COMPARISON REPORT

NIS2 in a European country comparison:
How are the member states implementing the new EU Cybersecurity Legislation?

The new European Cybersecurity Directive, which makes securing IT systems a cross-industry compliance obligation, had to be implemented by the European member states by October 17, 2024. The countries are taking very different approaches, as the following comparative study shows – and many of them had not yet completed their national implementation by the time this study was completed in January 2025. One of the key findings: 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 it, although there are many similarities.

CYBER|INTELLIGENCE .Institute

Author of the study:
Prof. Dr. Dennis-Kenji Kipker
dennis.kipker@cyberintelligence.institute
www.cyberintelligence.institute

Contents

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden

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 NI2. **It is currently assumed that the national NIS2 implementation in Austria will be completed by mid-2025.**

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 **entered 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. As the national law came into force on October 18, 2024, **registration must be completed by March 18, 2025 at the latest.** Institutions in the digital sector had 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://atwork.safeonweb.be/de/tools-resources/cyberfundamentals-framework).

Bulgaria

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

Following the public consultations, the Bulgarian government submitted an official draft for the national implementation of NIS2 to parliament on September 13, 2024, where it will be submitted to the relevant committees for review. The aim of the law is to revise the existing Cybersecurity Act. As a result of the dissolution of Parliament on September 16, 2024 and the new elections on October 27, 2024, the legislative process has been further delayed. **The content of the draft NIS2 transposition law in Bulgaria is closely based on the provisions of the directive itself.** It can currently be assumed that the draft law will also be incorporated into the final regulation in this form. Nevertheless, the Bulgarian regulation contains some special features: For example, a government decree must be issued within eight months of the national implementation coming into force, specifying the cybersecurity measures to be implemented. In addition, entities that fall within the scope of NIS2 are generally not required to notify the competent authorities for registration, as registration is ex officio. However, exceptions to this are provided for some providers and services. **The obligation to carry out cyber security training for management bodies and employees is set at two-year intervals.** As things stand at present, **it can be assumed that NIS2 will be implemented in Bulgaria by spring 2025.** The Bulgarian cybersecurity strategy is also to be revised as part of NIS2. The Ministry of Electronic Governance is responsible for national implementation.

Croatia

The NIS2 Directive has already been implemented in Croatia.

On February 15, 2024, the EU legal act was transposed into national law with the entry into force of the Cybersecurity Act. The scope of application, responsibilities and requirements are specified in four annexes, including for national strategic planning in cybersecurity involving SMEs not affected by NIS2 and the definition of various official responsibilities as part of the implementation of the Act, for example with regard to the Croatian National Bank or the Croatian Civil Aviation Authority. The National Cyber Security Center, which is part of the Security Intelligence Agency, is a central point of reference for implementation - the consolidation of state activities in cybersecurity and intelligence was heavily criticized during the legislative process with regard to conflicts of interest and the independence of decisions. **Overall, the Croatian implementation is very close to the wording of the NIS2 Directive. What is striking is the comprehensive inclusion of public administration bodies in the scope of application,** measured, among other things, by an assessment of their importance for the smooth implementation of important social or economic activities. Furthermore, the Croatian NIS2 implementation differs in that **the "minimum catalog" of cybersecurity measures from the directive text is included in a comprehensive additional regulatory framework** for the risk-oriented implementation of cybersecurity measures. The statutory implementation period for cybersecurity risk management in accordance with NIS2 is one year for affected institutions in Croatia.

Cyprus

The NIS2 Directive has not yet been implemented in Cyprus, but the legislative process is at an advanced stage.

The NIS2 Directive has not yet been implemented in Cyprus, but the legislative process is at an advanced stage. A corresponding draft law has been published that provides for amendments to the "Law on Security of Networks and Information Systems" from 2020 in order to implement NIS2. This is the law that transposed the original NIS1 directive from 2016 into Cypriot law. The Digital Security Authority (DSA) is responsible for enforcing NIS2 in Cyprus. A public consultation on the implementation of NIS2 took place and was closed on September 29, 2023. **The scope of application in the draft is closely aligned with the text of the directive.** Public institutions at regional level are affected following a risk-based assessment if they provide services with a critical impact. The cybersecurity authority is also to be given the power to define specific individual guidelines for individual aspects of information security as part of the national cybersecurity strategy, for example in the area of supply chain protection or vulnerability management. The risk management requirements under NIS2 will essentially be adopted unchanged for the facilities concerned. Due to the advanced stage of the legislative process, it was originally assumed that the regulations would enter into force on time, but no further information on the timetable is currently available. **It can be assumed that NIS2 will be implemented in Cyprus in the first half of 2025.**

