LEGAL ALERT

New Slovak cybersecurity laws

upon

NIS 2 Directive implementation

ČECHOVÁ & PARTNERS
advokáti attorneys

I. INTRODUCTION

The Directive (EU) 2022/2555, also known as Network and Information Security 2 Directive (the "**NIS 2**") represents a substantial overhaul and expansion of the EU's cybersecurity framework, aiming to address the growing and evolving cyber threats faced by critical infrastructure and key sectors across (EU) Member States. The NIS 2 came into force on 16 January 2023 and it seeks to build upon the foundation laid by its predecessor, the Directive (EU) 2016/1148 (the "**NIS**"), which was the first EU-wide legislation on cybersecurity.

THE ADOPTION OF THE NIS 2 AND BROADENING OF THE CYBERSECURITY LEGISLATION

The original NIS, enacted in 2016, aimed to ensure a high-level cybersecurity across the EU by compelling Member States to improve their national cybersecurity capabilities, enhance cooperation, and impose risk management and incident reporting obligations on operators of essential services and digital service providers. However, the rapidly evolving cyber threat landscape, characterised by the increased sophistication and frequency of cyberattacks, necessitated a more robust and comprehensive legislative response in the form of the NIS 2.

The key goals of the NIS 2 are to strengthen the security requirements imposed on entities, enhance the supervisory and enforcement measures, and improve cooperation and information sharing among Member States. Businesses should be aware that the NIS 2 expands its scope to include additional sectors compared to the NIS, introduces stricter requirements for risk management, incident reporting, and supply chain security. It also establishes a more rigorous framework for penalties and sanctions to ensure compliance and accountability.

Preliminary estimations of the National Security Authority indicate broadening of the supervised entities from a current range of approximately 1,000 to 2,000 subjects to new range of approximately 10,000 subjects after the effectiveness of the Slovak NIS2 transposing legislation.

IMPLEMENTATION AND TRANSPOSITION

The NIS 2 mandates that all EU Member States shall transpose its requirements into national legislation by **17 October 2024**. In Slovakia, a draft amendment to the current Act No. 69/2018 Coll. on Cybersecurity, as amended is currently being prepared as a response to the adoption of the NIS 2 at the EU level, the legislative process of which is, at the time of issuing this Legal Alert, in the stage of inter-ministerial comment procedure and is expected to be submitted to the Parliament (the National Council of the Slovak Republic) for discussion and approval in September 2024.

II. DOES YOUR COMPANY FALL WITHIN THE SCOPE?

The NIS 2 significantly broadens its scope compared to its predecessor by including a wider array of sectors and entities based on their size, sector, and the criticality of their services to the economy and society.

With some exceptions, the applicability of the NIS 2 is based on the size-cap rule and concerns primarily public or private entities listed in Annex I or II which qualify as medium-sized enterprises according to Article 2 of the Annex to the European Commission Recommendation 2003/361/EC, concerning the definition of small and medium-sized enterprises (SMEs). The NIS 2 also applies to entities exceeding the thresholds for medium-sized enterprises outlined in paragraph 1 of that Article, provided they offer services or operate within the EU.

Regardless of their size, the following entities are also subject to the NIS 2:

- **Providers of Public Electronic Communications Networks or Services**: Companies offering internet access services, mobile phone networks, and other communication services;
- **Trust Service Providers**: Entities that provide services for electronic signatures, seals, timestamps, and other trust services;
- **Certain Public Administration Entities**: Specific public administration bodies that play a crucial role in societal and economic functions;
- **Critical Entities Under Directive (EU) 2022/2557**: They are, in brief, entities that operate in sectors such as energy, transport, healthcare, finance, etc;
- **Domain Name Registration Service Providers**: These entities offer services related to the registration of domain names, ensuring the proper allocation and management of domain name resources.

Please note this list is not exhaustive and other entities may also be subject to the NIS2 regardless of their size.

SIZE-CAP RULE

As mentioned above, in order to determine which entities are subject to the NIS 2, the following general size-cap rule is introduced:

	Essential Entities	*Important Entities*	
Size	Large enterprises in Annex I	Medium enterprises in Annex I and II	Large enterprises in Annex II
Turnover	More than €50 million	More than €10 million	More than €50 million
Employees	More than 250	More than 50	More than 250
Criticality	Entities with high criticality	Entities still critical but with slightly less stringent requirements	

ARE THERE ANY EXEMPTIONS?

