January 2026

Current developments in Cybersecurity: Implementation of the NIS2 Directive in Germany and Cyber Resilience Act

On 13 November 2025 - after a delay of more than a year – the German Parliament (Bundestag) passed the Act on the Implementation of the NIS2 Directive and on the Regulation of Key Aspects of Information Security Management in the Federal Administration (NIS2UmsG). The law entered into force on 6 December 2025.[1] Article 1 NIS2UmsG amends and extends the Act on the Federal Office for Information Security and on Information Security in Institutions (BSIG). The NIS2UmsG also amends various federal laws, such as the Telecommunications Act and the Energy Industry Act.

Further European legal act concerning cybersecurity, specifically product security, entered into force on 10 December 2024: the Cyber Resilience Act (CRA)[2] . The CRA is a European regulation that sets minimum requirements on cybersecurity for all connected products and will be fully applicable in December 2027.

A. NIS2UmsG

In addition to reporting, information, verification and registration obligations, the NIS2UmsG provides for comprehensive mandatory risk management measures. These obligations are accompanied by far-reaching enforcement measures designed to boost the implementation of the NIS2 Directive. For example, Section 38 (2) BISG establishes manager liability (which is ancillary to the general provisions of company law) for violations of implementation, monitoring and training obligations. According to Section 65 (5) BISG, violations of the BISG are subject to fines.

I. Background

The NIS2UmsG transposes the NIS2 Directive into national law. For Germany, this means that the "regulatory framework created by the Act to Increase the

[1] https://www.recht.bund.de/bgbl/1/2025/301/VO.html.

[2] Also known as the "Cyber Resilience Regulation", https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402847.

Security of Information Technology Systems (IT Security Act) of 17 July 2015 (BGBl. I 2015, p. 1324) and the Second Act to Increase the Security of Information Technology Systems (IT Security Act 2.0) of 18 May 2021 (BGBl I 2021, p. 1122)" is extended and that requirements for the federal administration will be introduced. At the administrative level, a key element is the creation of the position of Federal Government Coordinator for Information Security, who coordinates the federal government's operational information security system and supports the ministries in implementing the requirements concerning the information security management.

II. Scope

The personal scope of application is extended by the NIS2UmsG in accordance with Art. 2 and Annexes I and II of the NIS2 Directive. While the NIS2 Directive distinguishes between essential and important facilities, the NIS2UmsG differentiates between particularly important facilities and important facilities, cf. Section 28 BSIG.

Companies must check for themselves whether they fall within the personal scope of application and are among the approximately 29,500 institutions supervised by the BSI. For this purpose, the BSI has provided a tool that companies can use to carry out an NIS2 impact assessment[3] . However, this assessment is only a guide based on the company's own information and is not legally binding. In particular, it does not replace the self-identification assessment and has no indicative effect on legal proceedings. Companies must therefore assess their own impact based on the following criteria, which depend on both the industry and the size of the company.

1. Particularly important facility

According to Section 28 (1) BSIG, a particularly important facility is:

No. 1: an operator of critical entities, i.e. a natural or legal person or a legally dependent organisational unit of a local authority which, taking into account the legal, economic and factual circumstances, exercises a decisive influence on one or more facilities which are active in the following sectors: energy, transport and traffic, finance, social security and basic security for job seekers, health care, water, food, information technology and telecommunications, space and municipal waste disposal, and which are of great importance for the functioning of the community, as the interruption or impairment of their functions would result in significant supply bottlenecks or threats to public safety (Section 28 (8) in conjunction with Section 2 No. 22, 24 BSIG); the individual types of facilities are specified in a statutory order to be issued by the Federal Ministry of the Interior pursuant to Section 56 (4) BSIG (Section 2 No. 22 BSIG).

No. 2: a qualified trust service provider, top level domain name registries or DNS service providers.

No. 3: a provider of publicly accessible telecommunications services or an operator of public telecommunications networks with at least 50 employees or an annual turnover or annual balance sheet total of more than 10 million euros.

No. 4: any other natural or legal person or legally dependent organisational unit of a local authority that offers goods or services to other natural or legal persons in return for payment and that can be classified as one of the types of entities referred to in Annex 1, and employs at least 250 employees or has an annual turnover of more than 50 million euros and an annual balance sheet total of more than 43 million euros.

