Katarzyna Chałubińska-Jentkiewicz*
Monika Nowikowska**

Entities in the domain name registration system in Poland in the light of the provision of the NIS-2 directive

Abstract

The article aims to analyze the entities in the domain name registration system in Poland in the light of the provisions of the NIS-2 Directive. The European Union NIS-2 Directive replaces the original network and information systems (NIS Directive) from 2016, to account for the changing character of the digital society and the increased need for improved cybersecurity. Quoting the directive: „The NIS Directive is not sufciently clear when it comes to the scope for operators of essential services and its provisions do not provide sufcient clarity regarding national competence over digital service providers". The legislation also imposes specific obligations on providers of DNS services in the EU, including registries and registrars, to maintain complete and accurate registration data and share this data in a timely manner to „legitimate access seekers"[1]. The article attempts to determine the entities involved in the domain name registration system and the mutual correlations.

Key words: domain, DNS, databases, registry, registrant, registrar

* 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: m.nowikowska@akademia.mil.pl, ORCID:0000-0001-5166-8375.
1 D. Clark, *The EU NIS-2 proposal and the DNS*, https://www.caida.org/catalog/papers/2022_eu_nis_2_proposal/eu_nis_2_proposal.pdf [access: 21.06.2023].

Introduction

This paper is concerned with the issues of domain name regulation and entities involved in this proces. The issue of domain registration is included in the provisions of the NIS2 Directive[2]. The Network and Information Security (NIS) Directive[3] was the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States[4]. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market. To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by NIS-2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term[5].

Recital 32 in the preamble to the Directive NIS-2 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

2 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.

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

4 See more: M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, ibidem 2019, no. 2; M. Karpiuk, *The Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, no. 2; M. Karpiuk, *Activities of the local government units in the field of telecommunications*, „Cybersecurity and Law" 2019, no. 1; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, ibidem 2021, no. 2; M. Karpiuk, *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 2.

5 *Dyrektywa NIS2: wspólny wysoki poziom cyberbezpieczeństwa w UE*, https://www.europarl.europa.eu/thinktank/EPRS_BRI(2021)689333 [access: 19.06.2023].

society depend"[6]. 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.

Analyzing that recital, it can be pointed out that the EU legislator sees the need to regulate the issue of domain registration. Taking account of their cross-border nature, DNS service provider and TLD name registries should be subject to a high degree of harmonisation at Union 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 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 Art. 6(1), point (c), of Regulation (EU) 2016/679[7]. 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[8]. 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.

In addition, the Union legislature points out in recital 110 that „The availability and timely accessibility of domain name registration data to

6 Directive (EU) 2022/2555..., recital 32.

7 Regulation (EU) 2016/679 of the European Parliament and of the Council 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 119/1.

8 K. Chałubińska-Jentkiewicz, M. Nowikowska, *Ochrona danych osobowych w cyberprzestrzeni*, Warszawa 2020, p. 34; 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* [w:] eadem, M. Nowikowska, *Informacje publiczne. Informacje niejawne. Ochrona danych osobowych*, Warszawa 2019, p. 241.

legitimate access seekers is essential for the prevention and combating of DNS abuse, and for the prevention and detection of and response to incidents"[9].

According to this 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 to the data[10].

It seems that the three above-mentioned issues determined the need to regulate the issue of domain registration in the NIS-2 Directive. These include: 1) upholding and preserving a reliable, resilient and secure domain name system (DNS); 2) accurate and complete databases of domain name registration data; 3) availability and timely accessibility of domain name registration data.

List of entities providing domain name registration services

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"[11]. 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

9 Directive (EU) 2022/2555..., recital 110.
10 K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2016, p. 104–105.
11 Directive (EU) 2022/2555..., recital 18.

Directive[12]. To that end, the Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA), 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 national level, Member States can decide on the appropriate mechanisms that allow for the identification of entities falling within the scope of this Directive.

Entities in the domain name registration system in Poland in the light of the provisions of the NIS-2 Directive

The registration of domain names involves the registrants, the registrars, the registries and other companies and organizations that provide infrastructure to the public DNS. However, the DNS ecosystem is not limited to these organizations. Others have a stake in domain name registration including intellectual property holders, researchers, practitioners, law enforcement agencies or brand protection companies[13].

The DNS ecosystem in Poland consists of a variety of stakeholders in several different roles. Those registering domain names can be individuals, businesses, public sector entities or other organizations. The process of registration involves a business relationship between registrants and registrars, which are accredited organizations that act as the retail channel for domain name registration[14].

