Missed opportunities: the NIS2 Implementation and Cyber Security Strengthening Act from a business perspective

On 7 May 2024, the Federal Ministry of the Interior (BMI) published the first official draft of the NIS2 Implementation and Cyber Security Strengthening Act (NIS2UmsuCG for short) and simultaneously launched the consultation with associations. The new draft bill contains some improvements, but has missed the opportunity to create legal clarity for businesses. Companies are still faced with almost impossible tasks.

The German NIS2 implementation

The NIS2 Directive was published in the Official Journal of the European Union (EU) on 27 December 2022 and entered into force on 16 January 2023. Member states have to transpose the directive into national law by 17 October 2024. Following a key issues paper, a discussion paper and several leaked drafts, each of which contained a different version of the NIS2UmsuCG, an official draft bill is now available.[1] The majority of the NIS2 Directive's requirements is to be implemented in the BSI Act (BSIG-E). A comparison between the last known version of the NIS2UmsuCG dated 22 December 2023 and the new version dated 7 May 2024 shows[2] that, in contrast to public bodies, there have only been a few relevant changes for companies.

Confusion of terms remains

The NIS2UmsuCG is confusing simply because it deviates from the official German version of the NIS2 Directive in terms of terminology. The latter divides regulated entities into *important* and *essential* ones, while the NIS2UmsuCG uses the terms *important* and *very important*. This is annoying, but would still be acceptable if it were not for numerous inaccuracies in the content. One example is the newly included definition of the term "space-based services". This term is used in the NIS2 Directive to define the space sector, but is not defined there. According to the NIS2UmsuCG, it should refer to services based on data and information either generated by or transmitted through space objects. In addition, the term is limited to services whose disruption may lead to wider cascading effects. This wording was taken from the recitals of the NIS2 Directive, but is used there in a different context - and not as a constitutive characteristic of a "space-based service". These two examples are characteristic of the carelessly drafted bill, which is likely to be partially contrary to European law.

[1] Draft of a NIS2 implementation and cyber security strengthening act, available at: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2umsucg.html (German).

[2] Comparison of the two versions, available at: https://draftable.com/compare/NjCpWUWyhpeH (German).

Scope of application contrary to European law

The NIS2 Directive contains numerous cyber security obligations for affected companies. However, even determining its scope of application poses considerable difficulties. Accompanied by numerous exceptions, it is based on a comprehensible basic idea: companies that carry out activities and provide services that fall under one of the two sectors listed in the annexes must implement the requirements if they are categorised as at least a medium-sized enterprise according to the EU Commission's definition of SMEs[3]. According to the clear concept of the NIS2 Directive, the entire legal entity must be taken into account when calculating the thresholds.

In contrast, Section 28 (3) BSIG-E provides for a significant restriction. For the calculation of the thresholds, only the business activity attributable to the type of organisation is taken into account. It is clear from the explanatory memorandum that only the part of a legal entity that actually carries out the activities listed in the annexes to the NIS2 Directive should be taken into account. If, for example, a large company only generates electricity on the side, it would be obliged to implement the cybersecurity requirements according to the concept of the NIS2 Directive, but not necessarily according to the German BSIG-E. However, there is no opening clause that would allow Germany to restrict the scope of application in this way. The provision is contrary to the clear wording of the NIS2 Directive and must be regarded as contrary to European law. Companies should therefore use the NIS2 Directive as a guideline when assessing whether they are affected or not.

No adjustment for energy producers

There is still no solution for the sprawling definition of the energy sector. The NIS2 Directive includes energy producers in its scope of application. For the definition, reference is made to Art. 2 No. 38 of the Internal Electricity Market Directive. It states succinctly that a producer is any natural or legal person who generates electricity. Whether this is an ancillary activity of the company is irrelevant. A photovoltaic system on the roof of the company building may therefore be sufficient to open up the scope of application. The NIS2UmsuCG refers to the German implementation law for the Electricity Directive for the definition. This does not change anything in terms of content. According to the Austrian draft for the Network and Information System Security Act (NISG) 2024, energy producers are only covered "if these activities are the main commercial or professional activity".[4] However, it remains to be seen whether this will succeed in restricting the sprawling scope of application in line with European law.

Clarifications on corporate IT sought in vain

With the providers of cloud computing services, data centre services and managed services, the NIS2 Directive also regulates traditional areas of corporate IT. At least for data centre services, the NIS2 Directive makes it clear in the recitals that in-house data centres are exempt. It is obvious that this also applies to the other services mentioned. However, the NIS2UmsuCG does not clarify that an IT department is not sufficient to bring a company within the scope of the NIS2 Directive. Corresponding

[3] SME definition of the EU Commission, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361

[4] Review draft of the Network and Information System Security Act 2024, available at: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Begut&Dokumentnummer=BEGUT_42FD65C8_76B7_40F0_97E3_BB29BDFC0CE9

clarifications and exceptions for organisations that are exclusively directly or indirectly owned by local authorities are, however, included. A comparable regulation for companies is desirable.

