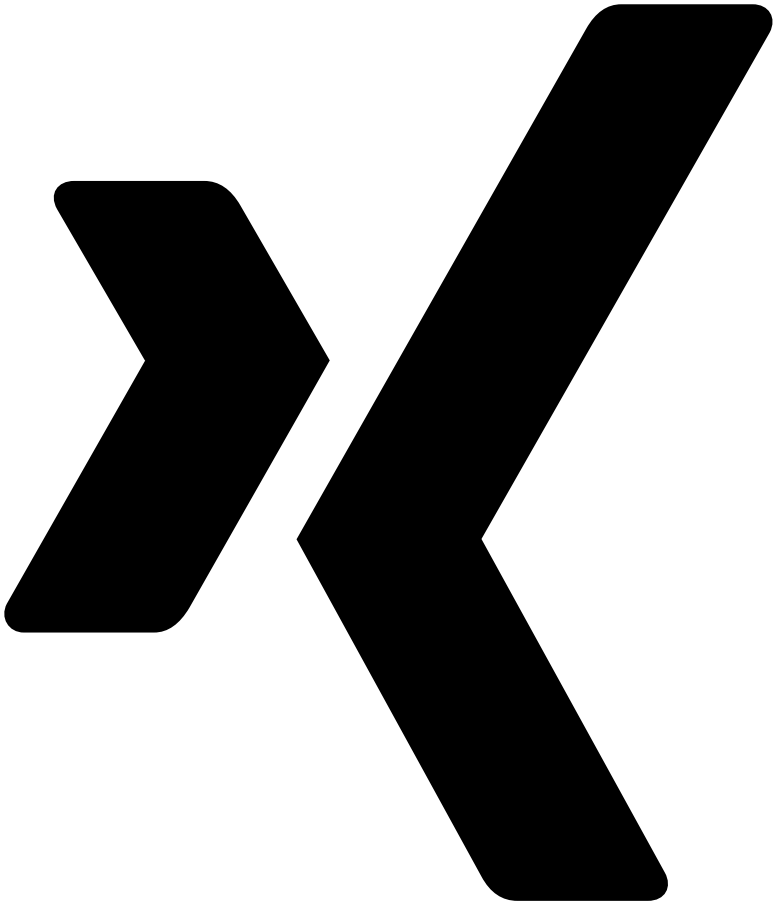
20.01.2026

[IT Security]

The German NIS2 Law: New cybersecurity obligations for companies

Share:







Quick read:

On 6 December 2025, the German NIS2 Transposition Law ('German NIS2 Law') entered into force. The Act transposes the European NIS2 Directive into German law, which introduces numerous new cybersecurity obligations for companies. The number of regulated entities in Germany will thus increase from around 4,500 to around 30,000. The core of the German NIS2 Law is the comprehensive amendment of the Federal Office for Information Security Act ('**BSIG**').

'Essential' and "important" entities covered by the BSIG must implement comprehensive IT security measures with immediate effect and without any implementation period, and must register with the reporting portal of the German Federal Office for Information Security ('**BSI'**) within three months of the

BSIG entering into force.

In addition, management may in future be held personally liable for violations of the BSIG. They must monitor the cybersecurity measures taken and regularly participate in cybersecurity training. In the event of violations, management faces personal liability internally and the company faces fines of up to 10 million euros or 2 percent of its global annual turnover.

1. Background to the regulation

By adopting the NIS2 Directive, European legislators aim to establish a high level of cybersecurity in the EU. The backdrop to this is the increasingly tense security situation: businesses and public authorities are increasingly exposed to attacks in the form of disinformation, hacking, espionage and sabotage. Not only critical infrastructure, but also all service providers operating in the public sector and performing key social functions are now increasingly targeted by cybercriminals. This is why the NIS2 Directive aims to strengthen the IT resilience of such institutions and, in turn, the German economy as a whole.

