advenica

The NIS 2 Directive

NIS 2 - The new NIS Directive

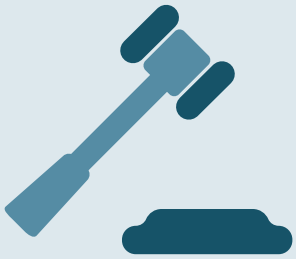
On the 10th of November 2022, the proposal for NIS 2 was adopted and the directive has now been published. NIS 2 means that there will be a risk of large fines if you do not meet the requirements. So how do you make sure that your organisation will not be hit by the sanctions? In our guide, we give you the tips you need!

The NIS Directive

The NIS Directive aims to promote security measures and boost EU member states' level of protection of critical infrastructure. In other words, it improves information security of operators in sectors that provide essential services to our society and economy.

The NIS Directive tightens the requirements for information security in terms of integrity and availability. It is important to take people, processes and technology into account to ensure information security in the affected organisations. Better understanding in general of information and system risk classification together with impact contingency and action plans is necessary to improve resistance to attacks. Incidents are to be reported as part of increasing knowledge and raising preparedness. Basically, focus lies on the network and information systems that are used.

Why NIS 2?



The initial NIS Directive included a process to conduct regular reviews of itself. This has led to a proposal for a directive for countries in the EU about measures for high common level of cybersecurity – this is called NIS 2.

The proposal for NIS 2 contains aspects that meet deficiencies with the original NIS Directive. These deficiencies where found:

- Businesses in the EU do not have a sufficient level of cyber resilience (cyber resilience is the resistance to a possible cyberattack, but also the ability to keep capacity up during an attack, and how well you return to your original capacity after an attack)
- There is inconsistency between member states and sectors concerning cyber resilience
- There is not a sufficient understanding among member states about present threats and challenges, as well as not having a joint crisis response

What is new with NIS 2?

The original NIS Directive contained a process for regular review of its own content. This has led to a proposed directive for countries in the EU on measures for a high common level of cybersecurity - this is called NIS 2.

NIS 2 contains aspects that address deficiencies in the original NIS Directive. Based on these shortcomings, new additions have been made, resulting in the new proposal NIS 2. These are the most prominent additions:

- Larger scale than NIS, more sectors considered essential services
- Managers are held responsible for securing operations
- Incident reporting must now be done within 24 hours instead of 72 hours
- Higher security and reporting requirements, where a list of minimum requirements must be met
- Security for supply chains and suppliers
- Stricter supervisory measures for national authorities
- The distinction between "operators of essential services" and "digital service providers" has been removed
- Stricter regulatory measures for national authorities, stricter compliance requirements
- Harmonise sanctioning systems between Member States and enable administrative fines. The fine will be up to EUR 10 million or 2% of the company's total turnover worldwide
- The Cooperation Group gets a bigger role, as well as increased information sharing and cooperation between member states' authorities

In October 2024, the directive will come into force and by then everyone affected must have adapted their operations. Among other things, the updated directive applies to more sectors and more additions.

Who will be affected?

In the current NIS Directive, there are seven affected sectors:

- **Energy, transport**
- **Banks**
- **Financial market infrastructure**
- **Health**
- **Water supply**
- **Digital infrastructure**.

In addition to these are newly added sectors:

- **Manufacturing of pharmaceutical products including vaccines and critical medical devices**
- **Public administration**
- **Space**

New sectors have been added based on their importance to society and the economy, and more companies in each sector will be affected. This as a measure to respond to Europe's increased exposure to cyber threats.

Key sectors that will also be affected are:

- **Postal and courier services**
- **Waste management**
- **Chemicals**
- **Food**
- **Manufacturing of other medical devices**
- **Computers and electronics**
- **Machinery**
- **Motor vehicles**
- **Digital suppliers**

All large and medium-sized companies from these sectors within the EU are now affected. Even smaller companies can be affected if it is considered necessary based on the company's profile.

The extension of the scope covered by the new rules, by effectively forcing more businesses and sectors to take measures to manage cybersecurity risk, will help to increase the level of cybersecurity in Europe in the medium and long term.

What happens if I do not comply?

What can happen if an important organisation does not meet the requirements is the following:

- Fines of up to EUR 10 million or 2% of the total global annual turnover
- Management must take responsibility
- Temporary bans targeting managers
- Appearance of a supervisor

How to avoid sanctions

So what to do now?

1. First of all: Find out if you and/or your customers are covered by the directive. For example, if you are a business that provides a service necessary to sustain critical societal and/or economic activities, such as an energy company, you are classified as an "essential service operator". Then start by finding out what requirements are placed on you and do a gap analysis of the current situation.

2. Appoint a cybersecurity officer at management level. Since it is the management that will be held responsible in the event of an inspection, it is important that the responsibility is placed at this level.

3. Work systematically and risk-based with information security.

4. Take security measures to protect network security and information systems. This includes risk analysis and security policies for information systems.

5. Make sure to implement a well-organised incident management. That is, a system to be able to report incidents that affect the continuity of services (prevention, detection, and response to incidents.

6. Work with a structured approach to risk management. You need to work in a structured way with business continuity and crisis management as well as supply chain security. This includes having policies and procedures in place for cybersecurity risk management measures.

7. Introduce policies and procedures regarding cryptography and, where appropriate, encryption.

8. Prepare for supervision by your sector's designated supervisory authority.

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at advenica.com

advenica

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED