KPMG Law

KPMG

NIS-2: For a higher level of security in Europe

Challenges, opportunities, solutions

Content

Introduction

NIS-2 is the directive on measures for a high common level of cybersecurity in the European Union (EU). The aim of the NIS-2 Directive is to create a harmonized level of protection for network and information systems of critical infrastructures.

With the NIS-2 Directive, the number of critical sectors has been expanded and more precisely defined by eleven sectors compared to the NIS Directive adopted in 2016.

The NIS-2 Directive has been in force since 16 January 2023 and should have been transposed into national law by 17 October 2024. In Germany, however, the planned implementation was not completed on time, meaning that the European Commission has initiated infringement proceedings.

Despite the pending national implementation, the NIS-2 Directive already provides specific requirements that companies should implement to protect their network and information systems.

NIS-2 becomes more specific and affects more companies

In addition to the extensive risk management measures, the NIS 2 Directive entails a risk of fines and a considerable liability risk for company management.

Companies should act now and assess their impact and NIS 2 readiness based on the Directive. KPMG's interdisciplinary experts will be happy to support you with their better practice in analyzing the impact, as well as planning and implementing the NIS 2 requirements.

Sector expansion

By extending the scope of application to new sectors, the cyber security level of the organizations concerned will be put to the test.

Numerous requirements

This expansion entails numerous requirements, ranging from organization and personnel security to technical skills.

Extensive governance requirements

It is to be expected that extensive governance measures relating to security in the company must be established, which are the responsibility of the company management.

Powers of the authorities

The powers of the competent supervisory authorities have been extended, which requires closer cooperation of the private sector and the state. The NIS-2 Directive provides for fines of up to €10 million or 2% of annual global turnover, whichever is higher, for non-compliance by the entities concerned.

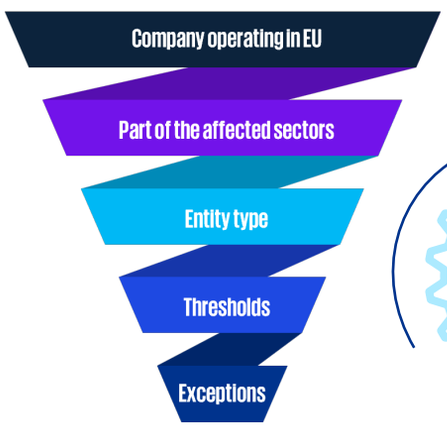
Better practices for preparation and implementation

The new NIS-2 specifications require intensive preparation, starting with an analysis phase to determine how a company is affected and a **readiness assessment** in the affected core areas.

On this basis, **necessary measures** can be defined and effectively implemented. Packages of measures such as governance, reporting and regulatory monitoring as well as workshops and training courses ensure implementation in line with requirements. This is particularly relevant against the background of management liability under NIS-2.

Based on and as a result of our analysis outlined above, you will receive a risk report from us that shows specifically to what extent your company is affected by the NIS 2 Directive, which areas are particularly critical and what measures should be taken.

The report contains the proposal of a concrete action plan for adapting to the requirements of the directive, including technical, organizational and legal steps. This allows you to respond to the requirements of the NIS 2 Directive in a targeted manner and prepare for the new obligations in good time.



Five steps of the impact analysis

Impact Analysis

An impact analysis is the first step in concretizing direct and indirect impacts in NIS-2 regulated sectors. This involves determining affected units, business processes and associated services, taking into account overarching processes, suppliers and customers, and thus identifying the degree of impact. Use our Quick Assessment to obtain an initial assessment of your impact.

Readiness Assessment

The readiness assessment forms the basis for an action plan. The aim of the assessment is to check how the company is prepared for the challenges ahead and which measures are still necessary.

NIS-2 Measures Implementation

Support for effective compliance with the NIS-2 directive and implementation of all necessary measures and requirements (such as IAM, incident response or BCM).

Workshops and Training

Conducting training courses and workshops with experienced and interdisciplinary experts with extensive knowledge in the areas of law, data protection, audit/revision, cyber security and technology.

Regulatory monitoring in implementation

The aim of regulatory monitoring is to include national characteristics, such as regulatory and official practice, into the implementation.

NIS-2-Governance

Ensure efficient management of NIS-2 measures to effectively fulfill the requirements.