[3] https://betroffenheitspruefung-nis-2.bsi.de/.

Federal administration institutions are excluded, provided they are not also operators of a critical entities.

2. Important facility

According to Section 28 (2) BSIG, an important institution is an institution which does not constitute a particularly important institution or part of the federal administration, but is

No. 1: a trust service provider, or

No. 2: a provider of publicly available telecommunications services or an operator of public telecommunications networks that employs less than 50 people and has an annual turnover or annual balance sheet total of 10 million euros or less, or

No. 3: any other natural or legal person or a legally dependent organisational unit of a local authority that offers goods or services to other natural or legal persons in return for payment and that is classified as one of the types of entities referred to in Annexes 1 and 2 (e.g. energy, transport and traffic, finance and healthcare, water, digital infrastructure, space) and employs at least 50 people or has an annual turnover and annual balance sheet total of more than 10 million euros in each case.

III. Obligations of operators of affected entities and facilities

The obligations of operators of relevant entities and facilities are set out in Part III, Chapter 2 of the BSIG. Essentially, the risk management measures (see III. 1.) and reporting obligations (see III. 2.) of the NIS2 Directive remain unchanged.

> In accordance with the NIS2 Directive, all operators of entities/facilities are subject to the same obligations under the NIS2UmsG.

1. Risk management measures

The risk management measures are regulated in detail in Section 30 BSIG. For reasons of proportionality, a distinction is made between the categories of facilities/entities in terms of the rigor of the respective measures. In paragraph 1, the requirements for particularly important and important facilities are stipulated in very general terms, paragraph 2 provides for specifications. Accordingly, the measures must be based on a risk-based approach that meets numerous minimum requirements, such as:

No. 1: Concepts relating to risk analysis and information technology security,

No. 2: Management of security incidents,

No. 3: Maintenance of operations, such as backup management and recovery after an emergency, and crisis management,

No. 4: Security of the supply chain, including security-related aspects of relationships with immediate suppliers or service providers,

No. 5: Security measures for the acquisition, development and maintenance of information technology systems, components and processes, including management and disclosure of vulnerabilities,

No. 6: Concepts and procedures for assessing the effectiveness of risk management measures concerning information technology security,

No. 7: Basic procedures of cyber hygiene, training and awareness-raising measures concerning information technology security,

No. 8: Concepts and procedures for the use of cryptographic methods,

No. 9: Development of concepts for staff security, access control and management of ICT systems, products and processes,

No. 10: Use of multi-factor authentication or continuous authentication solutions, secure voice, video and text communication, and, where appropriate, secure emergency communication systems within the respective entity/ facility.

2. Reporting obligations

The reporting obligations of the facilities and entities are set out in Section 32 of the BSIG. According to this, particularly important and important facilities must comply with the three-stage reporting system of the NIS2 Directive in the event of a significant security incident – early warning, official notification and reporting.

A security incident is an event that compromises the availability, integrity or confidentiality of stored, transmitted or processed data or the services offered or accessible via information technology systems, components and processes (cf. Section 2 No. 40 BSIG).

The security incident is considered significant if, according to Section 2 No. 11 BSIG, it

a) has caused or may cause serious operational disruptions to services or financial losses for the facility concerned; or
b) has caused or may cause significant material or immaterial damage to other natural or legal persons.

However, the bureaucratic burden on facilities should be minimized within the scope of implementation of the NIS2 Directive. The information to the BSI should be transmitted via a reporting option set up by the BSI in agreement with the Federal Office for Civil Protection and Disaster Assistance after consultation of the operators and trade associations concerned, cf. Section 32 (4) BSIG.

3. Further information obligations

In accordance with Article 23(1) sentence 2 of the NIS2 Directive, the BSI may, pursuant to Section 35 (1) BSIG, require operators of important and particularly important facilities to notify the recipients of the facility's services without undue delay if the significant security incident may affect the provision of the service. However, for simplified implementation purposes the notification may also be published online.

