EVERSHEDS SUTHERLAND

# NIS2 Directive and the new Bill on Cybersecurity

## How Eversheds Sutherland can support you

## What is the NIS2 Directive and from when does it apply?

**The NIS2 Directive** is an **EU directive** that imposes strict new **requirements** on certain companies and Member States **in the area of cyber security.** This is the EU's response to the massive increase in the damage caused to European companies by cyber-attacks.

NIS2 must be transposed into national law by EU Member States by **18 October 2024. The** requirements apply from that date.

**A transpositional bill** is being prepared in the Czech Republic **and is expected to come into force in October 2024.**

## When does your company fall under NIS2?

In order for a company to be subject to NIS2, **three cumulative conditions** must be met**:**

- **Condition 1: Minimum size**

> EUR 10 million annual turnover or
> 49 employees

***Please note:***
*For conglomerates: the data are aggregated together for the group as a whole. For particularly critical companies, sub-threshold applicability is possible!*

- **Condition 2: Activities in the EEA**

The company must be active in the EEA.

***Please note:***
*Establishment in the EEA is not a requirement; activity in the EEA is sufficient!*

- **Condition 3: Regulated services**

The company provides regulated services.

***Attention:***
*Even "regulated" minor services provided by a company are (usually) sufficient for regulation!*

**In particular,** the following are considered **critical** sectors**:**

| | | | |
|---|---|---|---|
| **Electricity** *Production, supply, storage and sale of electricity, oil, gas, hydrogen, etc., including electronic refuelling stations.* | **Mechanical engineering, electrical equipment, automotive** *Manufacture and assembly of machinery, apparatus, vehicles, including spare parts.* | **Healthcare** *Medical services, laboratories, production of medicines, medical devices, pharmaceuticals.* | **Digital infrastructure** *including trust services, data centres, cloud computing, communications networks and services, SaaS, IaaS, etc.* |
| ***Banks and financial markets*** *Please note: Special regulation (DORA) applies here!* | **Chemical industry** *Production and trade fuels, mixtures and chemical products.* | **Food industry** *Wholesale, industrial production and processing.* | **Waste management** |
| **Public administration** | **Online platforms** | **Postal and courier services** | **Research facilities** |
| **Transport** *Air, rail, ship, road and space transport.* | **B2B IT services** *including intra-group services.* | **Drinking and wastewater** | **Other *definitions*** *in national transposition legislation.* |

***Warning:*** *definitions are complex and often very broad!*

- **Indirect applicability:**

The contractors of the companies concerned may be **indirectly** affected by NIS2 as part of the supply chain - the companies concerned must contractually impose cybersecurity obligations on them under NIS2.

# What requirements must the companies fulfil?

Companies subject to NIS2 must comply with the following obligations**, among others**:

- **Registration required**:

The companies concerned must register with the National Office for Cyber and Information Security (NÚKIB) - in the Czech Republic, this should happen by the end of 2024 at the latest.

***Please note:*** *Requirements may apply in other countries. earlier registration requirements (e.g. Hungary).*

- **Notification duty in the event of a cyber incident:**

A significant cyber-attack or other cyber incident must be reported to the relevant authority within **24 hours** of discovery.

**Subsequent reports** must be made within 72 hours, one month after the incident is resolved and at any time upon request.

- **Preventive risk management measures:**

Companies must take measures to mitigate and manage cyber risk to their own systems.

Measures must be **proportionate to the** company and the risks. As a reference, the state of the art, relevant standards (e.g. ISO) and cost reasonableness must be used.

Compliance with the relevant risk measures must be demonstrated to the authorities upon request. Some companies are expected to be subject to regular security audits.

