

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
<b>Austria</b>	<b>Ongoing</b>	Ongoing legislative Process	<ul style="list-style-type: none"> <li>– Closely modelled on the NIS2-Directive. There may be some deviations as regards sector definitions.</li> <li>– Risk management measures are likely to be defined in secondary legislation (regulation issued by the Minister of the Interior).</li> <li>– Similar to Germany, Sect 25 para 4 of the existing draft excludes the attribution of corporate figures of affiliated and partner companies for the purposes of the Size-Cap-Rule, if an entity does not use a network and information system of affiliated or partner companies for the provision of services.</li> </ul>	Not before June 2025 (i.e. the date specified in the existing draft)	CERHA HEMPEL <a href="mailto:hans.kristoferitsch@cerhahempel.com">hans.kristoferitsch@cerhahempel.com</a>	10-Oct-2024
<b>Belgium</b>	<b>Enacted</b>	The NIS2 Directive has been transposed into Belgian law by the Act of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security.	<ul style="list-style-type: none"> <li>– Closely modelled on the NIS2-Directive.</li> <li>– The list of sectors and/or subsectors falling within the scope of the NIS2 Act may be extended by Royal Decree, and other elements may be further specified by Royal Decree.</li> </ul>	The NIS2 Act has been in force since 18 October 2024.	Liedekerke <a href="mailto:s.vandenbrande@liedekerke.com">s.vandenbrande@liedekerke.com</a>	30-Oct-2024
<b>Bulgaria</b>	<b>Ongoing</b>	Following public consultations, the Bulgarian government submitted the official draft of the NIS2 Implementation Act on 13 September 2024 to the national	<ul style="list-style-type: none"> <li>– The draft Implementation Act closely mirrors the provisions of the NIS2 Directive, and we anticipate that it will be enacted in its current form, with no significant revisions.</li> </ul>	It is difficult to predict whether the newly elected Parliament, once constituted in November, will prioritize	Penkov, Markov & Partners <a href="mailto:niko-lay.cvetanov@penkov-markov.eu">niko-lay.cvetanov@penkov-markov.eu</a>	16-Oct-2024

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
		<p>Parliament. The draft bill is intended to amend and supplement the existing Cybersecurity Act.</p> <p>As part of the legislative process, the draft has been presented with the relevant committees of the Bulgarian Parliament for review. However, it has yet to be examined, debated in plenary and voted on due to the recent dissolution of the Parliament on 16 September 2024, ahead of the upcoming parliamentary elections scheduled for 27 October 2024.</p>	<ul style="list-style-type: none"> <li>- Within 8 months after the entry into force of the NIS2 Implementation Act, the Bulgarian government must adopt secondary legislation (an ordinance to be approved by the Council of Ministers), which shall regulate the various technical, operational and organization measures for network and information security. Currently, no draft of such ordinance is available, but is expected to replace the existing one, maintaining identical scope.</li> <li>- Periodicity of cybersecurity trainings for members of the management bodies and employees of in-scope organizations is set at every 2 years.</li> <li>- In-scope organizations are not required to notify the designated competent authorities under the Cybersecurity Act in order to be entered with the respective registers of essential and important entities, maintained by these regulators. Categorization and registration will be carried out ex officio. An exception applies for TDNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data center service providers, content delivery</li> </ul>	<p>this draft. In any case, we anticipate that it is likely to be passed by the end of the calendar year.</p>		

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
			network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms whose main establishment is located in Bulgaria. These entities will have to notify and provide company details to the relevant authorities for initial registration purposes.			
<b>Croatia</b>	<b>Enacted</b>	NIS2 was implemented through the adoption of the Cybersecurity Act (Official Gazette No. 14/2024)	<p>The Croatian Cybersecurity Act deviates from the NIS2 Directive registering requirement for subjects in its scope – according to its provisions, the competent authorities will notify subjects of their categorization as essential or important entity by February 2025 at the latest. The competent authorities can also request information (if needed for the purposes of categorization) from subjects and that the subjects need to provide the requested information within 15 days of the receipt of the request.</p> <p>Other requirements are closely modeled after the NIS2 Directive, but there are several bylaws that would further specify its requirements that need to be adopted (some are currently in the public consultation phase).</p>	The Act has been in force since 15 February 2024.	Divjak, Topic, Bahtijarevic & Krka Law Firm <a href="mailto:tena.pavelic@dtb.hr">tena.pavelic@dtb.hr</a> and <a href="mailto:anella.bukovic@dtb.hr">anella.bukovic@dtb.hr</a>	18-Oct-2024.

