# NIS2 Directive

SORAINEN

## What you need to know

The **NIS2** Directive introduces new cybersecurity requirements for organisations to improve their protection against cyberattacks and incidents for enhanced cybersecurity in the EU.

Lithuania has transposed the Directive by adopting amendments to the Law on Cybersecurity, which entered into force on 18 October 2024.

## Why it is important

For an organisation to be better prepared to deal with threats, mitigate risks and negative impacts, and ensure business continuity in the event of cyber incidents, it is essential to act now. Preparation is a time-consuming and complex process, as cybersecurity is not just a technological issue. It is therefore important to prepare in advance by engaging a wide range of professionals:

**Lawyers**

**Cybersecurity professionals**

**IT professionals**

## Who is covered by the Directive

**Private and public sector organisations that provide services or products of critical importance to the state.**
The Law on Cybersecurity sets out **general and specific criteria** for determining which specific organisations in Lithuania are considered **cybersecurity entities (essential** or **important)** and have to **comply with the updated cybersecurity requirements.**

**For a full list of criteria (in Lithuanian), click here.**
**To check if your organisation is included in the Registry of Cybersecurity Entities (in Lithuanian), click here.**

Suppliers providing services, goods and works to cybersecurity entities will also be required to comply with NIS2 (ensuring supply chain security).

# Understanding the impact of non-compliance

An ill-prepared organisation is an easy target for cyberattacks, resulting in financial losses, reputational damage, loss of competitiveness, and threats to business continuity.

- **Fines.** For essential entities: **< EUR 10 million** or < 2% of the legal entity's total worldwide annual turnover; for important entities: **< EUR 7 million** or < 1.4% of the legal entity's total worldwide annual turnover.
- Reputational impact and loss of customer trust.
- Direct financial loss.
- Loss of income due to disruption of operations.
- Costs associated with the recovery, restoration and repair of affected IT systems.
- Loss and recovery of operational i nformation.
- Damage to other partner organisations involved in the provision of services.

# How we can help

**As the preparation for and implementation of NIS2 requires more than just legal expertise, we work with experienced cybersecurity experts to help our clients with the following:**

- Assessment of the specific requirements applicable to an organisation
- Gap assessment
- Network and information systems risk assessment
- Preparation of documentation
- Implementation of supply chain security requirements
- Management of cyber incidents and reporting to the authorities
- Penetration testing
- Training for managers and employees

# Main requirements

**Organisations are required to:**

- Assess the level of risk to their communic-ation and information systems and services.
- Apply adequate safeguards commensurate with the level of risk, keep them up-to-date and adapt them to evolving threats.
- Ensure supply chain security.
- Designate persons in charge of cybersecurity.
- Manage cyber incidents and report them to the competent authorities within 24 hours.
- Provide periodic training for board members, managers, and staff.
- Carry out periodic audits.

# Contact us:


Irma Kunickė
Counsel

M. +370 66 377 166
T. +370 52 685 040
irma.kirklyte@sorainen.com

Stasys Drazdauskas
Counsel, attorney-at-law

M. +370 61 122 910
T. +370 52 685 040
stasys.drazdauskas@sorainen.com

Raminta Matulytė
Associate

M. +370 61 062 865
T. +370 52 685 040
raminta.matulyte@sorainen.com

Sidas Sokolovas
Senior Associate

M. +370 62 304 665
T. +370 52 685 040
sidas.sokolovas@sorainen.com