What will be the final wording of the NIS 2 Directive?

Piotr Studziński-Raczyński
Senior DNS Specialist

How does the NIS 2 Directive differ from its predecessor? The Directive of the European Parliament and of the Council (EU) on measures for a high common level of cybersecurity across the Union, significantly extending the scope of entities previously covered, divides them into: essential entities and important entities. An important change is also the inclusion of the electronic communications sector in a single legal regime across the European Union. This seems to be a natural consequence of technological development, which has resulted in an increasing proportion of services provided electronically.

In relation to the consultations of the proposal for the NIS 2 Directive, which assumes an update of regulations concerning security of networks and information systems, conducted by the Chancellery of the Prime Minister, the Digital Council agrees in principle with the general direction of covering with the regulations the key sectors, including in particular the telecommunications sector and the public administration sector, which will make it possible to harmonise cyber security at both EU and national levels. The Council also notes that the proposed NIS 2 Directive should also be seen in the light of the new cyber security strategy „The EU's Cybersecurity Strategy for the Digital Decade", which includes an examination of the legislative solutions available to the EU for implementation. Such an examination would extend the EU capabilities, competences and resources and in consequence lead to achieve a satisfactory level of technological sovereignty.

The proposal for the NIS 2 Directive indicates in Recital 15 that maintaining a secure DNS system is essential to preserving the integrity and stability of the Internet. From the perspective of this assessment, it is also postulated that it is important to ensure up-to-date registrants' data („WHOIS data") and secure access to such data, which in turn translates into maintaining a high common level of cyber-security within the EU. Article 23 of the proposed NIS 2 Directive obliges Member States to ensure that data on domain name registrants is up-to-date and complete as well as collected and maintained by registries and registrars of TLDs with due diligence. By relating Article 23 to the above-mentioned idea of maintaining a high common level of cybersecurity in the EU, ensuring that the data on registrants is kept up-to-date and complete may have the influence, for example, on limiting the number of attacks using domain names to impersonate, for example, banks, energy providers or courier services.

On 3 May 2021, the European Parliament's Committee on Industry, Research and Energy (ITRE) issued a draft report on the proposal for the NIS 2 Directive. With regard to the obligation to maintain accurate registration data applicable to domain name registries and registrars, the draft report adds additional criteria to the obligation to collect „accurate and complete" registration data. According to the ITRE draft report, domain name registries and registrars should strive to ensure the integrity and availability of such data by implementing technical and organisational measures, such as a process for confirming registration data by registrants. Regarding access to such data, the draft report suggests that registries and registrars should respond to requests for access to registration data within 72 hours. The draft report also suggests including a definition of domain name registration services that covers services provided by domain name registries and registrars, privacy/proxy providers, domain name brokers or resellers and

any other services that are related to domain name registration. The ITRE draft report also specified that the relevant information that registries, registrars and other providers of domain name registration services collect and maintain as accurate, complete and verified should include at least the registrant's name, physical address, e-mail address as well as a phone number. The above would apply to both natural and legal persons' data. The ITRE draft report will be the cornerstone of Parliament's main line on the draft of the NIS 2 Directive. Particularly noteworthy in the draft report, with regard to ccTLDs, is the proposal for mandatory verification of registration data. According to rec. 59 of the report, verification processes should reflect current industry best practice (including the eID system).

On 3 June 2021, the European Commission presented its proposal for a regulation on European Digital Identity (EUID). The EUID proposal requires Member States to issue a European Digital Identity Wallet under a notified electronic identification system (National Electronic Identification Scheme), following a mandatory conformity assessment and voluntary certification under the European Cybersecurity Certification in accordance with the EU Cybersecurity Act. As the current eIDAS framework has not achieved its intended purpose of making cross-border eID schemes work in all Member States, the EUID proposal imposes a requirement on Member States to notify at least one eID scheme. To ensure that users can trace who is behind a website, the EUID proposal requires browser providers to facilitate the application of qualified certificates for the authentication of website. As regards the use of European Digital Identity Wallets by private parties, the consent of digital infrastructure providers is required for the use of such wallets to provide services for which strong user online authentication is required by national or EU law or by contractual obligation. The EC's EUID proposal is highly relevant in the context of the ongoing discussions on registration data under the proposal for the NIS 2 Directive and KYBC's obligation to „know your customer" in terms of the DSA (Digital Services Act) proposal, which may require registries to verify the registration data of domain name registrants. The EC's EUID proposal aims to ensure that all Member States have at least one functioning electronic identification system.