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
			Another deviation is that the Cybersecurity Act introduced a self-assessment requirement for important entities that must be performed at least once every 2 years.			
<b>Cyprus</b>	<b>Ongoing</b>	The draft bill is under review by the Council of Ministers. Upon approval by the Council of Ministers, the bill shall have to pass review by the House of Representatives, prior to its final enactment.	Not yet known, as the draft bill has not yet been made publicly available.	Given the number of steps pending for completion, the enactment of the implementing law is expected by the end of 2024.	Chrysostomides Advocates & Legal Consultants <a href="mailto:a.georgiades@chrysostomides.com.cy">a.georgiades@chrysostomides.com.cy</a>	29-Oct-2024
<b>Czech Republic</b>	<b>Ongoing</b>	The draft of the implementation act, the Czech Cybersecurity Law and its (currently) seven secondary decrees has been discussed in the Czech Parliament.	No significant deviations from NIS2 are contained in the current bill nor are expected.	Expected date of entry into force is between April - July 2025, this might change depending on the debate in the Czech Parliament.	PRK Partners <a href="mailto:zbynek.loebel@prk-partners.com">zbynek.loebel@prk-partners.com</a>	21-Oct-2024
<b>Denmark</b>	<b>Enacted and (partially) ongoing</b>	NIS2 is implemented into Danish law by several sector-specific laws:  1) One main bill for the <b>energy</b> sector (covering CER as well). Status: Public hearing July 2024. Expected to be presented in the Parliament Chamber by February 2025	We expect that the sector-specific regulations for the energy and telco sectors will be higher than those of the minimum requirements of the NIS2 directive.	1 July 2025 (but depending on the process in the Danish Parliament Chamber between Feb-Jun 2025)	Kromann Reumert <a href="mailto:cht@kromann-reumert.com">cht@kromann-reumert.com</a>	25-Oct-2024

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
		<p>and to enter into force on <u>1 July 2025</u>;</p> <p>2) One main bill for the <b>telco</b> sector. Status: Public hearing not held. Expected to be presented in the Parliament Chamber by February 2025 and to enter into force on <u>1 July 2025</u>;</p> <p>3) One main bill for <b>all other</b> sectors (ex finance), which will be broken down into 9 sector-specific executive orders. Status: Public hearing July/August 2024. Expected to be presented in the Parliament Chamber by February 2025 and to enter into force on <u>1 July 2025</u>; and</p> <p>4) Changes to the existing Financial Business Act for certain IT providers (subject to NIS2) to the <b>financial sector</b> (subject to DORA). Status: Entered into force on <u>18 October 2024</u>.</p>				

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
<b>Estonia</b>	<b>On hold</b>	The Estonian legislator has not yet published any drafts of the Act.	N/A	N/A	COBALT <a href="mailto:egon.talur@cobalt.legal">egon.talur@cobalt.legal</a> <a href="mailto:priit.pold@cobalt.legal">priit.pold@cobalt.legal</a>	14-Oct-2024.
<b>Finland</b>	<b>Ongoing</b>	The Finnish Government issued a draft bill to the Finnish Parliament in May (new Act on Cyber Security). As a next step the Finnish Parliament will debate on the Act in parliamentary committees before approving it in (likely amended form), after which it will be authorized by the Finnish President.	Not yet known, but no significant divisions from NIS2 are expected.	Q1-Q2/2025	Roschier <a href="mailto:johanna.lilja@roschier.com">johanna.lilja@roschier.com</a>	24-Oct-2024
<b>France</b>	<b>Ongoing</b>	The French government submitted the draft law transposing the NIS2 Directive to the Senate on 15 October 2024. After the examination of the text by the Senate, the latter shall be examined by the National Assembly. The agenda of the adoption of the draft law has not been published, therefore there is no clear	<ul style="list-style-type: none"> <li>- The current draft law is closely modelled on the NIS2 Directive.</li> <li>- The scope of application has been extended to other local authorities (i.e. all the departments, municipalities of more than 30,000 inhabitants, overseas collectivities). The scope has also been extended to educational institutions carrying out research activities. The prime minister may decide to exclude some educational institutes from the scope.</li> <li>- According to the draft law, a single authority shall be in charge of steering and</li> </ul>	No date announced yet	GIDE LOYRETTE NOUEL A.A.R.P.I <a href="mailto:aurelie.paucud@gide.com">aurelie.paucud@gide.com</a>	28-Oct-2024