Certain entities may be excluded from the scope of the NIS 2 if they do not meet the specified criteria. Such entities are subject to equivalent sector-specific regulations or are deemed not to pose a significant risk to the security of network and information systems. Specific exemptions include:

- **Micro and Small Enterprises**: Generally, these enterprises are excluded unless they provide services that are critical to society or the economy – may be selected by a Member State;
- **Public Administration Entities**: The NIS 2 does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences;
- **Entities under other Sector-specific regulations**: Entities already regulated under other EU legislation with equivalent cybersecurity requirements;
- **Entities exempted from Directive (EU) 2022/2554**: Member States may also decide to exempt certain financial entities specified therein.

ESSENTIAL ENTITIES AND IMPORTANT ENTITIES

Where an entity falls within the scope of the NIS 2, the NIS 2 distinguishes between so-called essential entities and important entities.

- **Essential Entity**: There are multiple criteria stipulating which entities are to be considered as essential. For the purposes of this Legal Alert, we will focus on the universal criterion. This category includes sectors such as energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, ICT service management, public administration, and space (further specified in Annex I). These sectors are deemed to be of high criticality, hence subject to stringent cybersecurity requirements of the NIS 2.

- **Important Entity**: Entities of a type referred to in Annex I or II of the NIS 2 which do not qualify as essential entities shall be considered to be important entities. In addition to the sectors mentioned in the Essential Entities section, this group encompasses sectors like postal and courier services, waste management, manufacturing of critical products, digital providers, and research. The NIS 2 also applies to entities exceeding the thresholds for medium-sized enterprises provided they offer services or operate within the EU. While these entities are also critical, the regulatory requirements of the NIS 2 are slightly less stringent compared to essential entities.

III. WHAT ARE THE OBLIGATIONS OF ENTITIES?

The NIS 2 imposes comprehensive obligations on regulated entities to enhance their cybersecurity by various means. The NIS 2 makes no distinction between the obligations imposed on essential and important entities, these obligations apply to both and include the following:

GOVERNANCE AND ACCOUNTABILITY

Management bodies of essential and important entities must be actively involved in cybersecurity governance. They are responsible for ensuring compliance with the NIS 2 requirements and integrating cybersecurity into the organisation's overall risk management framework.

Members of the management bodies are also required to follow training. Essential and important entities shall also offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices.

RISK MANAGEMENT MEASURES

Essential and important entities must adopt appropriate and proportionate technical and organisational measures to manage risks to their network and information systems.

This, among other things, involves the following:

- Implementing security policies;
- Incident handling;
- Securing supply chains - ensuring that third-party providers and partners adhere to high cybersecurity standards;
- Human resources security, access control policies and asset management;
- Using multi-factor authentication or continuous authentication solutions, etc.

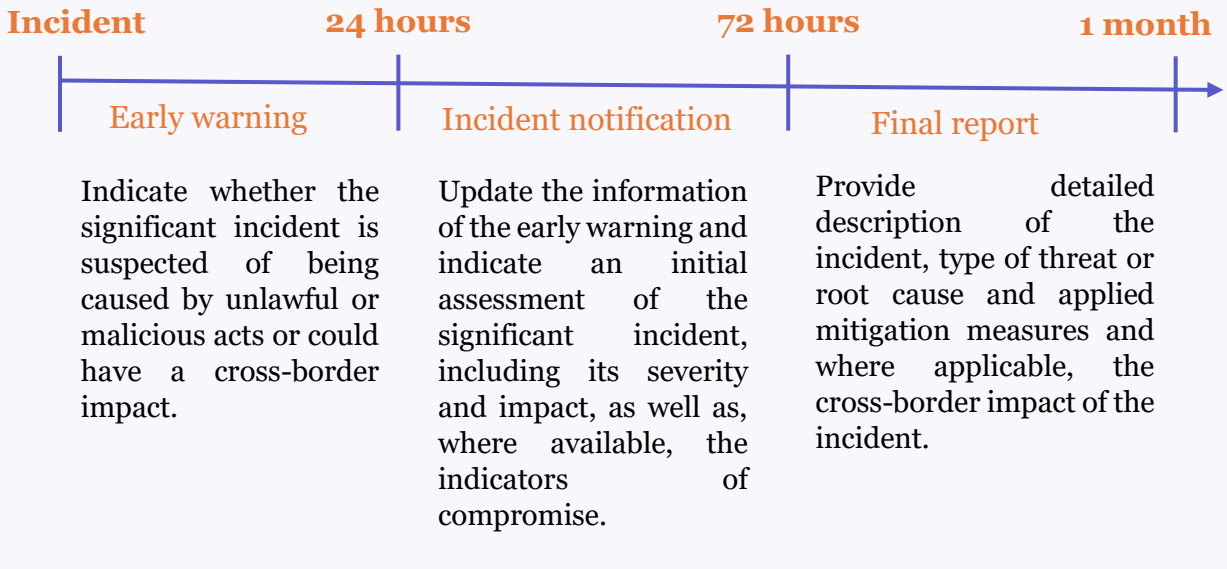
INCIDENT REPORTING

Entities are required to report significant cybersecurity incidents to relevant authorities (CSIRTs or other competent authorities). This rapid reporting aims to minimise the impact of incidents and facilitate a coordinated response.

