EXPERT INSIGHTS | 24 SEPTEMBER 2024

NIS2 in a European country comparison:

How are the member states implementing the new EU cybersecurity legislation?

Overview

"The new European Cybersecurity Directive (NIS2), which makes securing IT systems a cross-industry compliance obligation, **must be implemented by the European member states by October 17, 2024.** The countries are taking very different approaches, as the following comparative study shows. The key finding: just as there is no single way for the companies concerned to implement NIS2, there is no single way for the EU member states to implement the European directive."

Prof. Dr. Dennis-Kenji Kipker
Research Director

CYBER|INTELLIGENCE
.Institute

Contents

Austria

The NIS2 Directive has not yet been implemented in Austria, but the legislative process is at an advanced stage, at least in terms of content.

On April 3, 2024, the draft of an implementation law at federal level, including a comprehensive annex, was submitted to the public, with which the Network and Information System Security Act 2024 is to be enacted and the Telecommunications Act 2021 and the Health Telematics Act 2012 are to be amended. On June 19, 2024, the Austrian Parliament announced the national implementation of NIS2, but the bill was rejected by the National Council on July 4, 2024, which means that the timely implementation of the directive has failed for the time being. With regard to the technical and organizational measures to be implemented by operators, **the draft contains a special feature that goes beyond the requirements of NIS2: Appendix 3 describes in detail individual measures for risk management measure areas in the form of a tabular list with specifications** in the areas of governance bodies, security policies, risk management, asset management, human resources, basic cyber hygiene measures and cyber security training, supply chain security, access control, security in procurement, development, operation and maintenance, cryptography, handling of cyber security incidents, business continuity and crisis management as well as on environmental and physical security, thus emphasizing the holistic approach of NIS2. It can be assumed that NIS2 will no longer be implemented in Austria in time for October 17, 2024.

Belgium

The NIS2 Directive has already been implemented in Belgium.

On April 18, 2024, the Belgian Parliament passed the corresponding national transposition law entitled "Law establishing a framework for the cybersecurity of networks and information systems of general interest for public security", which will enter into force on October 18, 2024 in accordance with European requirements. In addition, a royal decree was published on 9 June 2024, which implements and specifies the legal provisions. The Centre for Cyber Security Belgium (CCB) and the National Crisis Center (NCCN) are responsible for the implementation of NIS2, including the national cyber emergency plan from 2017. This body must also be notified of significant cyber security incidents, as it acts as the national CSIRT. NIS2 is implemented nationally as part of the Belgian initiative "Safeonweb@work." Among other things, this is where the institutions affected by NIS2 are registered. **In principle, essential and important institutions and providers of domain name registration services have five months to register once the law comes into force. As the entry into force is scheduled for October 18, 2024, registration must be completed by March 18, 2025 at the latest.** Institutions in the digital sector have the option of registering by December 18, 2024. **For the implementation of risk management measures in accordance with NIS2, the CCB refers to the "CyberFundamentals Framework,"** which covers all aspects of the NIS2 minimum catalog (https://at-work.safeonweb.be/de/tools-resources/cyberfundamentals-framework).

Czech Republic

In the Czech Republic, the NIS2 Directive has not yet been implemented and the legislative process is at an advanced stage.

The draft bill for a new cybersecurity law (NZKB) to implement NIS2 was submitted to the Government Legislative Council at the end of 2023. On July 17, 2024, the Government of the Czech Republic approved the proposal by resolution and submitted it to the Chamber of Deputies the following week on July 25, 2024. In September 2025, the bill is currently undergoing further parliamentary deliberation. The National Office for Cyber and Information Security (NUKIB), which has created an information website on the implementation of NIS2 in the Czech Republic (https://portal.nukib.gov.cz/), is centrally involved in the legislative process. **A special feature of the Czech implementation is the linking of NIS2 with a comprehensive legal mechanism for assessing supply chain security as a measure that goes beyond the European requirements and is therefore controversial in terms of legal policy.** It is currently assumed that at least 6,000 new companies will be covered by the requirements. The requirements to be met by the affected institutions are to be specified in part by subordinate decrees of the NUKIB. The cyber security measures to be implemented are divided into two different risk categories of operators, which have to meet lower and higher requirements. The respective catalogs reflect the requirements to be met in a very high level of detail. It is currently assumed in the Czech Republic that the new Cybersecurity Act will come into force on January 1, 2025.

