CMS | Romania publishes draft law on cybersecurity implementing the NIS2 Directive

On 15 August 2024, the National Cyber Security Directorate in Romania (DNSC) released for public debate the draft law establishing a framework for cybersecurity of networks and information systems in the national civil cyberspace (Draft Law), transposing Directive (EU) 2022/2555 on measures for a high common level of cyber security in the European Union (NIS 2 Directive), which amends Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repeals Directive (EU) 2016/1148.

While the draft law may undergo revisions before its final adoption, it outlines the fundamental measures needed to comply with the NIS 2 Directive. (The directive's transposition deadline is 17 October 2024, but because the draft law is in the early stages of the legislative process, this deadline will likely be missed).

Background

Currently, Romania's primary law on cybersecurity is Law No. 362/2018 on ensuring a high common level of security of networks and information systems (**Law 362**), which was intended to strengthen cybersecurity capabilities across the EU, mitigate threats to networks and information systems used to deliver essential services in key sectors and ensure the continuity of these services when faced with incidents, thus contributing to the security of the EU and the effective functioning of its economy and society. Law 362 transposed Directive (EU) 2016/1148, which is now repealed by the NIS 2 Directive.

At EU level, the review of Directive (EU) 2016/1148 revealed that it was not effective in addressing current and emerging challenges in cybersecurity. As a result, the NIS 2 Directive was enacted in order to better adapt the legislative framework to emerging cybersecurity threats.

In order to transpose the provisions of NIS 2 Directive into national law, it is necessary to amend the current legal framework.

What is new in the Draft Law compared to the current legal framework?

1. Enlarged scope of application

More companies and economic sectors are subject to the Draft Law and NIS 2 Directive than in the current legal framework.

The NIS 2 Directive and the Draft Law broaden the scope of the law's application from seven critical sectors as

provided in Law 362 (i.e. energy, transport, banking, financial market infrastructures, health, water supply and distribution of drinking water, digital infrastructure) to 18 sectors, with the addition of the following: waste water, ICT service management, public administration, space, postal and courier services, waste management, chemical manufacturing, production and distribution, food production, processing and distribution, manufacturing, digital providers and research.

The NIS 2 Directive divides sectors between those of high criticality (i.e. energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, ICT service management, public administration and space) and other critical sectors (i.e. postal and courier services, waste management, chemical manufacturing, production and distribution, food production, processing and distribution, manufacturing, digital providers and research).

The Draft Law makes the same classification, but separates the central public administration from the local public administration. The former is considered a sector of high criticality, while the latter falls under other critical sector.

The Draft Law distinguishes essential and important entities.

This distinction did not exist in Law 362, which distinguished between digital services providers and essential services providers. This, however, is now abandoned.

According to the Draft Law, essential entities include the following:

1. qualified trust service providers, top-level domain name registries, DNS service providers, central public administration entities, managed security service providers, entities identified by the competent authority responsible for cybersecurity as essential entities, entities identified as critical entities under the Law on the resilience of critical entities –regardless of their size.

2. providers of public electronic communications networks or of publicly available electronic communications services, which qualify as medium-sized enterprises;

3. large entities, which provide services in a sector of high criticality.

Important entities are those which were not considered essential and include the following:

1. medium-sized entities that provide services in a high critical sector or other critical sector;

2. large-sized entities that provide services in other critical sector;

3. local public administration entities;

4. trust service providers, regardless of their size;

5. providers of public electronic communications networks and providers of publicly available communications services, regardless of their size;

6. entities identified as important by the competent authority responsible for cybersecurity.

Entities will have to notify the DNSC if they identify as essential or important entities and follow the registration process in the entities registry.

It should be noted that some providers fall under the scope of the law regardless of their size.

Also, compared to the NIS 2 Directive, local public administration entities are included within the scope of the law and are considered important entities. This addition is allowed under the NIS 2 Directive.

The Draft Law further provides rules on establishing the size of an entity, as well as on territoriality, explaining when the law applies to foreign entities.

Why is the distinction important?

Both essential and important entities are generally required to comply with the same cybersecurity measures. The main differences, however, lie in their monitoring and the sanctioning regime set by Romania's cybersecurity authority the DNSC and in the sanctioning regime applicable to the entity.

Essential entities are subject to proactive monitoring by the DNSC, whereas important entities are monitored only after an incident occurs, primarily for the purpose of imposing sanctions.

Additionally, essential entities must undergo a cybersecurity audit every two years, while important entities are audited every three years. Importantly, the requirement that important entities must undergo regular audits is an addition provided in the Draft Law that is not mandated by the NIS 2 Directive.

