Hogan Lovells

Engage

Legal insights and analysis

NIS2 Directive: German government adopts draft NIS2 Implementation Act

25 July 2024

The 17 October 2024 deadline for the national implementation of the NIS2 Directive is fast approaching, leaving only little time for the German legislature to finalize the necessary legislative measures. As a much anticipated step, the German government finally adopted their first official draft of the German NIS2 Implementation Act on 24 July 2024. The updated legal framework will bring extensive obligations, sanctions, and country-specific requirements for approximately 30,000 companies operating in Germany. This article provides an overview of the current status of the German NIS2 implementation legislation and what this means for companies.

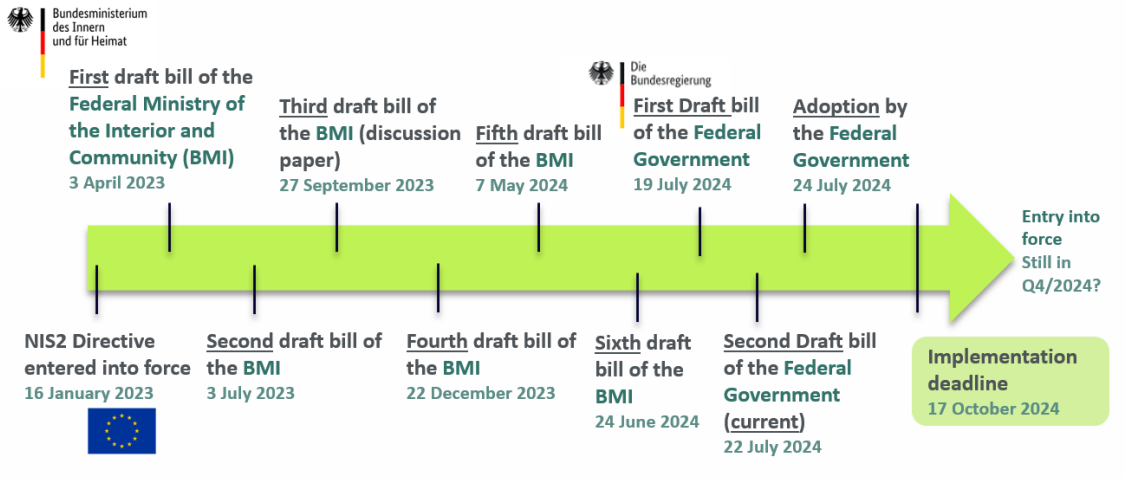
Background

In response to the increased frequency of cyberattacks targeting European companies and the significant economic and political impact resulting from such attacks the EU legislator enacted Directive (EU) 2022/2555 (**NIS2 Directive**; available here), which entered into force on 16 January 2023. This Directive builds upon and repeals (with effect from 18 October 2024) its predecessor, Directive (EU) 2016/1148 (**NIS1 Directive**). NIS2's primary objective is to raise the overall level of cybersecurity across the EU by harmonizing and strengthening cybersecurity measures. By doing so, NIS2 aims to address the disparities that arose from the national implementations of NIS1 among EU Member States. As a Directive, NIS2 does not apply directly in the Member States, but requires implementation into national law, leaving room for national particularities. Timewise, transposition needs to take place no later than 17 October 2024 (Art. 41 (1) NIS2 Directive). However, not all Member States seem to be on track to meet this deadline with the current status of legislative proceedings in Member States varying significantly. When and how national NIS2 implementations will be finalizes should therefore be monitored closely.

Timeline and Status of the Legislative Proceeding in Germany

Following the entering into force of NIS2, the German government swiftly initiated the legislative process for the German NIS2 implementation, with a first preliminary draft of the German NIS2 Implementation and Cybersecurity Strengthening Act (German: *NIS-2-Umsetzungs-* und *Cybersicherheitsstärkungsgesetz*, *NIS2UmsuCG*) having been published less than four months later by the Federal Ministry of the Interior and Community (BMI). In the following, however, the process stalled, with five further preliminary drafts being published before the German government finally adopted their

first official draft on 24 July 2024 (available in German here). Although this marks a significant step in the legislative process, the work is not done yet. Rather, the implementation act will still have to pass through the Federal Parliament. Whether Germany will meet the transposition deadline is therefore still uncertain.



Interplay with Other Regulations

The NIS2 implementation will happen in parallel to the implementation of Directive (EU) 2022/2557 (**Critical Entities Resilience (CER) Directive**; available here). The corresponding German draft for the CER Implementation Act (German abbreviated title: *KRITIS-DachG*; available in German here) focuses on implementing physical measures to strengthen the resilience of critical facilities. NIS2 and the German draft NIS2 implementation act on the other hand aim at enhancing the cybersecurity level. Despite these different scopes, there is some regulatory overlap.

This is particularly relevant for companies that classify as operators of critical infrastructure (German short form: *KRITIS*) and are therefore subject to the CER Directive (and its German implementation), as they will also be subject to the German NIS2 implementation. This is because these companies will also classify as essential entities pursuant to the German draft NIS2 implementation act. Companies in the KRITIS category must therefore navigate the requirements of both the CER Implementation Act and the NIS2 Implementation Act.