2. Target audience of the new regulations

Unlike the NIS1 Directive, which focused specifically on the regulation of operators of critical infrastructure (KRITIS), the ‘criticality threshold’ for the scope of application of the NIS2 Directive and the NIS2 Act has been lowered. As a result, the group of regulated entities has expanded significantly, and many entities that were not subject to cybersecurity obligations in the past will now fall within the scope of the BSIG. Against this backdrop, companies should urgently check whether the provisions of the NIS2 Act apply to them.

The German NIS2 Law classifies entities into essential entities (Sec. 28(1) BSIG) and important entities (Sec. 28(2) BSIG).

The following are considered essential entities:

- Operators of critical infrastructure (KRITIS),
- Qualified trust service providers (e.g. certain providers of electronic signatures or seals), top-level domain name registries or DNS service providers (regardless of their size),
- Providers of publicly available electronic telecommunications services or operators of public electronic telecommunications networks with at least 50 employees or an annual turnover and annual balance sheet total of

more than 10 million euros each, and

- Other companies listed in Annex 1 of the BSIG with at least 250 employees or an annual turnover of more than 50 million euros and an annual balance sheet total of more than 43 million euros (provided that the business activity is not negligible within the meaning of Art. 28 (3) BSIG).

Important entities are defined as all entities that:

- Employ at least 50 people or have an annual turnover and annual balance sheet total of more than 10 million euros,
- Belong to one of the sectors in Annex 1 or Annex 2,
- Do not carry out negligible business activities within the meaning of Art. 28 (3) BSIG, and
- Are not essential entities.

3. Essential obligations for companies affected

The BSIG contains both obligations that apply directly to the company and obligations that specifically address the company's decision-makers. The essential BSIG obligations include, in particular:

- **Registration obligation**: Essential and important entities must register with the BSI within three months (Sec. 33 BSIG). Registration is a two-step process via 'My Company Account' (MUK) and, since 6 January 2026, via the BSI portal.
- **Risk management measures**: Affected companies must take (documented) technical and organisational measures for IT security (Sec. 30 BSIG). These include at least the implementation of risk analysis, security incident management, backup management and disaster recovery, supply chain security, vulnerability management, employee training, cryptographic procedures, access control and multi-factor authentication. When implementing these measures, it is important to note that existing ISO/IEC 27001 certification covers part of the requirements, but is not sufficient to meet all of them.
- **Reporting obligations for security incidents**: Essential and important entities must report significant security incidents (via the BSI portal) (Sec. 32 BSIG).
- **Responsibility of management**: Management is obliged to implement and monitor risk management measures (Sec. 38 (1) BSIG). Personal liability may be incurred in the event of negligent breach of duties. In addition, management must regularly participate in cybersecurity training (Sec. 38 (3) BSIG).

4. Fines for non-compliance with the BSIG

The BSI may impose fines for non-compliance with the BSIG, such as inadequate risk management measures, delayed reporting of security incidents or failure to register on the BSI portal. Depending on the nature of the violation, essential entities face fines of up to €10 million or 2 per cent of their global annual turnover, whichever is higher. Important institutions face fines of up to €7 million or 1.4 per cent of their annual turnover for non-compliance.

5. What do companies need to do now?

As the new BSIG has already entered into force and does not provide for any transition periods, companies must now work with a clear roadmap for NIS2 implementation. This includes the following measures in particular:

- **Check whether you are affected**: sector affiliation, thresholds (employees, turnover, balance sheet total)
- **Prepare for registration**: Set up a MUK account; collect the necessary information; register with the BSI within three months of being affected
- P**erform a gap analysis/implement risk management measures**: Determine the current state of cybersecurity and compare it with the requirements of Sec. 30 BSIG; identify, prioritise and close gaps
- **Establish reporting processes**: Define internal reporting channels; assign responsibilities; create templates for 24-hour/72-hour/monthly reports
- **Involve and train management**: Ensure implementation is monitored; conduct regular cybersecurity training; define clear responsibilities.

Back to the news overview