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
		view on how long the process will take in France.	<p>coordinating the implementation of the government's cybersecurity policy and monitoring the obligations of the entities. The designated authority is the French Cybersecurity Agency (ANSSI).</p> <ul style="list-style-type: none"> <li>- In deviation of Article 32 of the NIS2 Directive, the current draft law provides that the costs of controls (security audit carried out by independent third parties, security scans, inspections of the local authority, audits carried out in case of incidents) shall be borne by the controlled/audited entity, unless the local authority decides otherwise.</li> <li>- The draft law may be subject to substantial modifications during its examination by the Senate and the Parliament.</li> </ul>			
Germany	Ongoing	<p>The Federal Government presented its official draft of the Act ("NIS2UmsuCG") in July 2024.</p> <p>The national parliament (<i>Bundestag</i>) first debated on the NIS2UmsuCG early October 2024. After adoption by the Bundestag, the NIS2UmsuCG needs to pass the Federal Council</p>	<p>In some respects, the official draft differs from the NIS2 Directive. For example, with regard to the "size cap rule", according to which only companies that meet certain employee, turnover and balance sheet thresholds fall within the scope of application, the German legislator intends to take into account only those employees, turnover and balance sheet amounts that are relevant for the specific activities in a NIS2</p>	Early 2025	Noerr <a href="mailto:julian.monschke@noerr.com">julian.monschke@noerr.com</a>	17-Oct-2024.

# LexMundi

## Bringing the best together®

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
		<p>(<i>Bundesrat</i>) before being authorized by the Federal President.</p> <p>In Germany, the relevant ministry expects the legislative process to be completed in early 2025.</p>	<p>sector. Additionally, some sector definitions differ.</p> <p>There will also be additional requirements for critical infrastructure operators (which may include intrusion detection systems, for example). Additional requirements will apply to physical resilience following the implementation of the CER Directive.</p>			
<b>Greece</b>	<b>On hold</b>	Not transposed yet. Public consultation is expected to start in October 2024	N/A	N/A	Zepos & Yannopoulos <a href="mailto:t.konstantakopoulos@zeya.com">t.konstantakopoulos@zeya.com</a>	14-Oct-2024.
<b>Hungary</b>	<b>Enacted</b>	Hungary has implemented the NIS2 Directive into Act XXIII (“ <b>Cybersecurity Act</b> ”) back in 2023. However, the Hungarian Government published a completely new Cybersecurity Act draft proposal on 15 October 2024. The legislator intends to consolidate the Hungarian respective legislation on one act to comply with NIS2 Directive and CER Directives, as well as the ENISA and DORA Regulations. The text of the draft Act is currently under public consultation until the end of October, its text	<p>The currently applicable Cybersecurity Act is closely modelled on the NIS2 Directive. The Cybersecurity Act mainly differs from NIS2 in one key aspect: the Act is not applicable to government and other state entities, nor to financial institutions.</p> <p>Furthermore, the current Cybersecurity Act is vague or silent on the applicability of its provisions on certain entities, like electronic service providers located outside of Hungary or other intermediary service providers. Also, the current Cybersecurity Act does not make it possible to suspend the executive officer of a non-compliant entity.</p>	The main provisions (e.g. regarding registration requirements) are already in force and the remaining will become effective on October 18, 2024.	Lakatos, Köves and Partners <a href="mailto:da-vid.b.nagy@lakatoskoves.hu">da-vid.b.nagy@lakatoskoves.hu</a>	17-Oct-2024.



Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
		may be changed until then. The envisaged entry into force is 1 January 2025. However, it does not change the obligations under the current Cybersecurity Act.	However, it seems that the new draft Act will solve these uncertainties.			
Ireland	Ongoing	The Irish Government published the General Scheme of the National Cyber Security Bill 2024 (“ <b>General Scheme</b> ”) on 30 August 2024. This Scheme will inform the drafting of the National Cyber Security Bill. The National Cyber Security Bill has not yet been published. The provisions contained within the General Scheme are therefore subject to change.	<p>The General Scheme is closely modelled on the NIS2 Directive, albeit with several local idiosyncrasies expected in transposition. Some of the more significant deviations include:</p> <ul style="list-style-type: none"> <li>– Enforcement The General Scheme introduces processes for exercising enforcement powers that are not prescribed in NIS2 Directive. It provides that the enforcement powers of the national competent authority are to be exercised by way of a ‘compliance notice’ that is served on the relevant essential/important entity. Certain Public Bodies (discussed below) and Public Administration Entities appear (although the drafting is unclear) to be exempt from enforcement actions and penalties.</li> <li>– Sensor Employment The General Scheme provides that the NCSC may deploy sensors on essential</li> </ul>	As the Cybersecurity Bill has yet to be published and go through the legislative process, the date on which final transposing legislation can be expected is not clear.	Arthur Cox <a href="mailto:colin.rooney@arthurcox.com">colin.rooney@arthurcox.com</a> <a href="mailto:vivian.spies@arthurcox.com">vivian.spies@arthurcox.com</a>	30-Oct-2024

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
			<p>and important entities, with their consent, where necessary to detect and manage risks to network and information security.</p> <ul style="list-style-type: none"> <li>- Public Body The General Scheme introduces the concept of “public bodies“ which is distinct from the concept of a “public administration entity“.</li> <li>- System of self-registration Head 31 of the General Scheme lists specific types of entities (TLD name registries, DNS service providers, domain name registration service providers, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, online marketplaces, online search engines and social networking platforms) that must self-register with the NCSC by submitting certain information to the NCSC by January 17, 2025. The General Scheme also provides that the NCSC must establish a list of essential and important entities by April 17, 2025 and that, in order to do this, the Minister shall require essential and important entities to submit certain</li> </ul>			

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
			details to the relevant competent authorities.			
<b>Italy</b>	<b>Enacted</b>	Italy has implemented the NIS2 Decree through adoption of Legislative Decree No. 138/2024 (the "Decree"), which was published in the Italian Official Gazette on 1 October 2024.	<ul style="list-style-type: none"> <li>- Closely modelled on the NIS2 Directive.</li> <li>- broader scope of application, including the following: (i) public administrations identified on the basis of a criterion of gradualness, the evolution of the degree of exposure to risk of the PA, the probability of incidents occurring and their severity; and, irrespective of size(i) entities providing local public transport services, (ii) educational institutions carrying out research activities, (iii) entities carrying out activities of cultural interest, (iv) in-house companies, investee companies and publicly controlled companies.</li> <li>- Although the NIS2 Directive will be applicable as of 17 October 2024, timeline for compliance obligations applicable to companies falling within its scope is broadly extended with the adoption of the Decree (e.g., companies are required to assess applicability of the Decree by end of the year; only from January 2025 those that deem to be included in its scope will be obliged to register on the platform created by the</li> </ul>	On 16 October 2024, the NIS2 Directive will become applicable within the Italian jurisdiction by means of the Decree.	Chiomenti <a href="mailto:marilena.hyeraci@chiomenti.net">marilena.hyeraci@chiomenti.net</a>	10-Oct-2024.