In Art. 6, the EU legislator adopted basic definitions of: domain name system, DNS service provider, top-level domain name registry, entity providing domain name registration services, representative.

Domain name system or DNS means a hierarchical distributed naming system which enables the identification of internet services and resources,

12 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.

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

14 Ibidem.

allowing end-user devices to use internet routing and connectivity services to reach those services and resources.

DNS service provider means 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, with the exception of 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.

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 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.

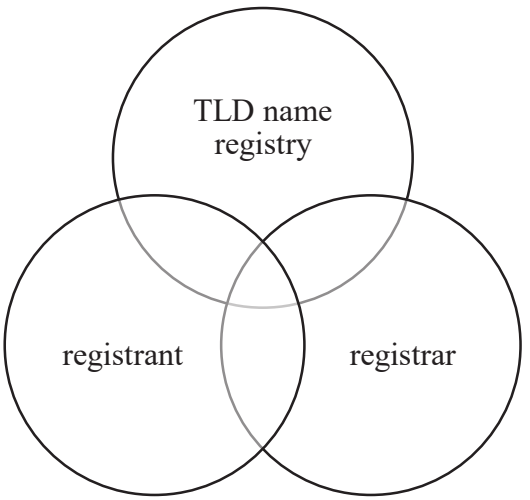
The primary entity in the registration system is the registrant. A domain name registrant is an individual or entity that registers a domain name. When the registrant registers a domain name, they enter into a contractual relationship with a registrar. The contract describes the terms under which the 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[15].

The second key entity is the registrar. A registrar is an organization that allows individuals and entities (registrants) to register domain names. During

15 Ibidem, p. 12.

the registration process, the registrar verifies that 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 form registrants and make that information available publicly. After registration, registrants can make updates to their domain name configuration through tools provided by the registrar. Registrars are able to sell domain names for many TLDs and have contractual arrangements with each of those TLDs[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[17].



Source: own elaboration.

Graph 1. Entities in the domain name registration system

16 S. Krasuski, A. Wolska-Bagińska, O. Zinkiewicz-Będźmirowska, *Działania naruszające prawa do domen internetowych*, Warszawa 2021, p. 36.
17 M. McFadden, E. Kantas, op. cit., p. 13.

The relationship between the registrant and registrar is a contractual offer of services by the registrar to the registrant[18]. 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.

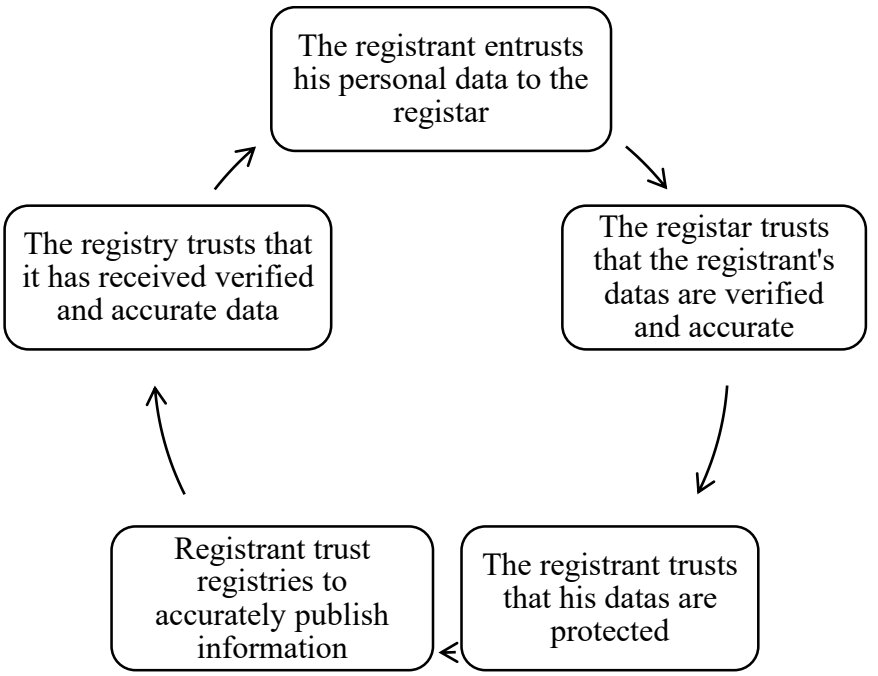
It should be emphasized that the entire domain registration process is based on mutual trust. A trust framework is a set of rules and policies that govern the relationships between the key participants in domain name registration. Those rules and policies include: 1) conducting identity management responsibilities; 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[19].

