Cybrela

Cyber Alert

May 2023

Weinhold Legal

Cybersecurity according to NIS2

The NIS2 Directive and its effectiveness

On 16 January 2023, Directive (EU) 2022/2555 of the European Parliament and of the Council on measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148, the so-called **NIS2 Directive**, entered into force. On this date, the **deadline** for the Czech Republic and other Member States of the European Union to **transpose** the minimum standard of rules set out in the NIS2 Directive began to run and **will expire on 17 October 2024.**

National Cybersecurity

The transposition of the NIS2 Directive started to be dealt with at the national level very early on, directly by the The National Cyber and Information Security Agency (NÚKIB), as the competent central administrative authority for cybersecurity. The first **bill on cybersecurity** was prepared and published on the NÚKIB website less than a month after the publication of the NIS2 Directive, i.e. at the end of January 2023. As a result of the publication of the bill, the professional public was invited to give their comments on the bill as part of a public consultation. Thus, at the moment, the bill on cyber security is in relative calm, but according to the Government's legislative work plan for 2023, the bill is expected to be **submitted to the Government for consideration in December 2023.**

Although not all the obligations that will be mandated by the new act on cybersecurity are known yet, it is already possible to **identify the entities that will be (newly) subject to the obligations of the NIS2 Directive.** However, in addition to the obvious obliged entities identified directly by the NIS2 Directive, this legislation provides for the possibility **of Member States to determine some of the obliged entities at their own discretion**, taking into account the importance or specific nature of the concerned entity.

Obliged entities

The key criteria for determining which entity will "fall" under the new cybersecurity legislation and to what extent are primarily (i) the **sector and subsector** in which the entity operates and (ii) the **size of the entity** as defined in European Commission Recommendation 2003/361/EC on the definition of micro, small and medium-sized businesses. By identifying according to these criteria, the **obliged entities are divided into two groups**, a group of **(1) basic entities** falling under the **higher obligation regime** and a group of (2) **important** entities falling under **the lower obligation regime**. In particular, entities which fulfil the size criteria and will also **operate in the following sectors should pay attention:**

- **energy,**
- **transport,**
- **banking and financial market infrastructure,**
- **healthcare,**
- **drinking and waste water,**
- **digital infrastructure,**
- **public administration,**
- **space and research,**
- **postal and courier services,**
- **waste management,**
- **manufacture, production and distribution of chemicals,**
- **manufacture, processing and distribution of food products,** and

- **manufacture of medical devices, computers, electronic and optical devices and electrical equipment and machinery, motor vehicles, trailers and semi-trailers and other transport equipment.**

Determination of obliged entities

In the absence of a corresponding obligation on Member States directly provided by the NIS2 Directive, as well as the amount of information that is needed for the assessment, entities will be required to **carry out the assessment on their own.** Subsequently, the obliged entity will be obliged to **register** within one of the groups mentioned on the **NÚKIB website.** The obligation to register is foreseen by the bill **within 30 days** from the date on which the entity has established that it fulfils the criteria set for one of the groups, but **no longer than 90 days** from their actual fulfilment.

However, in addition to the process of self-determination of the obliged entities according to the above criteria, it is expected that **some of them will be determined directly by the State,** probably through the NÚKIB. In such a case, the NÚKIB will inform the obliged entity directly of its obligation.

From the range of the above criteria alone, it is clear that it will be **time-consuming, staff-intensive and demanding** for the obliged entities to manage the **preparatory phase** within the above deadlines.

Obligations

Although still unofficial, the bill on cybersecurity gives a fairly clear idea of the obligations that the obliged entities will have to comply with, reflecting the general minimum set by the NIS2 Directive. The obligations will then vary slightly depending on which of the regimes the obliged entity falls under. For example, following an **initial risk analysis** or determination of technical assets and a business impact analysis under the lower obligation regime, this would include the **introduction of:**

- active **participation of top management** in cybersecurity management;
- **new management/liability roles** to ensure compliance of the obliged entity with the obligations under the draft law;
- information security **policies;**
- **contractual clauses** to ensure security within the supply chain;
- **cybersecurity education;**
- **security measures** and procedures for evaluating their effectiveness;
- **cryptography** and, if appropriate, encryption of information;
- **access control** rules;
- multi-factor **identity verification**, secure **communication tools** and emergency communication tools;
- rules for **managing** and **reporting** security **incidents** to **NÚKIB** or the National CERT operator;
- **crisis management** rules;
- rules for business **continuity, backup and recovery** in the context of a security incident.

Sanctions

After the expiration of the transitional period, which is currently assumed to be one year from the registration in the NÚKIB's register on the basis of the previous registration of the entity, thus, probably from **November 2025**, the NÚKIB will be empowered to impose sanctions for non-compliance with the obligations set out in the bill. In addition to **corrective measures and the sanction of suspension of the European Cybersecurity Certificate** granted under Regulation (EU) 2019/881 of the European Parliament and of the Council (Cybersecurity Act), the NÚKIB will be empowered to impose fines for **administrative offences** provisionally specified in the bill, **up to CZK 250,000,000** or **2% of the net worldwide annual turnover of the entity or**

Cybrela

Cyber Alert

May 2023

Weinhold Legal

its consolidation unit. As an additional point, the NÚKIB will have the power to impose a fine in the period **before November 2025** in case of **failure to comply with the obligation of on-time registration of the obliged entity of up to the maximum amount.**

The last type of sanction, which, however, will no longer be decided by the NÚKIB, will be a **decision made by the courts to suspend the performance of management functions** of persons in the position of, for example, a member of the statutory body, head of a branch plant or a proxy. The consequence of this sanction will be a **prohibition from exercising the function in management** of the underlying entity, i.e. under the **higher obligations regime, until the identified deficiencies are remedied, but always for at least 6 months.**

Next steps

The current task of each entity is to assess whether and, if necessary, to what scope the obligations under the new legislation will apply to it. For this purpose, our law firm is ready to provide you with the necessary legal services in close cooperation with the consulting company Cybrela s.r.o.

Cybrela s.r.o. is a consulting company on cyber-information security, especially with regard to organizational and procedural measures. Its main activities are focused on ISO 27001, ISO 27005, risk management, TISAX, Cybersecurity Act and Decree, NIS2, new drafts of the Cybersecurity Act and Decree, outsourcing the roles of Cybersecurity Manager and Cybersecurity Auditor. It It combines forces with Weinhold Legal to provide comprehensive cyber-information security services to clients.

Cyber Security team Weinhold Legal

Martin Lukáš
Partner
martin.lukas@weinholdlegal.com

Tereza Hošková
Managing Attorney
tereza.hoskova@weinholdlegal.com

Michal Švec
Attorney at Law
michal.svec@weinholdlegal.com

Klára Mladá
Attorney at Law
klara.mlada@weinholdlegal.com

Jiří Kvaček
Attorney at Law
jiri.kvacek@weinholdlegal.com

Deborah Paláková
Junior Attorney
deborah.palakova @weinholdlegal.com