A cyber threat is considered to be significant if:

- It has caused, or is capable of causing, severe operational disruption of the services or financial loss for the entity concerned;
- It has affected, or is capable of affecting, other natural or legal persons by causing considerable material or non-material damage.

Incident reporting timeframe:



USE OF EUROPEAN CYBERSECURITY CERTIFICATION SCHEMES

Member States have the option to require essential and important entities to use particular ICT products, ICT services and ICT processes certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. Furthermore, Member States shall encourage essential and important entities to use qualified trust services.

IV. SUPERVISION AND SANCTIONS

The supervision and enforcement mechanisms under the NIS 2 vary between essential and important entities:

- **Supervision of Essential Entities**: These entities are subject to more rigorous and proactive *ex ante* supervision.
- **Supervision of Important Entities**: While still under scrutiny, important entities face less stringent supervisory measures compared to essential entities. They are subject only to *ex post* supervision. However, they must still demonstrate compliance with the NIS 2's requirements.

MEASURES FOR SUPERVISION

Among other things, supervisory authorities are empowered to:

- **Conduct Audits and Inspections**: Regular audits and inspections ensure that entities adhere to the prescribed cybersecurity measures.
- **Issue Binding Instructions**: Authorities can mandate specific actions or changes to address identified weaknesses or non-compliance.

- **Request Information**: Entities must provide information on their cybersecurity measures and incident responses as requested by the authorities.
- **Monitor Incident Reports**: Authorities will closely monitor reported incidents to ensure timely and effective responses and remedial actions.
- **Security Scans**: Based on objective, non-discriminatory, fair and transparent risk assessment criteria.

SANCTIONS FOR NON-COMPLIANCE

The NIS 2 introduces substantial penalties for non-compliance to ensure adherence to its stringent requirements.

For essential entities, fines can reach up to €10 million or 2% of the total worldwide annual turnover, whichever is higher.

For important entities, fines can be up to €7 million or 1.4% of the total worldwide annual turnover, whichever is higher.

V. CONCLUSION AND EXPECTATIONS

The implementation of the NIS 2 into national legislations is expected to significantly improve cybersecurity of entities across the EU. Expected key outcomes include:

- **Enhanced Security**: With broader scope of regulated entities and stricter requirements for risk management and incident reporting, entities will be better prepared to prevent and respond to cyber threats.
- **Greater Accountability**: Management bodies involvement in cybersecurity governance ensures that cybersecurity is prioritised at the highest organisational levels.
- **Improved Incident Response**: Rapid incident reporting and coordinated responses will help mitigate the impact of cyber incidents.
- **Supply Chain Security**: Addressing cybersecurity risks within supply chains will enhance the overall resilience of critical infrastructure.

The NIS 2 marks a significant advancement in the EU's efforts to enhance cybersecurity across its Member States. By expanding the scope of regulated entities and imposing comprehensive obligations, the NIS 2 aims to ensure a high level of cybersecurity resilience. **Organisations must proactively prepare for due compliance by integrating cybersecurity measures, involving senior management in cybersecurity governance, and addressing risks within their supply chains.**

As Slovakia advances towards the transposition of the NIS 2 into the national law, entities operating within its jurisdiction should closely monitor legislative developments and begin their internal preparations to meet the newly coming additional cybersecurity requirements.

* * *

This Legal Alert was prepared in August 2024 for general information purposes only and does not constitute a legal advice. The alert is not a comprehensive or exhaustive summary and provides only a brief and indicative summary of the material legislative rules.

If your company falls within the scope of this cybersecurity regulation and you require further information, a specific assessment, or legal advice on the NIS 2, please do not hesitate to contact our law firm, in particular our cybersecurity team led by Simona Haláková, partner (simona.halakova@cechova.sk), who, together with our associate colleagues, Arnold Xavier Verhaege (arnoldxavier.verhaege@cechova.sk) and Ivan Kolenič (ivan.kolenic@cechova.sk), will be pleased to advise you.