Different sanctions may also apply based on whether an entity is classified as essential or important, reflecting the greater potential societal impact of disruptions to essential entities.

Another important consequence of this qualification is that, under the Draft Law and different from the NIS 2 Directive, essential entities of medium or large sizes and entities that are identified as critical entities under the Law on the resilience of critical entities are considered entities operating information and communication infrastructures of national interest (ICINs), as defined in Law 163/2021 on the adoption of measures relating to information and communication infrastructures of national interest and the conditions for the deployment of 5G networks. The Draft Law specifies additional obligations for these entities.

2. Main provisions of the Draft Law

The Draft Law imposes an obligation to essential and important entities to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems, which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. These measures are detailed by the Draft Law, which strengthens the security requirements by providing a minimum list of basic security elements that must be applied.

Among the measures, NIS 2 Directive and the Draft Law include the requirement to implement measures on the supply chain security, specifically addressing the security-related aspects of relationships between each entity and its direct suppliers or service providers. In addition to the requirements set forth by the NIS 2 Directive, the Draft Law introduces an obligation for essential and important entities to submit a list to the DNSC detailing all their providers in certain categories. These include DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and social networking service platforms, and providing these types of services to them.

The Draft Law introduces more precise provisions regarding the process of reporting incidents with significant

impact. Compared to Law 362, which did not provide strict timing for the reporting process, the Draft Law provides that entities should report information to the national cybersecurity incident response team:

(a) within 24 hours of becoming aware of the significant incident, which is considered an early warning;

(b) within 72 hours of becoming aware of the significant incident, which is an incident report that should include updates and an initial assessment of the incident;

(c) an intermediary report, upon request;

(d) a final report no later than one month after the transmission of the notification of the incident under point (b); and

(e) another final report if the incident was still under development within another 30 days of responding to the incident.

The Draft Law specifies the content of the reports and the steps the response team must take to address the notification.

Also, to ensure effective accountability for cybersecurity measures at the organisational level, the Draft Law provides that the responsibility for adopting the measures to manage cybersecurity risks lies with the management bodies of entities. These management bodies are also required to undergo training to develop the knowledge and skills necessary for cybersecurity oversight. Additionally, the Draft Law introduces several requirements for individuals responsible for the security of networks and information systems within certain entities.

The Draft Law also implements a national level policy on Coordinated Vulnerability Disclosure (**CVD**), by which any person can report vulnerabilities in ICT products or services and the DNSC will address such vulnerabilities with the services/products providers. The CVD is also a cooperation mechanism between the ICT services providers and the persons reporting vulnerabilities, which allows the adoption of necessary actions to eliminate new security risks. As the national Computer Security Incident Response Team coordinator (**CSIRT**), the DNSC is responsible for managing the coordinated vulnerability disclosure process and is designated as a coordinator acting as a trusted intermediary, facilitating, if necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or supplier of potentially vulnerable ICT products or ICT services, upon request of either party.

3. Significant sanctions

The Draft Law imposes a different sanctioning regime depending on the type of the company (i.e. an essential or important entity) and the legal provisions, which were infringed upon.

Important entities are subject to lower sanctions – up to 1.4% of the net annual turnover in the preceding financial year or RON 35 million (EUR 7 million), while for the essential entities authorities may impose fines up to RON 50 million (EUR 10 million) or 2% of the net annual turnover in the preceding financial year.

The Draft Law does not mention which limit applies (i.e. the fixed amount or the percentage from the turnover), but the NIS 2 Directive clarifies that the fines may be applied up to the higher amount of these numbers.

Where the entity did not have a turnover in the preceding financial year or the entity is newly created, fines may be imposed at a minimum of one and a maximum of 50 gross minimum wages.

Conclusion

The Draft Law has adopted a set of coherent, clear and transparent rules aimed at establishing a unitary national framework for ensuring cybersecurity and responding to cybersecurity incidents occurring at the level of networks and information systems of key entities, while transposing the mandatory requirements of the new NIS 2 Directive. While largely aligned with the directive, the Draft Law includes certain deviations, although it is not certain whether these variations will be retained in the final version of the law.

To ensure a smooth transition, companies should promptly assess whether and to what extent they fall under the scope of the Draft Law. If applicable, they should conduct a thorough review of their existing security practices and evaluate whether they have adequate resources to meet the Draft Law's requirements. This process may reveal a need to strengthen their incident response capabilities and implement more robust cybersecurity measures.

For more information on the transposition of the NIS 2 Directive in Romania and guidance on how the Draft Law affects your business, contact your CMS client partner or these CMS experts: **Cristina Popescu**, **Carmen Turcu** and **Raluca Cretu**.