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
			<p>competent Italian Authority; 9 months from notification of qualification as an essential or important subject (approximately around January 2026), companies will be obliged to implement reporting requirements, etc.).</p> <ul style="list-style-type: none"> <li>- With respect to governance issues, the NIS2 Directive refers to “management bodies” while the Decree refers to “governing and management bodies“, also including companies’ bodies having more operational roles and responsibilities. This has some implications, as while Italian companies may need to adopt a more structured approach (involving several levels of company bodies), the NIS2 Directive would entrust only management bodies (<i>i.e.</i>, a relatively lean group of decision-makers) who would be able to intervene quickly in the event of a crisis.</li> <li>- Failure to comply with the obligations under the Decree may result in significant penalties for operators. In particular, following the reporting of non-compliance by the competent Italian Authority (ACN), administrative sanctions of up to €10,000,000 or 2% of the total annual worldwide turnover for the</li> </ul>			

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
			previous financial year of the entity, whichever is higher, may be issued by the competent authorities. In addition, there is a personal liability of the directors and sanctions against them for non-compliance.			
<b>Latvia</b>	<b>Enacted</b>	<p>NIS2 Directive is implemented in national legislation with the adoption of the National Cybersecurity Law (<i>Nacionālais kibersdrošības likums</i>).</p> <p>In addition to the National Cybersecurity Law, separate Cabinet of Minister regulations shall be adopted, which will further implement the requirements of NIS2 Directive. Most importantly, Cabinet of Ministers Rules on Minimum Cybersecurity Requirements which implements Art. 21 of the NIS2 shall be adopted (not yet adopted).</p>	System of registration	<p>The National Cybersecurity Law came into force on 1 September 2024.</p> <p>Cabinet of Ministers Rules on Minimum Cybersecurity Requirements are expected to be adopted October – November 2024.</p>	<p>Ellex Klavins</p> <p><a href="mailto:sarmis.spilbergs@ellex.legal">sarmis.spilbergs@ellex.legal</a></p> <p><a href="mailto:mikijs.zimecs@ellex.legal">mikijs.zimecs@ellex.legal</a></p>	21-Oct-2024
<b>Lithuania</b>	<b>Ongoing</b>	The general requirements of NIS2 have been transposed into the amended Republic of Lithuania Law on Cyber Security (hereinafter – the “ <b>LCS</b> ”) (lit. <i>Lietuvos</i>	Head 31 of the General Scheme lists specific types of entities that must self-register with the NCSC by submitting certain information to the NCSC by January 17, 2025. The General Scheme also provides that	The LCS has been in force since October 18, 2024 whereas further implementing acts, detailing reporting	<p>Ellex Valiūnas</p> <p><a href="mailto:Migle.Petkeviciene@ellex.legal">Migle.Petkeviciene@ellex.legal</a></p> <p>and</p>	25-Oct-2024

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
		<i>Respublikos kibernetinio saugumo įstatymas</i> ), which was adopted on July 11, 2024, and came into force on 18 October 2024. Additional regulations, further elaborating on technical and organizational measures, reporting, designation of cyber security entities and more, are still under negotiations and are expected to be adopted soon.	the NCSC must establish a list of essential and important entities and that, in order to do this, the Minister shall require essential and important entities to submit certain details to the relevant competent authorities. Therefore, other essential and important entities outside the scope of Head 31 will also need to provide similar details when requested but are not under an obligation to proactively provide this information.	mechanisms, technical and organizational measures, enforcement measures and more, are expected to be adopted soon.	<a href="mailto:Ignas.Sidasas@ellex.legal">Ignas.Sidasas@ellex.legal</a>	
<b>Luxembourg</b>	<b>Ongoing</b>	On 13 March 2024, the Luxembourg government filed a draft law n°8364 which is currently under discussion. The draft law will amend four national laws: (i) the amended law of 14 August 2000 on e-commerce, (ii) the amended law of 23 July 2016 creating a high commission for national protection, (iii) the law of 28 May 2019 transposing NIS 1 and (iv) the law of 17 December 2021 transposing the European Electronic Communications Code. It is currently unknown when the draft law will be adopted by the Luxembourg Parliament.	No significant deviations from NIS2 are contained in the current bill nor are expected. The <i>Institut Luxembourgeois de Régulation</i> and the <i>Commission de surveillance du secteur financier</i> are designated as competent authorities. The <i>Haut-Commissariat à la Protection nationale</i> will be in charge of international and intersectoral cooperation and will be the cyber crisis management authority.	N/A	Arendt & Medernach <a href="mailto:Astrid.Wagner@arendt.com">Astrid.Wagner@arendt.com</a>	29-Oct-2024

