German NIS 2 implementation ahead!

01 August 2025

The NIS 2 Directive (EU) 2022/2555 is intended to raise the level of IT security in Europe significantly. The directive applies not only to federal government authorities, but also to entities deemed essential or important in sectors considered particularly critical. In order to determine whether a company is subject to the regulation, it must first be established whether it operates within one of the affected sectors. Secondly, the company must meet certain thresholds in order to be classified as an essential or important entity. For the entities concerned, stricter requirements will apply to network and information systems, and reporting obligations will be expanded. Management responsibilities will also increase. The directive will affect significantly more companies and sectors than before. As well as broadening the scope within sectors already regulated under the NIS 1 Directive such as energy, transport and healthcare, the NIS 2 Directive now covers additional areas, including digital services, postal and courier services, wastewater and waste management, and 'manufacturers of critical products'.

After the previous German government failed to implement the directive on time, many companies were unaware of the specific steps they would be required to take (for details, see our briefing dated 7 February 7 2025). As a result of this delay, the EU Commission initiated infringement proceedings against Germany at the beginning of May 2025. The new German government has therefore made the implementation of the NIS 2 Directive a top priority, revising the previous draft of the NIS 2 Implementation Act within just a few weeks, coordinating it between ministries and submitting it to stakeholders for consultation. On 30 July 2025, the German government adopted the draft law entitled 'Act on the Implementation of the NIS 2 Directive and on the Regulation of Key Aspects of Information Security Management in the Federal Administration'. It will now make its way through the parliamentary legislative process and is expected to come into force by the end of the year.

Changes to the scope of application

The adopted draft is largely based on the previous German government's work. However, the new federal government has made some notable changes:

- The revised version now includes provisions for so-called operators of digital energy services. These services enable centralised access to the control of energy installations or decentralised energy consumption installations. Operators whose systems are connected to an energy supply network will be required to ensure adequate protection against threats to telecommunications and electronic data

processing systems necessary for the safe operation of these systems. Of particular relevance in this context is the potential risk posed by possible remote control by foreign manufacturers. This is particularly important in the construction of wind farms, for example. Consequently, the German BSI (Federal Office for Information Security) and the BNetzA (Federal Network Agency) will collaborate to establish procurement requirements for plant assets in an IT security catalogue. The aim is to ensure the desired level of protection comprehensively. The BNetzA will be responsible for updating the catalogue and monitoring compliance and will therefore obtain extended powers.

- Another notable aspect of the new draft bill is the removal of references to the German Kritis-DachG, a law designed to implement the EU's Critical Entities Resilience Directive (CER Directive). This directive was adopted alongside NIS 2 and aims to regulate protective measures against physical threats, including natural forces and sabotage. Nevertheless, the objective of establishing a joint reporting platform for the BSI and the Federal Office for Civil Protection remains unchanged.

- Another new provision is that a company's business areas will only be taken into account if they cannot be explicitly classified as "negligible" (Section 28 (3) BSIG-E). This is intended to avoid regulation under the NIS 2 requirements that is perceived as disproportionate if companies only carry out minor ancillary activities in the regulated areas.

Clarification of ambiguities regarding “negligible” business areas

Following the publication of the first draft bill by the German Ministry of the Interior the vague term "negligible business activities" caused considerable legal uncertainty. During the official stakeholder consultation, criticism was especially levelled at the fact that neither the law nor the explanatory memorandum provided clear criteria for when an activity can be classified as "negligible." Criticism was levelled at the fact that neither the bill nor the explanatory guidelines provided clear criteria for classifying an activity as 'negligible'. As a result, amendments were made to the draft at the last minute, introducing possible indicators for this classification, such as:

- the number of employees working in this area,

- the turnover generated by this business activity,

- the balance sheet total for this area, and

- a reference to certain business activities in a partnership agreement or a comparable founding document of the entity.

These interpretative guidelines are helpful. However, due to the exception for "negligible business activities," companies that are potentially exempt must now carefully assess whether this is indeed the case.

NIS 2 implementation will apply immediately

Finally, it should be emphasized that the new implementing law for the NIS 2 Directive provides no transitional period. All new requirements and penalties will apply immediately (presumably no later than 1 January 2026). From this date, deadlines for providing evidence and documentation to the German BSI will also begin, including the three-year period for operators of critical infrastructures under Section 39 BSIG-E.

Companies potentially affected by NIS 2 must urgently prepare, if they have not already done so, to avoid legal risks and fines. Furthermore, IT service providers delivering services to the newly regulated entities should anticipate that certain IT security obligations will be passed on to them.

***

BLOMSTEIN will closely monitor further developments and keep you informed. If you have any questions regarding the implementation of NIS 2 or other developments in German IT security law, Christopher Wolters, Leonard von Rummel, and Moritz Schuchert, and the entire team is ready to assist you.

BLOMSTEIN | We provide legal support to our international client base on competition, international trade, public procurement, state aid and ESG in Germany, Europe, and – through our global network – worldwide.