Reporting to the Authorities

Design of the process for mandatory reporting to the relevant supervisory authority based on existing processes and systems for incident and crisis management.

Management liability risk under NIS-2

The standard of liability in the current draft of the German Implementation Act follows the framework of the NIS-2 Directive. Management boards in Germany are currently liable if they are grossly negligent in breaching obligations to ensure IT security.

The concrete standardization of duties in the NIS-2 significantly increases the de facto liability risk for management. If a specific obligation is not implemented, a breach of duty is likely.

At the same time, the specified canon of duties increases the risk that breaches of duty may also be considered gross negligence.

With the NIS-2 Directive, the EU thus confirms and reinforces the liability of management ("IT security is top management priority").

Who is part of the management?

Federal Executive Board, the respective executive boards and directorates/managing directors of the sponsors as well as the management of subsidiaries.

Duties of a management board

The legal standard is the breach of due diligence regarding IT security. Appropriate risk management measures (even without the enactment of the implementation law) are part of the duties of company management. Due to the generally increasing threat landscape and the corresponding legal addressing, this applies to a higher degree.

Standard of liability

The legal standard is the breach of the duty of care of a "prudent and conscientious manager" in the case of a stock corporation (AG) or "a prudent businessman" in the case of a limited liability company (GmbH). This means that even simple negligence may suffice.

Gross negligence

The more specific the duties of conduct are regulated, the more likely the accusation of gross negligence becomes. Especially if there are statutory regulations that are expressly directed at the management.

Risk

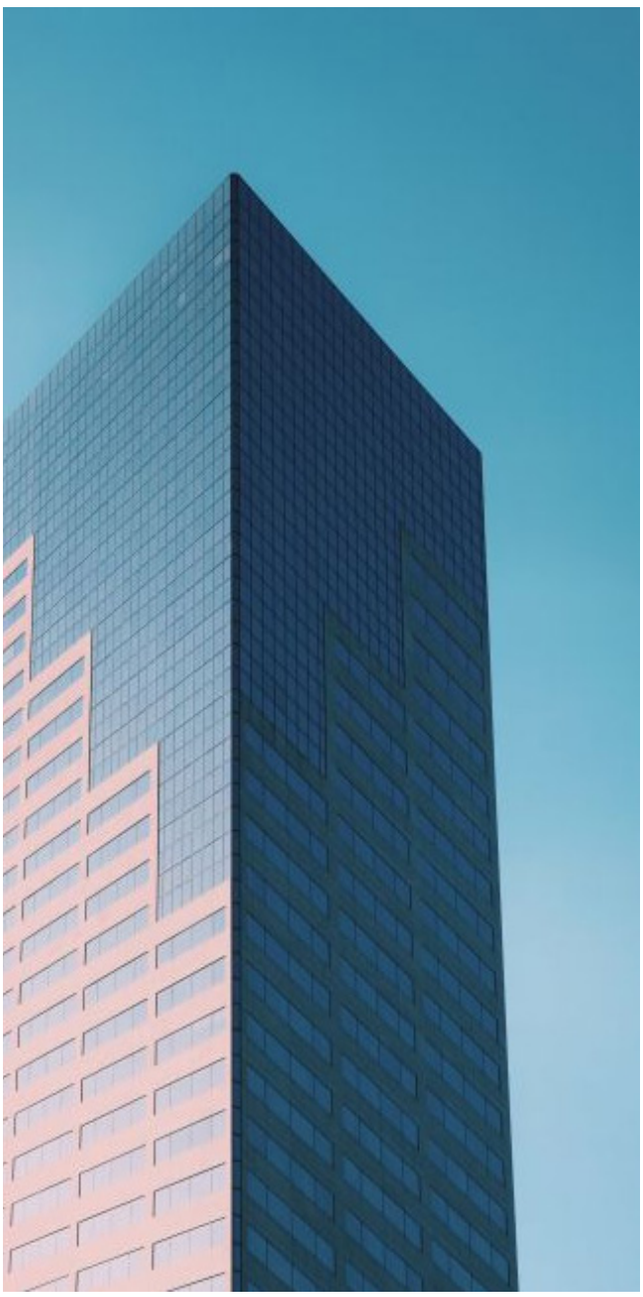
If, when making a business decision, the management could not reasonably assume that it had acted in the best interests of the company on the basis of appropriate information, the duty of care is breached. It must therefore be proven that a careful decision was made in the best interests of the company, taking IT security into account.