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 January 2025, the bill is currently undergoing further parliamentary deliberation. The prepared bill is now in the phase before the second reading in the Chamber of Deputies. Although the regulator began drafting the bill immediately after the publication of the final text of the NIS2 Directive, the adoption was repeatedly delayed by NUKIB's initiative to include institutions outside the scope of the directive in the bill. 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 cybersecurity 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 during the first quarter of 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 significant delays in the legislative process. In Denmark, the Ministry of Defense is responsible for implementation and presented a basic draft law on July 5, 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, but will be part of upcoming sector specific regulations. The Danish Center for Cybersikkerhed (CFCS) has the task of assisting with the content of the sectoral requirements. The parliament is expected to deal with an updated version of the draft bill in February 2025. **It is currently assumed that the implementation law for NIS2 will come into force in Denmark by the beginning of July 2025 at the latest.**

Estonia

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

Estonia introduced comprehensive legal regulations on cybersecurity back in 2018 with the Cybersecurity Act, which were amended in 2022 and will be adapted again in the future as part of the national implementation of NIS2. However, **the Estonian government is currently significantly behind schedule with the implementation of NIS2 and no publicly accessible draft legislation has yet been presented.** The Ministry of Economic Affairs and Communications (EMEAC) is responsible for drafting the legislation at national level. In Estonia, the Estonian Information System Authority, which falls under the remit of EMEAC, is responsible for the national implementation of NIS2. In preparation for national implementation, EMEAC held a public consultation in June 2023. Public security interests were also included in the consultations, in particular those relating to reporting obligations, the European exchange of information on cyber threats and the increased hybrid threat situation. While security concerns have been expressed by the Estonian side for the former, it is possible that the national NIS2 implementation for the latter aspect addresses physical infrastructure protection more clearly than is the case in other Member States. **There is currently no timetable for when NIS2 will come into force in Estonia, but it is expected to enter into force in summer 2025.**

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. **According to the current political status, it can be assumed that the Finnish implementation law will enter into force in the first or second quarter of 2025.**

France

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

The legislator is working with the French National Agency for Cybersecurity (ANSSI) on implementation. The legislative process in France was interrupted by the dissolution of the National Assembly. Finally, a corresponding government bill on “Resilience of critical infrastructures and strengthening cybersecurity” was submitted to the Senate in October 2024. This will then be submitted to the National Assembly. However, due to political events, deliberations on the bill had to be interrupted. The French cybersecurity authority ANSSI is responsible for monitoring and enforcement. The current draft law is closely based on the NIS2 Directive, but also contains various exceptions and special features. These concern, among other things, risk management in cybersecurity. As stipulated by NIS2, the implementation of appropriate measures is a prerequisite here. In addition, however, a decree of the Council of State can determine which individual objectives are to be implemented by the respective operators of affected facilities. Sector-specific particularities should also be taken into account here. Furthermore, **the scope of application has been extended to other regional authorities, and educational institutions that carry out research activities** should also be affected. **It is not yet clear when NIS2 will be implemented in France. As things stand at present, however, it can still be assumed that implementation will take several months, in particular due to the ongoing political uncertainties in France.** 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 started yet in Germany.

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, followed by parliamentary consultations in 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.** Due to the political termination of the federal government, all legislative projects were halted. **For this reason, the German "NIS2 Implementation and Cyber Security Strengthening Act" (NIS2UmsuCG) is not expected to be passed until fall 2025 at the earliest.**

Greece

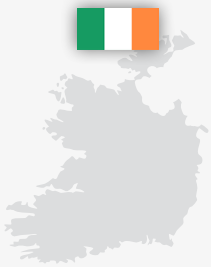
In Greece, the NIS2 Directive was transposed into national law with Law 5160/2024.

The law came into force on November 27, 2024. In addition to the use cases already predefined by the directive itself, NIS2 also applies in Greece to central government bodies and local self-government organizations. The National Cybersecurity Authority (NCSA) is responsible for implementation and identifies the affected institutions in cooperation with the sector-specific authorities. **The NCSA compiles a list of affected entities.** To compile the list, affected companies submit key company data and contact information within a period of two months. The cybersecurity measures required of companies during NIS2 implementation are largely based on the wording of the directive. The same applies to the reporting obligations, which must be fulfilled within 24 and 72 hours. A final report must be prepared one month after the end of the incident. This is also in line with the European requirements.

Hungary

The NIS2 Directive has already been implemented in Hungary with the “Cybersecurity Act”.

