutions – was the divergent regulations of the obligations of entities providing services or carrying out critical activities in different countries. The cybersecurity requirements imposed on these entities varied considerably in terms of type and level of detail and the method of supervision – depending on the Member State. Those disparities entailed additional costs and created difficulties for entities that offered goods or services across borders[22]. The different approaches in the design of

21 K. Basaj, A. Wachowska, *Dyrektywa NIS 2: kogo obejmą nowe przepisy – podmioty kluczowe i ważne*, https://www.traple.pl/dyrektywa-nis-2-kogo-obejma-nowe-przepisy-podmioty-kluczowe-i-wazne/ [access: 21.02.2024].

22 K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2023, s. 296; *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, ed. A. Besiekierska, Warszawa 2019.

cybersecurity requirements also had a negative impact on the overall level of cybersecurity. The reason was that it was left to the discretion of Member States to adopt systemic solutions. This is because Directive 2016/1148 provided the Member States with a wide margin of freedom regarding the implementation of the security and incident reporting obligations laid down. Those obligations were, therefore, implemented at the national level in significantly different ways and imposed on different entities.

The number, magnitude, sophistication, frequency and impact of incidents are increasing and present a major threat to the functioning of network and information systems. As a result, such incidents can impede the pursuit of economic activities in the internal market, generate financial loss and cause significant damage to the Union's economy and society. Therefore, cybersecurity effectiveness is becoming increasingly essential for the proper functioning of the internal market. The EU legislator decided to clearly define the entities involved in the policy of ensuring the security of network and information systems and to define the rules for international and national cooperation.

Bibliography

Banasiński C., Nowak W., *Europejski i krajowy system cyberbezpieczeństwa* [in:] *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.

Basaj K., Wachowska A., *Dyrektywa NIS 2: kogo obejmą nowe przepisy – podmioty kluczowe i ważne*, https://www.traple.pl/dyrektywa-nis-2-kogo-obejma-nowe-przepisy-podmioty-kluczowe-i-wazne/ [access: 21.02.2024].

Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2023.

Chałubińska-Jentkiewicz K., Nowikowska M., *Entities in the Domain Name Registration System in Poland in the Light of the Provision of the NIS 2 Directive*, „Cybersecurity and Law" 2023, no. 2.

Chałubińska-Jentkiewicz K., Nowikowska M., *Ochrona danych osobowych w cyberprzestrzeni*, Warszawa 2021.

Krasuski S., Wolska-Bagińska A., Zinkiewicz-Będźmirowska O., *Działania naruszające prawa do domen internetowych*, Warszawa 2021.

McFadden M., Kantas E., *DNS Identity Verification and Authentication of Domain Name Owners*, Athens 2023.

Nowikowska M. [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, ed. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, Art. 26.

Nowikowska M., *Cooperation Mechanisms to Ensure the Security of Network and Information Systems in the Light of the NIS Directive* [in:] *The Role of Cybersecurity in the Public Sphere – The European Dimension*, eds. K. Chałubińska-Jentkiewicz, I. Hoffman, Maribor 2022.

Ożegalska-Trybalska J., *Znaki towarowe a domeny internetowe* [in:] *System Prawa Prywatnego*, vol. 14C, *Prawo własności przemysłowej* ed. R. Skubisz, Warszawa 2017.

Piechocki A., *Wielostronne relacje prawne związane z rejestracją i utrzymywaniem nazwy domeny internetowej* [in:] *Domeny internetowe. Teoria i praktyka*, ed. I. Matusiak, Warszawa 2020.

Taczkowska-Olszewska J., *Ogólne rozporządzenie o ochronie danych osobowych RODO* [in:] J. Taczkowska-Olszewska, M. Nowikowska, *Informacja publiczne. Informacje niejawne. Ochrona danych osobowych*, Warszawa 2019.

Taczkowska-Olszewska J., Chałubińska-Jentkiewicz K., Nowikowska M., *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019.

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, ed. A. Besiekierska, Warszawa 2019.

Wróbel R., *Budowa i wzmacnianie odporności podmiotów krytycznych w Polsce*, „Zeszyty Naukowe Pro Publico Bono" 2022, no. 1.

Podmioty zaangażowane w politykę zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS 2 (cz. 1)

Streszczenie

Liczba, skala, zaawansowanie, częstotliwość i skutki incydentów wzrastają i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. W rezultacie zdarzenia te mogą utrudniać prowadzenie działalności na rynku wewnętrznym, powodować straty finansowe oraz poważne szkody dla gospodarki i społeczeństwa Unii. Dlatego skuteczność w obszarze cyberbezpieczeństwa staje się coraz ważniejsza dla prawidłowego funkcjonowania rynku wewnętrznego. 14 grudnia 2022 roku ustawodawca unijny przyjął dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zwaną dyrektywą NIS 2. Jej celem było ustanowienie mechanizmów skutecznej współpracy między odpowiedzialnymi organami w poszczególnych państwach członkowskich oraz aktualizacja listy sektorów i działań podlegających obowiązkom w zakresie cyberbezpieczeństwa. W artykule dokonano analizy podmiotów zajmujących się polityką zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS 2.

Słowa kluczowe: cyberbezpieczeństwo, incydent, ENISA, kluczowe podmioty, ważne podmioty