Chemical substances: worst-case scenario averted for the time being

Further problems with the NIS2 Directive arise from an unsuccessful reference[5] to the REACH Regulation. The latest version of the NIS2UmsuCG now contains a restriction, as does the current draft of the Austrian implementation law, to the effect that only companies that fall under category 20 of the statistical classification of economic activities in the European Community (NACE Rev. 2) are affected. This is a sensible restriction, but contradicts the wording of the directive. It remains to be seen whether this restriction is compatible with the NIS2 Directive. Affected companies should follow further developments closely.

Toxic mixture: trade with chemical substances

When defining the sector "production, manufacture and trade with chemical substances", the draft bill only refers to manufacturers and importers. However, the NIS2 Directive also regulates the trade with chemical substances and even mentions it three times: in the name of the sector, in the description of activities and by referring to the definition of distributor in the REACH Regulation. In the NIS2UmsuCG, trade is still mentioned in the title, but no longer in the description of the type of facility. As Germany has no possibility to exclude trade with chemical substances from the scope of application across the board, it can be assumed that this is a drafting error.

Liability of the management

Compared to earlier drafts there are changes to the regulations on the personal liability of management. According to the NIS2 Directive, institutions must be able to hold their management responsible for breaches of the Directive's requirements. In the older versions of the NIS2UmsuCG, a waiver of claims for damages against managing directors was generally excluded in Section 38 BSIG-E. This remains the case under the current draft. However, there is now an exception for settlements. A settlement between the management and the institution regarding claims for damages is possible if the content of the settlement is not grossly disproportionate to the existing uncertainty regarding the legal relationship. It remains to be seen how practicable this solution is. However, as the NIS 2 Directive does not specify how liability should be organised, there are no concerns under European law. It is also worth noting that the explanatory memorandum to the law now clarifies that the regulation is not intended to restrict the possibility of covering the liability risk by taking out D&O insurance. This clarification is to be welcomed so that capable managers are not deterred from responsible positions by incalculable liability risks.

Provisions on fines

The new BSIG-E has also made minor adjustments to the scope of fines. According to Section 61 (6) BSIG-E, a fine of up to 2% of the global annual turnover can be imposed on particularly important institutions if they violate mandatory risk management measures or reporting obligations. For particularly important institutions the maximum amount of the fine in these cases is 1.4% of global annual turnover. In any case the maximum fine is up to ten million euros for *very important* organisations and up to

[5] VDMA working paper: NIS2 and REACH , available at: https://www.reuschlaw.de/en/news/working-paper-nis2-and-reach/

seven million euros for *important* organisations. The German legislator is thus orientating itself towards the minimum maximum amount stipulated by the NIS2 Directive.

What happens next?

The official draft bill was published to mark the start of the consultation process for associations. Comments can be submitted until 28 May 2024. A hearing will take place on 3 June 2024. However, there is only a short time left until 17 October 2024. It is very unlikely that the draft bill will pass the Bundestag, be signed by the Federal President and published in the Federal Law Gazette by then. As long as the NIS2 Directive has not been transposed into national law, it will not result in any obligations for companies.[6] '

First aid for companies

Affected companies do not have to fulfil the requirements in Germany until the NIS2UmsuCG has been published in the Federal Law Gazette. However, as the fulfilment of the new requirements is associated with considerable effort, companies should start implementation at an early stage. Companies can only be recommended to orientate themselves on the wording of the NIS2 Directive itself. If no changes are made as part of the legislative process, one or other of the provisions of the NIS2UmsuCG will probably only have a short half-life. It is also already clear that the NIS2 Directive completely fails to achieve the goal of harmonising cybersecurity law across Europe.

Conclusion

Although the new draft bill contains some improvements, it does not solve the fundamental problems of the NIS2 Directive. The German legislator has missed several opportunities to create legal clarity. Instead of a political tug-of-war between the ministries and an entanglement of the NIS2UmsuCG with other political demands, pragmatism and clarification of the open legal issues at European level are now required in the further legislative process. It remains to be seen whether this will succeed.

(Status: 10/05/2024)

Next Step: get in touch with us!

We will be happy to support you with any questions you may have about how you are affected by the NIS2 Directive and how you can implement the requirements in your company. We would be happy to explain our approach to you in detail in a personal meeting. Contact us now without obligation!

T + 49 681 / 859 160 0
E info@reuschlaw.de

[6] NIS2 Directive: Verpasst Deutschland die Frist zur Umsetzung (Is Germany missing the deadline for implementation), German article, available at: https://www.linkedin.com/pulse/nis2-richtlinie-verpasst-deutschland-die-frist-zur-umsetzung-hessel/.