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. Cybersecurity incidents in Hungary must be reported to the National Cyber-Security Center. **Further deadlines in Hungary are October 18, 2024, by which the ordered cybersecurity measures had to be implemented, December 31, 2024, by which a contract with a qualified information security auditor had to be concluded, and December 31, 2025, by which the first information security audit had to 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.



Ireland

The NIS2 Directive has not yet been implemented in Ireland, but the legislative process is at an advanced stage.

On August 30, 2024, the Irish government submitted the draft National Cyber Security Bill to Parliament, which forms the basis for the national implementation of NIS2. The National Cyber Security Center (NCSC) is primarily responsible for the implementation of NIS2 in Ireland and also acts as the national CSIRT. In addition to the centrally responsible authority, the draft bill also provides for the responsibility of sector-specific specialist authorities, for example the Central Bank of Ireland is responsible for the banking and financial market sector. In terms of content, the draft bill is closely based on the provisions of NIS2, but deviations are also provided for in various places. For example, although the definitions for “essential” and “important entities” are adopted, it should also be possible for the competent minister to issue regulations to determine an entity as an essential or important entity. **Some of the official powers are also more extensive than NIS2. For example, the possibility of “sensor employment” is provided for the affected institutions in order to collect data relevant to cybersecurity (metadata, IP addresses, transmitted data volume, traffic data).** In addition, the requirements for public bodies are broader in that local government bodies and universities are also covered by the term “public bodies”. Alongside NIS2, Ireland is also planning to develop a new national cybersecurity strategy for 2025. In November 2024, the NCSC also published a NIS2 guide (https://www.ncsc.gov.ie/nis2/FAQ/). **It is currently unclear when the national NIS2 implementation will be adopted in Ireland, but it is expected to be adopted in 2025.**

Italy

The NIS2 Directive has already been implemented in Italy with the adoption of the legislative decree no. 138/2024 which has been published on October 1, 2024.

Further implementing acts are expected. The content of the proposed cybersecurity measures essentially corresponds to the requirements set out in the NIS2 Directive. The National Cybersecurity Agency ACN, which is primarily responsible for implementation, 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. The ACN has presented a digital platform for registration, which is a central element of NIS2 implementation in Italy. **Since October 18, 2024, the ACN has 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 was brought forward to 17 January 2025. The ACN will prepare a list of essential and important entities falling within the scope of NIS2 by March 31, 2025 and will provide feedback to the affected entities between April 1, 2025 and April 15, 2025. The obligations to comply with the directive begin on the date of the ACN's notification to those affected and last 9 months for incident notification obligation and 18 months for obligations relating to administrative bodies and security measures.

Latvia

The NIS2 Directive has already been implemented in Latvia.

The National Cybersecurity Law transposing the Directive was published on July 4, 2024 and entered into force on September 1, 2024. In addition to the national NIS2 transposition law, separate Cabinet of Ministers regulations are adopted in Latvia, which further specify the requirements of the Directive, including the minimum cybersecurity requirements under Art. 21 NIS2, which are not further specified in the national transposition law compared to many other European countries. The Cabinet of Ministers can also decide on security requirements for the operation of data centers, cyber hygiene and requirements for a centralized defence against DDoS attacks. **Particularly striking is a regulation that exists outside of NIS2, which regulates the limitation of internet data traffic to Latvian territory and the decoupling of Latvia from the global data network.** Otherwise, the requirements of NIS2 in Lithuanian law are closely based on the **European requirements. Potentially affected institutions must carry out a self-assessment of their vulnerability and notify the supervisory authority if the result is positive.** The National Cybersecurity Centre (NCC), which is part of the Ministry of Defense, is primarily responsible for implementation in Latvia. This is not only the central point of contact for infrastructures in the areas of "essential" and "important", but also the supervisory authority for compliance with the requirements. The Constitution Protection Bureau, on the other hand, is responsible for monitoring the critical infrastructure of information and communication technology. State and local government institutions are covered by the legal requirements. **With regard to the implementation of information security, regular audits and training sessions are prescribed.**

Lithuania

The NIS2 Directive has already been implemented in Lithuania.