Denmark

In Denmark, the NIS2 Directive has not yet been implemented and the legislative process is at an advanced stage.

Originally, national implementation was to take place as soon as possible, but due to the complexity, there have been delays in the legislative process. In Denmark, the Ministry of Defense is responsible for implementation and presented a basic draft law on 5 July 2024. **This basic national law only creates the general framework for NIS2 in Denmark. The sector-specific requirements will be determined by the relevant ministries, which will issue national NIS2 implementing regulations.** The energy, finance and telecommunications sectors are not subject to the main national NIS2 law. The Danish Center for Cybersikkerhed (CFCS) has the task of assisting with the content of the sectoral requirements. It can currently be assumed that Denmark will not transpose the NIS2 Directive into national law on time by October 17, 2024, as legislative activities are planned until at least the end of October.

Finland

In Finland, the NIS2 Directive has not yet been implemented and the legislative process is at an advanced stage.

On December 29, 2022, it was decided to set up a corresponding working group for the national implementation of NIS2 within the Ministry of Transport and Communications. The first draft bill was published for public consultation in November 2023 and on May 23, 2024, the government submitted a legislative proposal to the Finnish Parliament for the national implementation of NIS2. **The content of NIS2 implementation in Finland is likely to be based on the European minimum requirements, so the draft does not specify any extensions to the scope of application or obligations.** A new Finnish Cybersecurity Act is to be drawn up for national implementation, the monitoring of compliance with which is not to be centralized, but rather transferred to sector-specific authorities. The responsible supervisory authorities would be the Finnish Transport and Communications Agency (Traficom), the Energy Agency, the Finnish Safety and Chemicals Agency, the South Savo Centre for Economic Development, Transport and the Environment, the Finnish Food Administration, the National Welfare and Health Inspectorate (Valvira) and the Finnish Medicines Agency (Fimea). The national cyber security center is in charge of the Finnish CSIRT. It is expected that NIS2 can still be implemented in Finland on time by October 17, 2024, with national implementation deadlines scheduled after this date.

France

In France, the NIS2 Directive has not yet been implemented and the legislative process is still at an early stage.

The legislator is working with the French National Agency for Cybersecurity (ANSSI) on implementation. The first draft of the national implementation law is still being structured. The legislative process in France was interrupted by the dissolution of the National Assembly and the NIS2 implementation law must therefore be put back on the parliament's agenda. The bill was actually due to be presented to the Council of Ministers on June 12, 2024. However, following the dissolution of the National Assembly, the presentation of the draft law was postponed. As part of the project to implement the NIS2 Directive, the ANSSI held consultations over several months with the professional associations of the sectors affected by the Directive on the one hand and with the associations of elected representatives of local authorities on the other. These dialog sessions made it possible to obtain the opinions of the various stakeholders in order to guide the future text implementing the Directive. They will be continued during the regulatory phase and later during the implementation of the Directive. The results of these consultations were presented on two dates in April and May 2024. In total, it is estimated that around 15,000 French companies and local authorities will be subject to the new cybersecurity obligations. The scope of activity has been extended to 18 sectors, with additions such as healthcare, digital service providers or municipalities with more than 30,000 inhabitants. The French government, together with the ANSSI, has published an official information page on NIS2: https://monespacenis2.cyber.gouv.fr/.

Germany

The NIS2 Directive has not yet been implemented in Germany, but the legislative process is at an advanced stage, at least in terms of content.

In Germany, various unofficial and official draft versions (draft bills) have been published by the Federal Ministry of the Interior, which is responsible for implementation, since April 3, 2023. The official government draft was adopted on July 22, 2024, which means that the national implementation law will now be transferred to the ordinary legislative procedure in the national parliament, the Bundestag. The nationally proposed risk management measures are essentially based on the catalog specified by NIS2 itself. **For the reporting procedure of cyber security incidents, the draft version proposes a clearly graduated catalog that distinguishes between an early initial report, a confirmatory initial report, the interim report, the progress report and the final report. A characteristic feature of the national implementation in Germany is the comprehensive exclusion of public-law institutions from the scope of application of NIS2.** The legislative process will continue after the parliamentary summer break in the fall of 2024. It can be assumed that NIS2 will no longer be implemented in Germany in time for October 17, 2024, but that the national implementation "NIS2 Implementation and Cyber Security Strengthening Act" (NIS2UmsuCG) will only come into force at the beginning of 2025.

