The NIS 2 directive to improve cybersecurity in the EU

The NIS 2 directive (December 2022) replaces its predecessor, the NIS 1 directive (2016). Its aim is to improve the cybersecurity resilience and responsiveness of the public and private sectors and of the European Union as a whole. To this end, it prescribes “measures for a high common level of cybersecurity in the Union”. All EU member states must implement the directive into national law by October 17, 2024. By then at the latest, the requirements, especially in the area of cyber risk management, will also apply directly to “public and private institutions” from certain sectors, including authorities and businesses. Until then, the provisions of the NIS 1 directive apply.

Objectives of the NIS 2 directive

To improve cybersecurity in the EU, national cybersecurity strategies have to be implemented along with the designation or establishment of competent national authorities, cyber crisis management authorities, cybersecurity contact points, and Computer Security Incident Response Teams (CSIRTs). NIS2 sets out the requirements for cybersecurity management, including corresponding reporting obligations, the exchange of cybersecurity information between EU states, and how supervision is carried out in individual member states.

Wider area of application

The NIS 2 directive expands the scope to include additional sectors. Annex I to the directive is a list of “sectors with high criticality” and “other critical sectors”:

Sectors with high criticality	Other critical sectors
Energy	Postal and courier services
Transport	Waste management
Banking	Production
Financial market infrastructures	Handling and trading of chemical substances
Health	Handling and trading with food
Drinking water	Manufacturing industry

Sectors with high criticality	Other critical sectors
Digital infrastructure	Digital providers
Waste water	Research
ICT service management	
Public administration	
Space	

Sectors newly added by the NIS 2 directive are highlighted in blue.

Companies that fall into at least one of the sectors mentioned are covered by the directive if they are classified as a "medium-sized enterprise". This applies to companies with between 50 and 249 employees and an annual turnover of between 10 and 50 million euros. Irrespective of their classification, providers of public communications networks and services, trust service providers, and top-level name registries including DNS service providers are always included. In certain cases, small and micro businesses may also fall under the NIS2 directive.

Obligations

The institutions concerned now have a range of obligations:

- → Management bodies are held accountable for cybersecurity risk management. They must approve appropriate measures, monitor their implementation, and be held accountable for violations.
- → Management bodies and employees must participate in cybersecurity training.
- → Essential and important facilities must take suitable and proportionate technical, operational, and organizational measures for IT security (risk management measures).
- → Comprehensive reporting and notification obligations apply in the event of security incidents.
- → Authorities can mandate the use of specific ICT products, services, and processes with cybersecurity certification.
- → Registration requirements are in place for institutions in certain sectors.
- → Institutions are to exchange cybersecurity information with each other.

Risk management measures include risk analysis and security concepts; business continuity, backup and crisis management; multi-factor authentication; concepts for access control and employee security; encryption concepts; vulnerability analyzes; and security aspects regarding the supply chain and relationships with other suppliers or service providers.

In addition to general cybersecurity regulations, the NIS 2 directive also defines specific requirements for individual sectors. These include, for example, requirements for the security of energy and transport systems or the requirements for the security of medical data in healthcare.

Supervision and fines

Responsible authorities should take effective, proportionate, and deterrent supervisory and enforcement measures against covered entities. The fine for non-compliant institutions is at least EUR 7 million or 2 % of the previous year's worldwide turnover.

Eight questions and answers about NIS 2

1. **The implementation of the NIS 2 directive in national law is expected for 2024. When should you start preparing for it?**

Public and private institutions affected by the NIS 2 directive should already start working on the implementation of the obligations arising from the directive into national law now. To do this, they can use the text of the directive as a guide, as it serves as a template for the EU states to implement the requirements in their respective national laws. The obligations of the NIS 2 directive become mandatory from October 18, 2024 – the time until then is short. Affected facilities will not be given more time. The EU member states are also not likely to extend this period. In Germany, some of the requirements from the NIS 2 directive already apply today, as they are already included in the IT Security Act 2.0.