The implementation of NIS2 in Lithuania is based on the Amending Law to the Cyber Security Law of the Republic of Lithuania, which entered into force on October 18, 2024. Supplementary requirements, in particular regarding technical and organizational cybersecurity measures and reporting obligations as well as the competent authorities, are contained in an accompanying resolution adopted on 11 November 2024. Cybersecurity policy in Lithuania is coordinated by the Ministry of National Defense. The National Cyber Security Center, the Lithuanian Police and the State Data Protection Inspectorate are responsible for operational cyber security in Lithuania. The National Cyber Security Center is assigned to the Ministry of Defense. **Overall, the Lithuanian implementation is very closely based on the requirements of the directive.** The legal requirements for affected companies therefore largely correspond to the requirements of the NIS2 Directive. A secure national data transmission network is provided for state institutions and municipal institutions and bodies. The more specific requirements from the Lithuanian NIS2 resolution include detailed specifications on the cyber incident management plan, incident management, the impact assessment for cyber incidents, the identification of affected companies and the description of cybersecurity requirements, including securing the supply chain. Institutions that fall within the scope of NIS2 do not have to register with the authorities. The National Cyber Security Center will determine which entities fall within the scope of NIS2 and contact the affected entities so that they are included in a special list of NIS2 entities by April 17, 2025. **The entities falling within the scope have a transition period of 12-24 months to implement the cybersecurity measures under NIS2 in practice.**

Luxembourg

The NIS2 Directive has not yet been implemented in Luxembourg, but the legislative process is at an advanced stage.

The NIS2 Directive has not yet been implemented in Luxembourg, but the legislative process is at an advanced stage. On March 13, 2024, a draft bill was submitted to the Chamber of Deputies and an opinion was issued. The Luxembourg Council of State published a further opinion on October 8, 2024. In Luxembourg, various authorities are responsible for the national implementation of NIS2: The “Institut Luxembourgeois de Régulation”, the “Commission de Surveillance du Secteur Financier” and the “Haut-Commissariat à la protection nationale” as far as crisis management and international cooperation are concerned. **The implementation of NIS2 in Luxembourg is very closely based on European law.** This concerns both the scope of application and the requirements for technical and organizational measures to be implemented by the institutions concerned. **No further public information is currently available on the date of national NIS2 adoption in Luxembourg, but it can be assumed that this will be completed in the first half of 2025 due to the advanced stage of the legislative process.**

Malta

The NIS2 Directive has not yet been implemented in Malta, but the legislative process is at an advanced stage.

On September 6, 2024, the Maltese Ministry for Home Affairs, Security and Employment published a first draft for public consultation. The consultation period ended on October 7, 2024. In Malta, NIS2 is being implemented with the "Measures For A High Common Level Of Cybersecurity Across The European Union (Malta) Order". **The content of the draft law is closely aligned with the wording of the NIS2 Directive.** Facilities at regional level are covered by NIS2 if their failure could have a significant impact on critical or social activities. The cybersecurity measures to be implemented in the Maltese regulatory proposal stipulate the **appointment of a security officer who has the necessary expertise, oversees the implementation of the cybersecurity measures and acts as a point of contact** between the competent authority and the CSIRTs. The reporting obligations for cybersecurity incidents are to be addressed to the CSIRTMalta. **In Malta, the national NIS2 implementation is expected to be adopted in the first quarter of 2025.**

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. **The Dutch government currently assumes that the draft for a national implementation law will be submitted to parliament in the first quarter of 2025 and will enter into force in the 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 first 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 public hearing on the first draft bill was concluded on May 24, 2024. Due to its high level of regulation, it was subject to extensive criticism in the public process. Accordingly, a second and revised draft was published by the responsible ministry on October 7, 2024 and introduced into the further legislative process. **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"** – this applies to both the first and the second draft bill. For example, according to the first draft, 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. **According to the current status of the parliamentary procedure, national NIS2 implementation in Poland can be expected in the first or second quarter of 2025.**

Portugal

The NIS2 Directive has not yet been implemented in Portugal.

On November 22, 2024, the draft law for national implementation was included in the public consultation. The consultation process was subsequently extended and ended on December 31, 2024. In Portugal, the National Cybersecurity Center (CNCS) is responsible for the implementation of NIS2 alongside sectoral authorities. In addition, a comprehensive scope of application is defined for public administration bodies. **The institutions concerned are obliged to carry out a self-identification process and complete it within 60 days of the electronic platform to be used for this purpose being made available. There is also an obligation to keep the information entered up to date.** At a political level, the implementation of NIS2 in Portugal is accompanied by the "National Cyberspace Security Strategy" (ENSC). **A "National Cybersecurity Reference Framework" (QNRCS) is intended to ensure the identification of existing norms, standards and best practices in cybersecurity.** What is particularly striking in Portugal is the high complexity of the cybersecurity landscape with general and sectoral authorities, emergency bodies, advisory bodies and commissions. Accordingly, the national implementation law contains numerous provisions that concretize this regulatory structure. Institutions affected by NIS2 are obliged to implement risk management. In this respect, numerous requirements from NIS2 are adopted. It is also envisaged that the CNCS may issue technical harmonization instructions. The sectoral cybersecurity authorities will also be authorized to issue sector-specific cybersecurity measures. **There is currently no timetable for when the national implementation of NIS2 will be completed in Portugal.**

Romania

The NIS2 Directive has already been implemented in Romania.