In the trust model: a) registrants trust 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 proces; b) registrants trust and verify registration data needed for both use by the registrar and the data needed 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[20].

18 See: J. Ożegalska-Trybalska, *Znaki towarowe a domeny internetowe* [in:] *Prawo własności przemysłowej. System prawa prywatnego*, vol. 14 C, 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.

19 M. McFadden, E. Kantas, op. cit., p. 17.

20 K. Mania, *Domena internetowa jako przedmiot polubownego rozstrzygania sporów*, Warszawa 2016, p. 39.



Source: own elaboration.

Grapf 2. Trust relationships in place during the initial registration of a domain name

In the process of trust, the most important 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 for the purposes of registering 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 that meets the needs of the registration ecosystem and also addresses requirements in NIS-2. In Estonia, local registrants use national eIDs to carry out registration at the ccTLD[21]. Third-party identity assessment can be based on a large variety of documentation including: government ID; driving licence; passport; credit card; company ID[22].

21 M. McFadden, E. Kantas, op. cit., p. 30.
22 Ibidem, p. 33.

Database of domain name registration data

The rules for the database on the registration of domain names are set out in Art. 28 of the NIS 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 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.

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 with regard to the disclosure of such data to be made publicly available.

Conclusion

The registration of domain names involves the registrants, the registrars, the registries and other companies and organizations 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 to ensure that the information collected is accurate and complete, as well as implementing strong authentication controls to guarantee the protection of the accounts related to the domain names[23].

Protecting the participants in that ecosystem starts with strong authentication of potential registrants. Without strong authentication, there are risks to intellectual property, the ability of legitimate law enforcement to investigate crimes, and an enterprise's identity and presence on the internet[24].

The EU legislator sees the need to regulate the process of registration 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.

Bibliography

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2016.

Chałubińska-Jentkiewicz K., Nowikowska M., *Ochrona danych osobowych w cyberprzestrzeni*, Warszawa 2020.

Clark D., *The EU NIS-2 proposal and the DNS*, https://www.caida.org/catalog/papers/2022_eu_nis_2_proposal/eu_nis_2_proposal.pdf [access: 21.06.2023].

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.

23 Ibidem, p. 5.
24 Ibidem, p. 49.

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.
Karpiuk M., *Activities of the local government units in the field of telecommunications*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 2.
Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.
Karpiuk M., *The Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, no. 2.
Krasuski S., Wolska-Bagińska A., Zinkiewicz-Będźmirowska O., *Działania naruszające prawa do domen internetowych*, Warszawa 2021.
Mania K., *Domena internetowa jako przedmiot polubownego rozstrzygania sporów*, Warszawa 2016.
McFadden M., Kantas E., *DNS Identity. Verification and Authentication of Domain Name Owners*, Ateny 2023.
Ożegalska-Trybalska J., *Znaki towarowe a domeny internetowe* [in:] *Prawo własności przemysłowej. System prawa prywatnego*, vol. 14 C, 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* [w:] J. Taczkowska-Olszewska, M. Nowikowska, *Informacje 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.

Podmioty w systemie rejestracji nazw domen w Polsce w świetle przepisów dyrektywny NIS-2

Streszczenie

Celem artykułu jest analiza kluczowych podmiotów biorących w systemie rejestracji domen w Polsce w świetle przepisów dyrektywy NIS-2. Dyrektywa Unii Europejskiej NIS-2 zastępuje pierwotne systemy sieciowe i informatyczne (dyrektywa w sprawie bezpieczeństwa sieci i informacji) z 2016 roku, żeby uwzględnić zmieniający się charakter społeczeństwa cyfrowego i zwiększoną potrzebę poprawy cyberbezpieczeństwa. Cytując dyrektywę, dyrektywa w sprawie bezpieczeństwa sieci i informacji nie jest wystarczająco jasna, jeżeli chodzi o zakres dla operatorów usług kluczowych, a jej przepisy nie zapewniają wystarczającej jasności w odniesieniu do kompetencji krajowych w zakresie dostawców usług cyfrowych. Przepisy dyrektywy NIS-2 nakładają również szczególne obowiązki na dostawców usług DNS w UE, w tym na rejestry i rejestratorów, w celu zachowania kompletnych i dokładnych danych rejestracyjnych oraz udostępniania tych danych w odpowiednim czasie „uprawnionym osobom ubiegającym się o dostęp". W artykule podjęto próbę określenia podmiotów biorących udział w systemie rejestracji nazwy domeny oraz występujących wzajemnych korelacji.

Słowa kluczowe: domena, DNS, bazy danych, rejestr, rejestrujący, rejestrator