

# NIS-2 implementation in Germany – What's next?

07 February 2025

Last week it became official: Germany' will not implement the Directive (EU) 2022/2555 (known as the *NIS-2 Directive*) to improve cybersecurity in the EU under the current administration. See below for some guidance on what that means:

## Minimum requirements according to the NIS-2 Directive

On 16 January 2023, the NIS-2 Directive came into force at the European level. It replaced Directive (EU) 2016/1148 (known as the *NIS-1 Directive*). The NIS-2 Directive aims to establish a more coherent cybersecurity regime within the EU. Compared to the NIS-1 Directive, the scope of the NIS-2 Directive affects significantly more institutions and companies. While the NIS-1 Directive covered around 2,000 entities, up to 30,000 organizations are covered by the new Directive, according to the German Federal Office for Information Security (German only). In addition to the sectors already covered by the NIS-1 Directive, such as energy, transport and healthcare, the NIS-2 Directive now also includes additional sectors such as digital services, postal and courier services, wastewater and waste management, manufacturers of critical products and public administration. Covered entities, which the NIS-2 Directive divides into essential and important entities, are subject to significantly more comprehensive and specific cybersecurity measures. Among other things, the new Directive implements:

- New minimum requirements for the security of network and information systems
- Extended reporting obligations for cybersecurity incidents
- Stricter liability conditions for management

For breaches of the minimum security requirements and reporting obligations described above, maximum fines of up to 2% of the total worldwide annual turnover will be imposed in accordance with Art. 34 of the NIS-2 Directive, depending on the criticality of the entity.

## Delayed implementation in Germany

Germany has so far failed to implement the NIS-2 Directive on time. In the summer of 2024, the Federal Ministry of the Interior presented a first draft of a possible implementing law (the NIS2UmsuCG). However, the draft, which in some respects went beyond

the minimum requirements of NIS-2, failed to secure a majority in the German parliament after the end of the current coalition government. As a result, the legal situation for affected institutions and companies remains unchanged for the time being: Without a national transposition act, the NIS-2 Directive itself does not create any direct obligations for individuals. Even if the European Court of Justice has recognized the direct effect of directives in the past, this has only been to the benefit of private parties. In short: for the time being, entities covered by the NIS-2 Directive are not at risk of being fined for failing to implement the new cybersecurity requirements prescribed by the Directive.

The situation is different for the German Federal Government, against which the European Commission has initiated infringement proceedings due to the delayed implementation of NIS-2. For this reason, and of course because of the undeniable need for action in the area of cybersecurity, the future German government will have to tackle the implementation of NIS-2 without delay. However, it remains to be seen whether the future government will build on the existing draft. The CDU/CSU parliamentary group, which is expected to be part of the new federal government, has so far advocated a 1:1 transposition of the NIS-2 Directive into German law and has opposed the previous (in some places more far-reaching) draft for the NIS-2 transposition.

## **Recommended action for entities affected by NIS-2 in the future**

In view of the foreseeable legislative changes in German regulatory requirements for cybersecurity, companies should prepare themselves at an early stage, at least with regard to the minimum requirements of the NIS-2 Directive. The BSI's NIS-2 Impact Assessment (German only) provides a starting point for checking whether your company falls within the scope of the Directive and what obligations it will have to comply with in the future. However, due to the delayed implementation in Germany, there is still some time for internal company adjustments.

BLOMSTEIN will continue to monitor the implementation of NIS-2. Please contact Christopher Wolters, Leonard von Rummel and Moritz Schuchert at any time if you have any questions on how to deal with the developments in German IT security law.

\*\*\*