4. Further obligations

In addition, the NIS2UmsG also provides for additional facility-specific obligations, such as:

a. Registration obligations

According to Section 33 BSIG, there will be a registration obligation for particularly important and important facilities as well as for domain name registry service providers. The required data must be provided to the BSI. If the obligation is not fulfilled, the BSI may also carry out the registration process itself, cf. Section 33 (3) BSIG. Operators of critical entities are subject to stricter obligations under Section 33 (2) BSIG. In addition, Section 34 BSIG provides a specific registration obligation for certain types of facilities.

Facilities subject to the registration obligation must undergo a two-stage registration process.[4] The BSI recommends creating an account by the end of 2025, so that they can, in a second stop, register with the BSI portal (which has been newly developed in the context of the adoption of the NIS 2 Directive) from the beginning of 2026. The BSI portal is scheduled to go live on 6 January 2026 and will serve as a reporting center for significant security incidents.

b. Implementation, monitoring and training obligations for management

According to Section 38 (1) BSIG, the management of particularly important and important facilities is required to implement the risk management measures under Section 30 BSIG and to monitor their implementation. Pursuant to Section 38 (2) BSIG, the management is liable for damages incurred by the facilities because of a breach of the obligation under paragraph 1, either in accordance with existing general principles of company law, e.g. Section

[4] For more information, see https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/251205_NIS-2-Umsetzungsgesetz_in_Kraft.html.

93 (2) AktG, or – in the absence of existing liability provisions – in accordance with the BSIG.

> Section 38 (1) BSIG establishes obligations, the violation of which may lead to manager liability in accordance with the general principles of company law or, in the absence of such liability provisions, in accordance with Section 38 (2) BSIG.

c. Additional requirements for operators of critical entities

Section 31 BSIG imposes additional requirements on operators of critical entities. In particular, they are required to use threat detection systems for their IT systems, components and processes that continuously and automatically record and evaluate suitable parameters and characteristics of ongoing operations, cf. Section 31 (2) BSIG. The deployment of the threat detection system is, in turn, subject to the reporting obligation under Section 39 BSIG.

IV. Enforcement measures

1. Establishment of a "CISO Bund"

According to Section 48 BSIG, the Federal Government Coordinator for Information Security is responsible for coordinating the federal government's operational information security management and supporting the ministries in implementing the requirements concerning the information security management.

2. Warnings

Pursuant Section 13 (1) BSIG, the BSI may issue warning. These include:

a) Warnings about vulnerabilities and other security risks in information technology products and services,
b) Warnings about malware,
c) Warnings in the event of loss of or unauthorised access to data,
d) Information about security-related IT properties of products, and
e) Information about violations of the BSIG by particularly important facilities or important facilities.

3. Certifications

According to Section 52 (2) BSIG, it is possible to apply to the BSI for security or personal certification or certification as an IT security service provider for certain products or services at the BSI.

4. Voluntary IT security label

The BSI is introducing a uniform IT security label to inform consumers about the IT security of products in certain product categories specified by the Federal Office for Information Security, cf. Section 55 (1) BSIG. The label consists of a manufacturer's declaration and security information, cf. the legal definitions in Section 55 (2) BSIG. However, it does not make any statement about the data protection conformity of a product.

5. Imposition of fines and penalty payments

If a breach of one of the obligations listed above constitutes an administrative offence, cf. Section 65 (1)-(4) BSIG. A fine may be imposed in accordance with Section 65 (5) BSIG. With regard to the amount of the fine, paragraphs 6 and 7 distinguish between the types of facilities concerned.

B. Cyber Resilience Act

I. Overview

The Cyber Resilience Act harmonizes the rules on cybersecurity for products with digital elements within the EU. The aim is to guarantee trustworthy and reliable digital services across the EU. As a regulation, the CRA applies directly and does not require national implementation legislation as is the case with the NIS2 Directive. However, a transition period is provided in order for market operators to have to adapt and prepare for the new requirements. The CRA will be implemented in several stages[5] from the end of 2024 to the end of 2027:

- **11 June 2026:** The provisions on the notification of conformity assessment bodies (CABs) will apply.
- **11 September 2026:** Manufacturers of connected products are subject to the obligation to report actively exploited vulnerabilities and security incidents.
- **11 December 2027:** All CRA requirements apply, including compliance with essential cybersecurity requirements before a product is placed on the market, handling vulnerabilities throughout the product lifecycle, and transparency requirements towards users.

