# NIS2

## Who does it apply to?

**Providers of essential services**

- Scientific research
- Provision of digital services
- Manufacturing
- Food production, processing and distribution
- Waste management
- Production and distribution of chemicals
- Postal and courier services

**All companies with more than 50 employees and more than 10 MEUR annual turnover or balance sheet volume**

**Providers of vital services**

- Energy
- Transportation
- Banking
- Financial market infrastructures
- Healthcare
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management (business-to-business)
- Public administration
- Space

European Union directive

**NIS2**

Network and Information Security Directive 2

## Deadline

**Hurry!**

The regulation entered into force in January 2023 ⇒ To be transposed into national laws by **October 17, 2024** at the latest

**NIS2 (Network and Information Security Directive 2) is a European Union directive that sets a high common level of cyber security for EU member states and critical and important entities/companies operating in them.**

**NIS2 harmonises companies' cyber security measures, focusing on risk management and supply chain security, and imposes harmonized fines for breaches.**

## Who does NIS2 apply to?

In short – **indirectly for all companies operating in the EU**, because the companies to which the directive applies must also ensure the cyber security of their supply chain.

## What are the sanctions for non-compliance?

**Fine up to € 10 million**

**For the company**
Up to 10 MEUR or 2% of global annual turnover (higher of the two).

**For top managers**
Significant fines for private individuals. Possible criminal liability.

## How to comply with the NIS2 directive?

- Perform NIS2 compliance and risk assessment.
- Perform a comprehensive cyber security and infrastructure audit.
- Create a plan to implement a cyber security framework (for example ISO27001).
- Add to the plan the steps resulting from the NIS2 directive, which are not covered by ISO 27001.
- Implement the plan step by step (prove progress).
- Implement incident detection and notification process according to NIS2.
- Train employees and management regularly.
- Ensure cyber security level of supply chain partners meets requirements – assess and monitor regularly.
- Document everything and keep the documentation up to date.

**Choose a partner!**

Perform compliance and risk assessment and cyber security audit.
Create a plan to implement a cybersecurity framework.
Implement the plan step by step (prove progress).

OIXIO Cyber

**Erki Markus**
erki.markus@oixio.eu
+372 520 1293

**www.oixio.eu**