Key Points of the Draft NIS2 Implementation Act

The German draft implementation act, which is unofficially referred to as the “IT Security Act 3.0” (German: *IT-Sicherheitsgesetz 3.0*), involves amendments to various existing German laws (such as the Telecommunication Act or the Energy Industry Act), with a primary focus on the Act on the Federal Office for Information Security (German: *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen*; “**BSIG**”), which will undergo significant changes with a substantial number of new provisions, and serves as the overall basis for the German NIS2 implementation.

In addition to transposing the provisions of NIS2 into national law, the German draft NIS2 implementation act makes use of the leeway provided by NIS2, introducing modifications and providing specific guidance on the general requirements outlined in the Directive.

In particular, the draft contains regulations on the following points (non-exhaustive):

- **Designation of the BSI as competent authority**: The authority competent for enforcing the German NIS2 requirements will be the German Federal Office for Information Security ("**BSI**") (Sec. 1, 5 (3) no. 5 BSIG-Draft).
- **"Very important entities" and "important entities"**: Many of the changes and particularities within the draft NIS2 Implementation Act pertain to the definition of "very important entities" (corresponding to the notion of "essential entities" in the NIS2 Directive) and "important entities". The draft NIS2 Implementation Act indicates that the German legislator aims for a slightly broader scope of application than the NIS2 Directive.
    - For instance, to qualify as large sized enterprise under the NIS2 Directive (see Art. 2 (1) of the Annex to Recommendation 2003/361/EC), an entity must meet the following criteria:
        - >250 employees and
        - EUR >50 million annual turnover and/or a balance sheet total EUR >43 million.
    - In comparison, the current German NIS2 Implementation Act (cf. Sec. 28 (1) no. 4 BISG-Draft) defines a large sized enterprise, as follows:
        - >250 employees or
        - EUR >50 million annual turnover and a balance sheet total EUR >43 million
- **Key obligations:** The obligations that important and very important entities must comply with are specified in Part 3 Chapter 2 of the BSIG-Draft, and include, among others, obligations to
    - implement risk management measures and related documentation, including with regard to potential supply chains risks (Sec. 30 BSIG-D); the implementation of an Information Security Management System (ISMS) under international standards such as ISO27001 plays a crucial role in this regard; and
    - report incidents to the BSI in line with updated timelines under NIS2, starting with an initial notification within 24 hours (Sec. 32 BSIG-D), as well as to provide information in case of incidents to service recipients and/or the public upon instruction of the BSI (Sec. 35, 36 BSIG-D); and
    - register with the BSI within three months where an entity falls into the scope of the BSIG-Draft (Sec. 33, 34 BSIG-D); and
    - ensure robust governance on a company management level, including monitoring and training obligations for management members (Sec. 38 BSIG-D); and
    - audits in individual cases (Sec. 61, 62 BSIG-D).

For KRITIS (i.e. operators of critical infrastructure), additional stricter requirements apply, for instance with regard to risk management measures (Sec. 31 BSIG-D), specific audit obligations (Sec. 39 BSIG-D),

or reporting obligations regarding critical components (Sec. 41 BSIG-D).

- **Supervisory and enforcement measures**: The enforcement framework differentiates between measures against “very important entities” which must pro-actively comply with orders and specifications issued by the BSI (Sec. 61 BSIG-D, ex-ante enforcement) and “important entities” whose compliance with key obligations can be investigated and further enforced by the BSI (Sec. 62 BSIG-D, ex-post enforcement). Sanctions are set out in Sec. 65 BSIG-D and are linked to different types of infringements:
    - Fines of up to EUR 10 million/2% of the annual worldwide turnover for very important entities and EUR 7 million/1.4 % of the annual worldwide turnover for important entities e.g. regarding adequate risk-management measures and incident reporting; percentage fines are possible if the entities have an annual worldwide turnover of more than EUR 500 million (Sec. 65 (6) – (8) BSIG-D);
    - Fines of up to EUR 2 million/1 million for KRITIS (i.e. operators of critical infrastructure) regarding the obligation to provide proof for fulfilling the requirements of adequate risk-management measures;
    - Other fines of up to EUR 2 million/500.000/100.000 depending on the nature of the infringement.
- Possible personal liability: Notably, there are also increased personal liability risks for the board of directors with regard to their governance obligations (Sec. 38 BSIG-D).

With regard to the territorial scope, it is noteworthy that entities established or providing services in Germany as well as specific entities (e.g. DNS service providers, online marketplaces) with a main establishment in Germany or located outside the EU with a designated representative in Germany are covered by the German NIS2 Implementation Act (Sec. 59, 60 BSIG-D).

What’s Next?

The German implementation is still work in progress, leading to growing doubts whether the German legislator will meet the implementation deadline. Potentially affected companies should nevertheless monitor the legislative procedure in Germany closely in order to ensure that they can comply with the new obligations once they are finalized. Where companies are likely covered by NIS2, it is therefore recommended to perform

1. a NIS2 applicability assessment, which should include as assessment of the applicability of the German NIS2 Implementation Act; in case subsidiaries are located in different EU Member States, it is also recommended to evaluate the jurisdiction position and consider the location of the main establishment under the NIS2 framework; and
2. an impact assessment to identify compliance gaps with regard to applicable obligations to implement appropriate cybersecurity measures, incident procedures, governance framework and registration obligations.

On this basis, identified compliance gaps can be addressed in a subsequent implementation project which should take into account potential cross-border implications.

Authored by Dr. Henrik Hanssen and Anna Theresa Vogel.

We thank Mika Simon Haberlandt (paralegal in our Hamburg office), who contributed to the drafting of this article.