Greece

In Greece, the NIS2 Directive has not yet been implemented and the legislative process is at an advanced stage.

An initial draft bill entitled "National Cybersecurity Authority and Other Provisions" was published for public comment on January 3, 2024. On August 28, 2024, the bill was submitted to the Council of Ministers by the Greek Digital Minister. **In addition to the companies defined according to European benchmarks, the central government, the regions and the municipalities are also affected.** The Greek draft designates the National Cyber Security Authority (NCSA) as the authority solely responsible for implementation. The Greek draft places particular emphasis on improving cooperation between the public and private sectors, the strategic planning of national cyber security and the definition of a framework for the coordinated disclosure of vulnerabilities. For the comprehensive implementation of NIS2, training programs are to be developed in Greece in cooperation between public and private bodies, **offering the possibility of certification and thus contributing to the creation of a uniform domestic cybersecurity ecosystem. It is quite possible that NIS2 will be implemented in Greece in time for October 17, 2024.**

Hungary

The NIS2 Directive has already been implemented in Hungary.

The national transposition law came into force on May 23, 2023 following a consultation phase. According to the Hungarian transposition, affected companies had to register online with the Hungarian Supervisory Authority for Regulated Affairs (SARA) by June 30, 2024. Companies affected by NIS2 in Hungary are divided into different risk classes, starting with a basic level, qualified requirements up to a high security class that must be complied with. The detailed requirements to be met by companies are specified in a ministerial decree, the Cyber Science Act, which came into force on June 24, 2024. Cyber security incidents in Hungary must be reported to the National Cyber-Security Center. **Further deadlines in Hungary are October 18, 2024, by which the ordered cyber security measures must be implemented, December 31, 2024, by which a contract with a qualified information security auditor must be concluded, and December 31, 2025, by which the first information security audit must be completed. The "Cyber Science Act" is particularly relevant for the Hungarian implementation of NIS2 in practice: The 120-page document contains precise specifications for cyber security certification** and monitoring with regard to risk management, a catalog of measures and a catalog of hazards. The catalog of measures includes more than 160 test points for the "simple" protection class, more than 300 for the "significant" protection class and almost 400 mandatory test and inspection points and associated measures for the "high" protection class. The regulation also contains around 530 additional protective measures, the application of which is not mandatory in principle, but which companies can consider integrating into their information security management system depending on their sector and area of activity. The protective measures are divided into a total of 19 categories, including access control, training, system monitoring, business continuity, security incident management and supply chain security.

Italy

The NIS2 Directive has already been implemented in Italy.

On August 7, 2024, the Italian Council of Ministers met and decided on the national implementation of NIS2 in a corresponding legislative decree. The obligations arising from NIS2 will therefore come into force in Italy on October 18, 2024. The content of the proposed cybersecurity measures essentially corresponds to the requirements set out in the NIS2 Directive. The National Cybersecurity Agency ACN can specify the requirements. **It is noticeable in the scope of application that, for example, legal services for large food retailers are also covered by the regulations, as well as the cultural sector, as the latter has a significant added value in Italy.** According to preliminary estimates by the Director General of the Italian National Cybersecurity Agency ACN, around 50,000 additional companies in Italy will be covered by NIS2. From October 18, 2024, the ACN will set up a platform where all companies affected by NIS2 will have to register. The entities concerned must provide a list of their activities and services. From January 1 to February 28, 2025, key entities can register on the platform or update their registration. For providers of domains, cloud computing and data centers, the deadline will be brought forward to 17 January 2025. The ACN will provide feedback to the affected entities by March 31, 2025, at which point national implementation will also begin. The obligations to comply with the directive begin on the date of the ACN's notification to those affected and last 9 months for incidents and 18 months for obligations relating to administrative bodies and security measures.

Netherlands

The NIS2 Directive has not yet been implemented in the Netherlands, but the legislative process is at an advanced stage, at least in terms of content.