With regard to the aforementioned relationship of the proposal for the NIS 2 Directive with the objectives of the new cybersecurity strategy, it should be noted that on 10 June 2021, the European Parliament adopted a resolution on the EU cybersecurity strategy which calls, among others, for „a new robust security framework for EU critical infrastructures in order to safeguard EU security interests". The resolution calls on the European Commission to „prepare provisions to ensure the accessibility, availability and integrity of the public core of the internet and, therefore, the stability of cyber-space, particularly as regards the EU's access to the global DNS root system". The resolution also presents the proposal for a European Domain Name System (DNS4EU) as an element affecting the resilience of the Internet. It also asks the Commission to assess how DNS4EU could benefit from the new technologies, security protocols and cyber security know-how to provide all Europeans with a fast, secure and resilient DNS system. The resolution points out the need to better protect the BGP protocol and stresses that EU countries should accelerate the deployment of IPv6. It also promotes the open source model, which - often as a basis for the functioning of many branches of the Internet - has proven to be effective and efficient. In the context of the relationship described above, it should be remembered that although European Parliament resolutions are not binding legal instruments, they do provide general direction for Parliamentary action in various policy areas.

On 10 June 2021, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) issued a draft opinion on the proposal for a NIS 2 Directive. The draft opinion takes into account a number of recommendations made by the EDPS (European Data Protection Supervisor) on the EU Cybersecurity Strategy and the proposal for the NIS 2 Directive. With regard to the obligation of accuracy of registration data applying to

TLD registries and registrars, the draft opinion proposes changes to the categories of data to be published in respect of legal entities and limits the list of authorised entities seeking access to registrant's data to competent national authorities, including but not limited to law enforcement authorities, CERT/CSIRT teams and data protection authorities. The amendments proposed in the draft opinion, similarly to the ITRE report, also specify that relevant information collected by registries and registrars should include the name, physical address, email address and phone number of the domain name registrant. The amendments proposed in the LIBE Opinion appear to be among the more balanced ones as they attempt to address the concerns raised by the EDPS.

The Internal Market and Consumer Protection Committee of the European Parliament (IMCO) also presented its comments on the proposal for the NIS 2 Directive. On 14 July 2021, the members of the above mentioned committee adopted an opinion on the discussed directive. The IMCO opinion, like the ITRE report, proposes revisions to include in Article 23 privacy/proxy service providers, internet domain brokers or resellers and any other services that are related to domain name registration. Some amendments aim to further align the obligations on the accuracy of data collected with the GDPR. According to the IMCO Opinion, the data accuracy obligation in Article 23 should be extended to include an additional data verification obligation for relevant information necessary to identify and contact domain name registrants. According to the opinion, this relevant information should include at least the name of the registrant, the registrant's physical address, e-mail address and the registrant's phone number. With respect to providing access to domain name registration data to entitled access seekers, the IMCO opinion provides for an amendment obliging registries, registrars and other domain name registration service providers to respond to such authorities within 72 hours. It is worth noting that the amendments proposed by IMCO reflect the same approach as for ITRE.

And how does CENTR (*Council of European National Top-Level Domain Registries*) comment on the proposal for the NIS 2 Directive?

CENTR underlines that although maintaining a registration database is part of the responsibilities of ccTLD registries, WHOIS is not what constitutes a domain name system (DNS). The statement regarding the relationship between accurate and complete registration data and the security, stability and resilience of the DNS in Article 23 of the proposed NIS 2 Directive is, in CENTR's view, incorrect and does not reflect the reality of cyber threats targeting DNS infrastructure. According to CENTR, Article 23(2) should be amended to include relevant information to identify and contact domain name registrants and their TLD administrators. According to CENTR, such information should be limited to what is strictly necessary and appropriate under the relevant legal basis for the data processing as provided for by EU or Member States' law. Bearing in mind the provisions of Article 5 of the GDPR, Article 23 of the NIS 2 Directive should, according to CENTR, clearly indicate the purpose for which domain name registration data are processed by TLD registries and domain name registration service providers. With regard to paragraph 5 of the Article in question, CENTR shares the view of the LIBE Committee and IMCO and recommends that the list of authorised entities seeking access should be limited to competent national authorities, including national law enforcement bodies, provided that access to registration data is granted on the basis of an appropriate legal basis that fulfils the conditions set out in the EU data protection framework.