NIS 2 Directive: Responsibility without national law

The NIS-2 Directive sets new standards for cybersecurity and was supposed to be transposed into national law by October 17, 2024. As the legal implementation in Germany was not completed on time, the legal situation remains unclear - but the requirements of the directive still apply.

With the implementation laws coming into force in many EU countries, the obligations should already apply to many companies. In Germany, too, specific cybersecurity requirements from NIS-2 can already come into effect due to the due diligence standard based on the state of the art and generally recognized standards, so that NIS-2 can in fact already take effect independently of a national implementation law. Companies should therefore not rely on delayed legislation but should address the existing requirements at an early stage.

The NIS-2 Directive makes the implementation of cyber security a corporate duty. Those who take measures at an early stage can not only minimize regulatory risks, but above all strengthen the resilience of their own company.



Immediate effect

Specific requirements for cybersecurity from the NIS-2 Directive are already having an impact due to the diligence standard that must be aligned with the state of the art and generally accepted standards, which will be applied in assessing the personal liability of the management. In the event of security incidents, legal liability issues arise directly - also in connection with data protection requirements.

Specific requirements from NIS-2

The measures already to be implemented include, in particular, the performance of regular risk analyses, the implementation of technical and organizational cyber security measures (e.g. firewalls, intrusion detection system (IDS)/intrusion response system (IRS), encryption), the establishment of an incident management system and the documentation and verification of these measures, even if the law is not yet in force.

Corporate responsibility

Early, appropriate implementation protects against regulatory uncertainties.

Clear internal processes to fulfil the requirements are crucial.

Risks of lack of action

Delays increase the risk of compliance issues. The German NIS-2 Implementation Act is not expected to contain any transitional periods for the implementation of the obligations. As soon as the law comes into force, the NIS 2 obligations will apply directly to affected companies.

Why KPMG?

KPMG helps organizations navigate the complexities of the NIS-2 Directive and its implementing legislation.

KPMG Law stands for comprehensive legal expertise combined with in-depth industry knowledge and a global network.

Our lawyers have in-depth knowledge of IT law, data protection and cyber security. Our clients benefit from our ability to translate complex technological issues into a clear legal framework while always keeping the business objectives in mind.

KPMG offers comprehensive advice to strengthen your network and information security.

Our cyber security experts offer you comprehensive advice and support in relation to NIS-2, the Cyber Resilience Act (CRA) and cyber incidents.

We carry out risk assessments, implement customized security solutions and train your staff to strengthen your company's cyber security.

Together

The close cooperation between KPMG and KPMG Law makes it possible to translate and implement the legal requirements in practice and, conversely, to seamlessly integrate findings from consulting into the legal strategies. This enables us to achieve a holistic view of our clients' risk landscape and compliance requirements. This collaborative approach has proven to be particularly effective as it not only helps our clients to meet compliance requirements, but also to optimize their business processes and strengthen their competitiveness.

Through our in-depth expertise and commitment to excellence, we can offer our clients not only legal certainty, but also a real strategic advantage in an increasingly complex and competitive market environment. KPMG provides solutions for organizations facing the dynamic challenges of cybersecurity, data protection and compliance.

Contact

KPMG Law
Rechtsanwaltsgesellschaft mbH

Francois Maartens Heynike
LL.M. Rechtsanwalt, Partner
Technology, Media & Telecommunication
T +49 69 95119-5770
fheynike@kpmg-law.com

Dr. Daniel Taraz,
Rechtsanwalt, Senior Manager
IT/Data/Digital
T +49 40 360994-5483
danieltaraz@kpmg-law.com

KPMG AG
Wirtschaftsprüfungsgesellschaft

Wilhelm Dolle
Partner
Consulting, Cyber Security & Resilience
T +49 30 2068-2323
wdolle@kpmg.com

Marko Vogel
Partner
Consulting, Cyber Security & Resilience
T +49 201455-8838
mvogel@kpmg.com

Dr. Michael Falk
Partner
Consulting, Cyber Security & Resilience
T +49 69 9587-3680
mfalk@kpmg.com

Jan Stoelting
Partner
Consulting, Cyber Security & Resilience
T +49 711 90604-2774
jstoelting@kpmg.com

kpmg.de/socialmedia

kpmg.de