The draft law implementing the directive, known as the “Cybersecurity Act”, was released for public consultation on May 21, 2024, with the consultation period ending on July 1, 2024. The National Cybersecurity Center (NCSC) is expected to be responsible for implementation in the Netherlands. In contrast to the text of the NIS2 Directive and many other national implementations, **the latest version of the Dutch draft law does not describe a minimum catalog of cybersecurity due diligence obligations. Instead, the specific requirements are to be determined by a general decree, which can also be tailored to sector- specific characteristics.** It can be assumed that NIS2 will no longer be implemented in the Netherlands in time for October 17, 2024. Instead, the Dutch government assumes that the national implementation law will not come into force until the second or third quarter of 2025.

Poland

In Poland, the NIS2 Directive has not yet been implemented and the legislative process is at an advanced stage.

On April 23, 2024, the Polish Ministry of Digital Affairs made available a draft amendment to the Act on the National Cyber Security System (NCSSA), which is intended to integrate the NIS2 Directive into the Polish legal system. **The special feature of the currently proposed Polish NIS2 implementation is that it goes beyond the European requirements in some respects - also known as “gold plating”. For example, NIS2 should also apply to providers of managed cybersecurity services, regardless of their size. The provisions of the national implementation law should also apply to all public institutions regardless of their size.** Another special feature of the national implementation in Poland is the handling of hardware and software suppliers, which is also to be included in the implementation law, but is not directly linked to NIS2 in terms of content. For example, the Ministry of Digital Affairs is to be enabled to carry out procedures to determine a supplier as a high-risk supplier. This applies not only to the 5G network, but in principle to all areas of technology in which products and services are used whose origin may pose a threat to state security. **Overall, the Polish draft is significantly more administrative than comparable drafts in the EU.** Particularly noteworthy from this point of view is the possibility of issuing immediately enforceable, publicly announced cybersecurity protection orders that affected entities must comply with, for example to install a security patch, reset software or carry out a risk assessment. It can be assumed that NIS2 will no longer be implemented in Poland in time for October 17, 2024. In fact, it is now considered certain that the national law will not come into force until 2025.

Spain

In Spain, the NIS2 Directive has not yet been transposed and the legislative process is at an initial stage.

Information on a draft transposition law is currently not publicly available, nor are any significant public consultations on the national implementation of the directive known. **According to information from the responsible Spanish Ministry of the Interior in April 2024, work is underway to transpose NIS2 into Spanish law on time, but as no drafts have yet been publicly communicated and discussed, this seems rather unlikely.** In addition to the implementation of NIS2, the political approach of establishing an autonomous cybersecurity authority in Spain has been communicated. To date, the Spanish cyber security authority INCIBE has published a continuously updated FAQ on the implementation of NIS2 (https://www.incibe.es/incibe-cert/sectores-estrategicos/FAQNIS2#indice) as well as a compliance table for resources and services (https://www.incibe.es/empresas/blog/cumpliendo-con-la-nis2-recursos-y-servicios-para-la-pyme). However, it is currently still unclear which authority in Spain will ultimately be responsible for monitoring compliance with NIS2. A NIS2 implementation guide has been published by the National Cryptologic Center (CCN) (https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7235-ccn-stic-892-perfil-de-cumplimiento-especifico-para-organizaciones-en-el-ambito-de-aplicacion-de-la-directiva-nis2-pce-nis2/file.html). It can be assumed that NIS2 will no longer be implemented in Spain in time for October 17, 2024.

Sweden

In Sweden, the NIS2 Directive has not yet been implemented and the legislative process is at an advanced stage.

A Special Investigator was appointed by the Swedish government on February 23, 2023, who is responsible for making the necessary adjustments to Swedish law through NIS2. On March 5, 2024, an interim report entitled “New Rules on Cybersecurity” (SOU 2024:18) was published, detailing the proposed adjustments and the introduction of a new law called the “Cybersecurity Act”. On June 24, 2024, the Swedish Post and Telecommunications Agency (PTS) proposed an e-service to identify operators affected by NIS2. Affected companies must register with the PTS. Overall responsibility lies with the Swedish Civil Contingencies Agency (MSB), with partial responsibilities for various supervisory authorities, which has so far been criticized by industry associations during the legislative process. It can be assumed that Sweden will no longer transpose the NIS2 Directive into national law on time by October 17, 2024. National implementation in Sweden is scheduled for January 1, 2025.

We are committed to helping you succeed and hope this report has provided valuable insights. If you have any questions or would like to discuss how these insights apply to your business, we are here to help.

CONTACT US

9AKK108470A0847

For more information, please visit:

go.abb/nis2