The new EU cyber directive NIS-2 affects many companies

HDI Global SE → Cyber

Digital infrastructures and systems are becoming increasingly complex. Today, a cyberattack can often affect not just one company, but entire value chains.

Cyber incidents have become a serious threat to the global economy. More stringent European security standards are intended to reduce these risks.

In order to increase cybersecurity in Europe, the EU adopted the new cyber directive NIS-2 (Network and Information Security Directive 2) on 27 December 2022, expanding on the version that came into force on 16 January 2016. A large number of businesses must now do more to increase their cybersecurity and in some cases even prove that they have undertaken such measures. Those who cannot do so may face fines in the millions. **Plus, the Directive must be transposed into national law by 17 October 2024.**

Challenges for businesses

Companies that are affected will not be informed and called upon to act, but rather must **enquire on their own** if they fall within the scope of application. As **the transposition period expires soon**, preparations must be undertaken immediately, and companies must secure support ahead of time. The new directive poses a particular **challenge for smaller companies** as they often lack the resources to implement the requirements themselves. In addition, demand for service providers and cybersecurity experts will increase and result in limited capacities.

What companies need to act now?

While only a smaller number of companies were required to comply with certain cyber regulations in the past, a larger number is now affected. Companies with **at least 50 employees** and an **annual turnover or a balance sheet total of more than EUR 10 million** may fall within the scope of the NIS-2 directive if they are also considered essential or important entities:

Essential entities

- Energy
- Traffic & transport
- Banking & financial markets
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- ICT services (B2B)
- Public administration
- Space

■ Already affected under NIS-1

Important entities

- Postal and courier services
- Waste management
- Production, manufacture and distribution of chemicals
- Research institutions
- Production and manufacturing of goods*
- Production, processing and distribution of food
- Digital services providers

* Pharmaceutical products (NACE 21); electronics/optical products (NACE 26/27); machinery and equipment (NACE 28); motor vehicles and parts/accessories (NACE 29/30)

In future, the institutions concerned will be subject to the following obligations:

1 **Reporting of cyber incidents**
Entities that are covered must report significant cyber incidents to the national authorities within 72 hours. This allows authorities to respond quickly to threats and minimise their impact.

2 **Security precautions**
Entities that are covered must implement appropriate technical and organisational measures to ensure cybersecurity. This includes securing networks and systems as well as implementing security guidelines.

3 **Responsibility of the management**
Management is required to monitor the implementation of the measures. In doing so, it is liable for violations. Participation in appropriate training is mandatory and must also be offered to employees.

Sanctions for violations

In the event of **breaches of risk management measures (article 21) or the obligation to report security incidents (article 23) under the NIS-2 directive,** fines and other sanctions may be imposed. The obligations of the essential entities (see overview above) are basically the same but differ in the intensity of monitoring and the amount of the fines in case of non-compliance. These entities may face maximum amounts of **at least EUR 10 or 7 million or 2 % or 1.4 % of the worldwide turnover in the previous year.**

How can HDI provide support?

In addition to offering classic cyber insurance, HDI Global SE has expanded its range of services to include **„cyber services". This offering is aimed at both existing and prospective clients.** The scope of service in this respect consists of **1:1 support** (the support and expertise of HDI cyber risk engineers) and various pre-selected and approved service providers from HDI Global's range of **value-added services**. The client thus benefits from special conditions through existing framework agreements with HDI Global SE.

HDI services provide support to companies regarding NIS-2 either holistically or selectively:

NIS-2 security requirements incl. HDI Global service offer

Area	NIS-2 requirement	Service provided by HDI Global SE
Policies	Guidelines for risk and information security	✔
Incident management	Prevention, detection and management of cyber incidents	✔
Business continuity	BCM with backup management, disaster recovery, crisis management	✔
Training	Cybersecurity hygiene	✔
Cryptography	Requirements for cryptography and – where possible – encryption	✔
Asset management	Information security management system (ISMS)	✔
Authentication	Use of multi-factor and single sign-on (SSO)	✔
Emergency communication	Use of secure systems (voice, video and text)	✔

Further NIS-2 requirements upon request:
Supply chain (security in the supply chain), purchasing (procurement of IT and network systems), effectiveness (specifications for monitoring cyber and risk measures), personnel (HR security), access control, communication (secure communication tools)

Are you unsure whether your company falls within the scope of application, or do you not know where and how to start? HDI cyber experts will be happy to help you with questions about the new cyber policy and will work with you on developing an action plan with concrete recommendations.

Your contact persons:

Larissa Schrader
Head of Cyber
Risk Engineering Services
Larissa.Schrader@hdi.global

Florian Köhler
Risk Engineering Services
Cyber & Financial Lines
Florian.Koehler@hdi.global

HDI Global SE
HDI-Platz 1
30659 Hannover
www.hdi.global

404-FL026-202405