II. Scope

With a few exceptions, this covers all products with digital elements that are made available on the EU market and whose intended purpose or reasonably foreseeable use involves a data connection with a device or network (Art. 2 CRA). "Products" can be both hardware and software (Art. 3 No. 1 CRA).

III. Obligations of economic operators

The CRA imposes obligations on all operators along the value chain (manufacturers, importers, distributors, etc.). For the manufacturer of the products in question, the most rigorous obligations apply (Art. 13 ff. CRA). Their primary responsibility is to ensure that the products meet the requirements specified in Annex I, Part I of the CRA. These include, in particular

- maintaining a secure configuration of the product,
- the possibility of subsequent security updates,
- protection against unauthorised access, integrity, data minimisation, etc.

To this end, a risk assessment for the entire life cycle of the product must be carried out in advance. This assessment has to be included in the technical documentation of the product. After the product has been placed on the market, the manufacturer must provide regular cybersecurity support for the product for at least five years.

In addition, the manufacturer has information and reporting obligations in order to enhance transparency.
The manufacturer must demonstrate compliance with the requirements by way of a conformity assessment procedure (Art. 32 CRA). The exact nature of the procedure in an individual case is determined by the classification of the product into one of several risk classes. While a self-assessment may be sufficient for non-critical products, external conformity assessment bodies may need to be consulted for products with a higher risk. In this respect, the CRA distinguishes between different product categories.

The other parties along the value chain (importers and distributors, see Art. 19 ff. CRA) must, above all, verify that the manufacturers of the products meet (certain) requirements of the CRA. In addition, they

[5] https://digital-strategy.ec.europa.eu/de/factpages/cyber-resilience-act-implementation.

must cooperate with the market surveillance authorities.

IV. Imposition of fines and penalty payments

Violations of the CRA are subject to substantial fines (up to EUR 15,000,000 or up to 2.5% of the total worldwide annual turnover of the previous financial year, whichever is higher, see Art. 64 CRA).

C. Practical advice

Companies should critically examine whether they fall within the (personal) scope of the NIS2 Directive and thus the NIS2UmsG. If this is the case, the requirements of the NIS2 Directive and compliance measures should be identified immediately.

Based on experience, the implementation of security systems and concepts takes a long time, so we advise affected companies to start implementing the relevant measures without undue delay. This is urgently recommended, in particular in view of the management obligations established in the NIS2UmsG and the associated management liability.

We would be happy to support you in implementing a cybersecurity framework that complies with the requirements of the NIS2 Directive.

The recommendation to implement appropriate measures as early as possible also applies to the provisions of the CRA, even though some of the requirements of the regulation will not apply until the end of 2027.

Legislative developments at EU and national level continue to unravel. Just three years after the adoption of the NIS2 Directive, the Commission already proposed amendments to the NIS2 Directive in its Digital Omnibus draft of 19 November 2025. These concern the establishment of a "single entry point" for reporting security incidents in accordance with Art. 23 of the NIS2 Directive. This refers to an interface between companies and supervisory authorities to be provided by the EU, which companies should, in future, use to report security incidents.

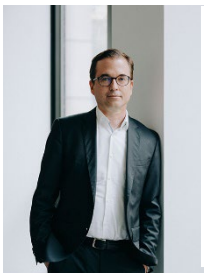
This client information merely contains a non-binding overview of the subject area addressed therein. It does not replace legal advice. The following persons are available as contact persons for this client information and for your consultation:

Dr Thomas Nägele
Partner
Intellectual Property

T +49 621 4257 222
E Thomas.Naegele@sza.de

Dr Marc Löbbe
Partner
Corporate law / M&A / Compliance

T +49 69 976 96 01 201
E Marc.Loebbe@sza.de



Dr Steffen Henn
Counsel
Intellectual property

T +49 621 4257 386
E Steffen.Henn@sza.de

Dr Anke Hofmann
Senior Associate
Intellectual Property

T +49 621 4257 222
E Anke.Hofmann@sza.de

Serpil Dilbaz, LL.B.
Associate
Intellectual Property

T +49 621 4257 222
E Serpil.Dilbaz@sza.de