On January 1, 2025, the National Directorate for Cybersecurity (DNSC) announced the adoption of the national transposition of NIS2 under Emergency Ordinance no. 155/2024 and is also the central authority responsible for national transposition, alongside various sector-specific authorities. At the directorate level, the transposition of the NIS2 Directive into national law was the responsibility of the Romanian General Directorate for Regulation and Control (DGRC), which organized a broad consultation process throughout 2024 involving the relevant stakeholders and experts from the public and private sectors in Romania. **Essentially, the NIS2 implementation in Romania is based on the European Directive.** Local public administration bodies such as municipalities and cities are comprehensively included in the scope of application. The companies affected by NIS2 are identified by the DNSC. The technical and organizational measures to be implemented essentially correspond to the requirements of NIS2. **Deviations in the Romanian implementation can be seen in the deadlines that essential and important institutions must meet. The regulations on the information to be provided by the affected entities are also more extensive.** Romanian law is stricter than other European transpositions with regard to fines for violations. For example, **the authorities have the option of imposing double the amount of fines in certain cases.**

Slovakia

The NIS2 Directive has already been implemented in Slovakia.

The national implementation **law came into force on January 1, 2025,** after it was signed and published by the President. The law amends the existing Cybersecurity Act. The National Security Authority and the specialist ministries are responsible for national implementation. In addition, a national CSIRT, the “Center SK-CERT”, has been established in Slovakia. The scope of application of the regulations was essentially taken from NIS2 and transferred to Slovakian law in sector tables in the annex to the act. In addition, a further annex contains specific official responsibilities for the individual sectors. The Slovakian legislator has made use of the option to also apply the requirements from NIS2 to local administrative units. The technical and organizational measures to be implemented largely correspond to the text of the directive, as do the options for controls and sanctions provided for in Slovakian law. **However, the list of minimum measures provided for in the NIS2 Directive is not identical; for example, additional requirements for physical and environmental security are specified.** The NIS2 Implementation Act is accompanied by the national cybersecurity strategy, which comprehensively defines the Slovak Republic’s strategic approach to ensuring a high level of cybersecurity.

Slovenia

The NIS2 Directive has not yet been implemented in Slovenia, but the legislative process is at an advanced stage.

In February 2024, the legislative proposal for a new Slovenian Information Security Act was published, which amends the existing law transposing the NIS1 Directive from 2016 into national law. Numerous proposals were submitted for the draft law, so the Slovenian government is currently preparing a revised proposal for the Slovenian Information Security Act. An updated draft bill has not yet been published, but it can be assumed that further changes will be made in an updated draft. The "Office of the Government of the Republic of Slovenia for Information Security" (URSIV) is responsible for implementation in Slovenia. The original draft contains various differences to the European directive in that it directly reflects the affected sectors and industries in the legal text. The operator obligations are also regulated in different articles, depending on the relevance of the institution and the sector to which it belongs. The draft contains detailed regulations on the approval and use of cryptographic products. **The provisions on fines also deviated significantly from the NIS2 Directive.** Comprehensive changes can therefore be expected in a revised draft version. **It is currently assumed that the NIS2 implementation in Slovenia will be adopted in the first quarter of 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.** Corresponding inquiries in September 2024 were answered similarly. 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). **Due to the difficult political situation in Spain, it is currently not possible to predict when NIS2 will be implemented. It is therefore intended to implement NIS2 temporarily by means of a royal decree-law. However, this is only permissible in exceptional cases due to constitutional reasons.**

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. An additional detailed government report including the implementation of the European CER Directive was published by the Swedish government on September 18, 2024 (SOU 2024:64, https://www.regeringen.se/contentassets/4df0dff-c35e4488d8366ef25da09527a/motstandsk-raft-i-samhallsviktiga-tjanster-sou-202464.pdf). In terms of content, the Swedish implementation of NIS2 intends to be closely aligned with the requirements of the European directive. **The NIS2 Implementation Act is not expected to come into force in Sweden until summer 2025 at the earliest.**

We're 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're here to help.

CONTACT US

—

For more information, please visit:

go.abb.com/nis2

9AKK108470A0847