2. **Which requirements from the NIS2 directive should be treated with the highest priority?**

The highest priority should go to risk management. The NIS 2 guideline focuses on risk management in the field of cybersecurity. For this, "appropriate and proportionate technical, operational, and organizational measures" are required. They must correspond to the technical state of the art as well as relevant international and European standards. Establishing the necessary structures and processes, including the appropriate human resources, often takes a considerable time and should therefore be tackled first.

3. **In how far does the General Data Protection Regulation (GDPR) still apply?**

The NIS 2 directive does not affect the General Data Protection Regulation and the independence of data protection authorities for the processing of personal data. This means, for example, that a data leak in the context of a security incident may trigger notification obligations under the GDPR, but also obligations under the NIS 2 laws of the EU states. The NIS 2 supervisory authorities are also obliged to inform the data protection authorities about incidents relevant to data protection. For institutions affected by the NIS 2 directive, it is also right to involve the company data protection officer in the implementation of the requirements.

4. Will there be a transitional period of lenience, or are fines to be expected right from the deadline?

When the national laws implementing the NIS2 directive come into force, all requirements and also the regulations on fines will come into effect. Basically, the transition period is between now and October 18, 2024. Thus, this period of time should be used wisely by the affected facilities. This applies in particular to institutions from sectors that are being included for the first time.

When imposing any fines, the competent authorities must take the circumstances of the individual case into account. The principle of proportionality plays a crucial role here. The NIS2 directive also lists criteria to account for when calculating fines. This includes the severity and duration of the infringement, previous violations, the damage caused, negligence or intent on the part of the responsible persons, damage limitation measures, and the degree of cooperation with the authorities. Authorities usually apply milder penalties before imposing fines. A certain level of "goodwill" may exist after October 18, 2024, but there is no legal entitlement to this.

5. Which additional services can system vendors / IT consultants offer their customers to help them prepare accordingly?

Affected institutions must comply with the obligations of the NIS2 directive. To set up the processes, teams, security technology, et cetera, they can make use of external system houses and IT consultants. This is highly advisable if the necessary skills are not available in-house. The authorities will not accept a lack of resources as a reason for failing to meet NIS2 obligations altogether.

6. What kind of risk-based security strategies are required to comply with the coming regulations?

The NIS 2 directive requires compliance with the technical state of the art, as well as international and European standards. The "IT-Grundschutz" (basic IT protection) of the "Bundesamts für Sicherheit in der Informationstechnik" (BSI in short, German Federal Office for Information Security), but also the ISO 27001 and 9001 standards follow risk-based approaches to information and cyber security. The concrete implementation in an affected institution depends on the individual case. However, a security strategy can only be risk-based if the risks are specifically determined in relation to the institution.

7. What role do IT security audits play?

The NIS 2 guideline does not directly prescribe IT security audits. However, they are mentioned in ISO 27001, for example, and can be carried out as internal or external audits. They generally serve to determine whether a cyber- or IT security system of a facility meets the requirements set for it and where there is a need for improvement. These requirements include the laws implementing the NIS 2 directive.

IT security audits also help managers verify that they are meeting their NIS 2 obligations and can reduce the risk of regulatory action. Insurers, as well as contractual partners, may also demand that IT security audits be carried out regularly, over and above the usual legal requirements.

8. **A wide range of institutions is addressed, including the manufacturing industry and providers of digital services. Which sectors and companies will not be affected by the expected regulations?**

The obligations under the NIS 2 directive are aimed at institutions from a total of 18 sectors, divided into the those of “high criticality” and “other critical sectors”. This sector listing is final. Companies not belonging to at least one of these sectors are not affected.

In principle, only small and medium-sized (SMEs) and large companies are affected. However, small and micro businesses are included if, for example, they are systemically important or “essential for the maintenance of critical social or economic activities”.

About the author

Tobias Haar
LL.M. (Legal Informatics), MBA (Kellogg-WHU)
Lawyer
Vogel & Partner Rechtsanwälte mbB
www.vogel-partner.eu

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de
www.lancom-systems.com