**Attention: ISO alone is not enough!**

Examples of measures:

| | | | |
|---|---|---|---|
| **Role and responsibilities of statutory bodies** | **Cyber hygiene** and security in **human resources** | **Asset management** | **Cryptography** and **encryption** |
| **Risk analysis**, **risk management** and **system security** processes | Regular **training** and **awareness** raising **on cyber security** for employees and governing bodies. | Security in the **acquisition, development, operation** and **maintenance of** IT systems | **Business continuity** and **crisis management**, including backup and **recovery** concepts |
| **Access control**, **access authorization**, **password management** and **multi-factor authentication** | **Cybersecurity in the supply chain**, including reviewing and adjusting contracts with suppliers and service providers. | Guidelines and procedures for **dealing with cyber security incidents** | **Environmental** and **physical security of** systems |

***Note:*** *Additional requirements may be specified for specific sectors.*

# What are the responsibilities of the company management?

The regulation explicitly states that cybersecurity is the **responsibility of the company's management**. The following duties are therefore expressly addressed to the management bodies of the companies concerned (the board of directors, the managing directors, the supervisory board, etc.):

- **Monitoring implementation:**

The managing authorities must **approve the** above risk management measures and **monitor** their **implementation**. This task cannot be delegated.

The managing authorities will be **personally** liable for **any** damage caused by a breach of this obligation.

- **Mandatory training:**

Management bodies must regularly receive **training in cyber security management.**

The content of the training must also include **measures for** cyber risk **management** specific to the company.

## Consequences of non-compliance

The new regulation provides for strict consequences in case of non-compliance:

- **Administrative fines:**

The fines can be up to **€10 million** or **2% of the group's worldwide revenues** (whichever is higher).

- **Management Responsibility:**

The managing authorities will be held **personally** liable for any breach of their **obligations**. This responsibility cannot be delegated.

- **Supervisory measures:**

The competent authority for cybersecurity may **carry out control measures** or have them carried out by external auditors **at any time**.

The NÚKIB may order the **infringement to be remedied** by an official notice.

In the event of an **imminent threat, the activities of** some organizations may be temporarily **banned,** or their **leadership removed.**

## How Eversheds Sutherland can support you

The new NIS2 Directive imposes stricter cybersecurity obligations on many companies from the autumn of 2024. Failure to comply can lead to hefty fines and personal liability of company management for damages caused by non-compliance with the new rules. In addition to the technical requirements, the implementation of the NIS2 Directive poses a major legal challenge for companies.

**How we can help you implement NIS2:**

**Impact assessment:** the question of whether a company falls under NIS2 is often complex. We will carry out this assessment for you and explain all the legal aspects.

**Management training:** the NIS2 requires regular management training. Together with our technical partners, we offer training for your management - tailored to your needs and bundled with legal services. This allows you to demonstrate that you have met this obligation.

**Gap analyses and implementation plans:** the implementation of NIS2 requires planning. We are happy to assist you with an analysis of where your company currently stands and what steps are still required to achieve the NIS2 requirements.

**Support for implementation - nationally and internationally:** the implementation of NIS2 is not only a technical but above all a legal challenge. Our dedicated team will be happy to support you both in the Czech Republic and with the help of our colleagues in other European jurisdictions.

**Legal Incident Response for cybersecurity emergencies:**
In the event of an emergency, you need to act quickly. Initial notification under NIS2 must be made within 24 hours. Violation of this obligation can lead to heavy fines.
In the event of an emergency, we will provide prompt support to help you manage the legal issues of a cyber incident and minimize the damage. This is not only in the Czech Republic, but worldwide if necessary.

**eversheds-sutherland.cz**

**Our Eversheds Sutherland NIS2-Hub:** Track the status of NIS2 implementation in different EU Member States, including more up to date information on proper NIS2 implementation - always free and up to date at ezine.eversheds-sutherland.com/eu-nis2-directive.

## Contact

We would be happy to invite you for a non-binding consultation on what NIS2 means for your company and how we can support you.

**Jaroslav Tajbr**
*Partner* | *Prague*

T: +420 737 328 278
jaroslav.tajbr@
eversheds-sutherland.cz