CERHA HEMPEL
CEE NEWSLETTER
Austria

# The Network and Information Systems Security Act 2026

Transposition of the NIS 2 Directive in Austria

Following a protracted legislative process, the Austrian legislator finally transposed the European Union's NIS 2 Directive into national law at the end of last year – more than a year behind schedule – by enacting the Network and Information Systems Security Act 2026 (NISG 2026). The NISG 2026 will enter into force on 1 October 2026, but it is already making its presence felt due to the extensive list of obligations it introduces and the significant time and effort required to implement it.

The NISG 2026 establishes regulations to ensure the security of technical systems in companies, public authorities, and a wide range of other entities. The new legislation builds upon the NIS 1 Directive adopted in 2016, which was transposed into Austrian law in 2018 by the Network and Information Systems Security Act (NISG). Whereas the first NISG had a very limited scope of application – affecting fewer than 100 critical infrastructure companies in light of its narrow material scope of application – the NISG 2026 applies to a far larger number of companies and public bodies in Austria (with estimates suggesting up to 5,000 companies might be affected). Unlike under the first NISG, whether the NIS rules and requirements under the NISG 2026 apply to a company will no longer be determined by the NIS authority adopting an official decision. Instead, companies must conduct a self-assessment, which from a legal perspective is extremely challenging due to the vague wording used in the sector definitions and given the complex rules governing aggregation determining the scope of application of the NISG 2026.

Broadly speaking, the obligations under the NISG 2026 can be divided into two categories: Firstly, entities are required under the NISG 2026 to implement technical, organizational, and operational risk management measures to ensure they have attained an appropriate risk level. Secondly, reporting and information obligations toward authorities and customers must be satisfied under the NISG 2026.

Among the obligations related to risk management measures, particular emphasis should be placed on those directed specifically at management bodies; namely, the obligation to participate in training and ensure and oversee compliance with risk management measures (Section 31 of the NISG 2026). Furthermore, with regard to risk management, the entity must implement a variety of measures, including in the areas of (1) monitoring and logging of IT and OT, (2) incident handling, (3) business continuity and crisis management, (4) supplier management, (5) the development, maintenance, and operation of IT and OT, (6) personnel, (7) access control, (8) asset management, and (9) environmental security, with a view to establishing an appropriate level of cybersecurity for the entity. These measures have already been specified by the European Commission in Commission Implementing Regulation (EU) 2024/2690 for entities operating in certain economic sectors and they are to be fleshed out in more detail for the other entities by an ordinance yet to be issued by the Austrian Cybersecurity Agency. Based on current information, however, this ordinance will likely refer to the requirements set out in Commission Implementing Regulation (EU) 2024/2690 and also declare these to be applicable to all other entities subject to the NISG 2026.

Media owner and publisher: **CERHA HEMPEL Rechtsanwälte GmbH**, Parkring 2, A-1010 Vienna | Tel: +43 1 514 350 Fax: +43 1 514 35 35 | email: office@cerhahempel.com | Although this newsletter was created with the greatest of care, we nevertheless do not accept any responsibility whatsoever for its content being correct, complete or up to date | **Visit us at www.cerhahempel.com** | **CERHA HEMPEL** Austria Bulgaria Czech Republic Hungary Romania Slovak Republic Slovenia

With regard to the reporting and information obligations under the NISG 2026, the entity must first register with the Cybersecurity Authority (Section 29(2) of the NISG 2026) and, as part of a self-declaration, it must submit information on the risk management measures it has implemented (Section 33(1) of the NISG 2026). Subsequently, a report by an independent body must be submitted, if requested by the Cybersecurity Authority, which verifies that the risk management measures implemented have been assessed (Section 33(2) and (3) of the NISG 2026). Furthermore, the authority and, where applicable, customers must be informed on a case-by-case basis if a significant cybersecurity incident has occurred (Section 34(1) to (3) of the NISG 2026).

Given the multitude of obligations and the significant time and effort involved, companies should assess in a timely manner whether they fall within the scope of application of the NISG 2026. If the entity is subject to the NISG 2026, it must evaluate whether the risk management measures currently implemented by the entity satisfy the requirements under the NISG 2026 and which measures need to be taken to address any gaps. Furthermore, it is necessary to verify whether the risk management measures that have been implemented and those yet to be implemented have been documented in accordance with the requirements laid down in the NISG 2026. Finally, entities must establish reporting channels to ensure timely compliance with reporting obligations.

## Authors

Dr. Hans Kristoferitsch LL. M.
Partner
hans.kristoferitsch@cerhahempel.com
+43 1 514 35 290

Dr. Felix Krysa
Senior Associate
felix.krysa@cerhahempel.com
+43 1 514 35 537

Media owner and publisher: **CERHA HEMPEL Rechtsanwälte GmbH**, Parkring 2, A-1010 Vienna | Tel: +43 1 514 350 Fax: +43 1 514 35 35 | email: office@cerhahempel.com | Although this newsletter was created with the greatest of care, we nevertheless do not accept any responsibility whatsoever for its content being correct, complete or up to date | **Visit us at www.cerhahempel.com** | **CERHA HEMPEL** Austria Bulgaria Czech Republic Hungary Romania Slovak Republic Slovenia