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
Malta	Ongoing	<p>On the 6 September 2024, the Ministry for Home Affairs, Security and Employment published a draft Legal Notice for public consultation.</p> <p>The consultation closed on 7 October 2024, and the Legal Notice transposing the Directive was supposed to be published by the 17 October 2024, and come into force on the 18 October 2024. However, the Legal Notice has not been published, to date.</p>	<p>The draft legal notice entitled “Measures for a High Common Law of Cybersecurity Across the European Union (Malta) Order, 2024“, mirrors closely the NIS2 Directive.</p> <p>Article 2(5)(b) of the Directive has not been implemented and therefore education institutions fall outside the scope of the Order. Article 2(5)(a), on the other hand, has been implemented and the Order applies to public administration entities at local level.</p>	This should have entered into force on the 18 October 2024 as per the communication in the Public Consultation, but the Legal Notice has not been published yet.	Ganado Advocates <a href="mailto:pmgrimaud@ganado.com">pmgrimaud@ganado.com</a>	24-Oct-2024
Netherlands	Ongoing	<p>On 21 May 2024, the Dutch government published a consultation document for the implementation legislation of the NIS2 Directive, the Dutch Cybersecurity Act (<i>Cyberbeveiligingswet</i>), which consultation period ended on 1 July 2024.</p> <p>It is currently unknown when the Dutch Cybersecurity Act will be submitted as a bill before the Dutch Parliament.</p>	<ul style="list-style-type: none"> <li>– Closely modelled based on the NIS2 Directive.</li> <li>– Scope has been extended to local governments (e.g. the provinces, municipalities and water boards) which have been assigned the status of essential entities. Educational institutions can be assigned the status of essential or important entity in individual cases based on a ministerial decree.</li> <li>– Essential and important entities must report significant incidents to both the CSIRT and the competent authority (the relevant Ministry in that sector).</li> </ul>	N/A	HOUTHOFF <a href="mailto:t.de.werd@houthoff.com">t.de.werd@houthoff.com</a> and <a href="mailto:m.moeskops@houthoff.com">m.moeskops@houthoff.com</a>	15-Oct-2024

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
			<ul style="list-style-type: none"> <li>– Entities which are not important or essential can report incidents on a voluntary basis to a CSIRT.</li> </ul>			
<b>Poland</b>	<b>Ongoing</b>	<p>A draft legal act has been prepared by the relevant Ministry for Digital Affairs and published on 23 April 2024.</p> <p>Public consultations of the initial draft bill have been held for a one-month period and formally concluded on 24 May 2024. The initial draft implementing act has been subject to significant criticism, particularly the extent to which it proposes solutions going beyond the minimum requirements set by the NIS2 directive.</p> <p>In response to this criticism, the Ministry for Digital Affairs has published a revised version of the draft act on 7 October 2024. According to the Ministry for Digital Affairs, the revised draft will be shortly submitted for deliberation by the Polish Parliament, formally beginning the actual legislative process.</p>	<ul style="list-style-type: none"> <li>– The draft act, including the revised version, is generally considered more rigorous and wider in scope than the directive. In particular, it includes a wider list of sectors considered as essential, e.g. wastewater supply, managed IT and cybersec services, as well as manufacturing of medical devices.</li> <li>– The draft act goes somewhat beyond the directive with respect to personal responsibility of management. It specifies, for example, that in case of multi-member management, if a single member has not been appointed as responsible for cybersec, all members will bear joint and several responsibility.</li> <li>– The draft act also foresees an additional type of fine in case a regulated entity causes a direct and serious cybersecurity threat to Polish defense, state security, public safety and order, human life and health. In such cases the maximum threshold for the fine is higher, i.e., up to PLN 100.000.000 (approx. EUR 23.000.000).</li> </ul>	Q1-Q2/2025	Wardynski & Partners <a href="mailto:jakub.baranski@wardynski.com.pl">jakub.baranski@wardynski.com.pl</a>	31-Oct-2024



Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
			<ul style="list-style-type: none"> <li>The draft act will also transpose the EU Commission's Toolbox for 5G Security to Polish law.</li> </ul>			
<b>Portugal</b>	<b>On hold</b>	On 24 October 2024, the Portuguese government approved for public consultation two projects on cybersecurity legislation - one of which is a draft for the implementation of the NIS2 directive (the other being a new cybersecurity legal regime for Portugal). Public consultation of the drafts is expected to start in November 2024. It is currently unknown when the projects will be submitted as bills before the Portuguese Parliament (information indicates the Government's intention would be to do so once the current work, in Parliament, for the approval of the 2025 State Budget is completed).	Not yet known, as the draft bill for the implementation of the NIS2 directive has not yet been made publicly available.	N/A	Morais Leitão, Galvão Teles, Soares Da Silva & Associados <a href="mailto:htb@mlgts.pt">htb@mlgts.pt</a>	24-Oct-2024
<b>Romania</b>	<b>Ongoing</b>	On 15 August 2024, the Romanian Cybersecurity Authority ("DNSC") has issued for public consultation a draft for the implementation of the NIS2 directive.	<ul style="list-style-type: none"> <li>In principle closely modelled based on the NIS2 Directive.</li> <li>The Romanian transposition particularly deviates with respect to the deadlines which must be observed by the essential and the important entities (e.g.,</li> </ul>	October-November 2024	NNDKP <a href="mailto:iurie.co-jocaru@nndkp.ro">iurie.co-jocaru@nndkp.ro</a>	17-Oct-2024

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
		<p>After such public consultation, DNSC published on 15 October 2024 an updated draft.</p> <p>As the update draft is prepared in the form of a Government Emergency Ordinance (“<b>GEO</b>”), it is expected that the draft will be sent to the Government for approval in an urgency procedure which does not require a parliamentary debate.</p> <p>It is expected that the draft GEO will enter the agenda of the Government in October or November 2024.</p> <p>The Parliament of Romania will have to confirm or reject the GEO after its adoption by the Government, but until such parliamentary confirmation/rejection, the GEO adopted by the Government remains in force.</p>	<p>the deadlines in which any amendments must be notified to DNSC are longer than that provided by the NIS2 directive).</p> <ul style="list-style-type: none"> <li>– Moreover, as another example where the draft deviates from NIS2 directive, the amount of information that the essential and important entities must notify to DNSC is more significant than provided under the NIS2 directive.</li> <li>– A particularly important provision is the possibility granted in certain cases to the competent authority to impose the double of the amount of fines set forth under the transposition (including to double the top fines of EUR 10 million and 2% of the turnover).</li> </ul>			
<b>Slovakia</b>	<b>Ongoing</b>	<p>On 4 October 2024, the Slovak Government submitted an amendment to Act No. 69/2018 Coll. on Cybersecurity, as amended ( “<b>Amendment</b>“), to</p>	<ul style="list-style-type: none"> <li>– There are nearly no material deviations from the text of NIS2 in the current wording of the Amendment. However, pursuant to Article 2(5)(a) NIS2, Slovakia has opted to use the possibility to</li> </ul>	1 January 2025	<p>ČECHOVÁ &amp; PARTNERS</p> <p><a href="mailto:ArnoldXavier.Verhage@cechova.sk">ArnoldXavier.Verhage@cechova.sk</a></p>	16-Oct-2024

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
		<p>the National Council of the Slovak Republic (“<b>Slovak Parliament</b>“) for discussion and adoption. The Amendment, drafted by the National Cybersecurity Authority, serves as the implementing legislation for the NIS2 Directive.</p> <p>The exact date for the discussion in the Slovak Parliament is not yet known, as the schedule for the upcoming parliamentary session has not been published.</p> <p>However, we expect the Amendment to be adopted by the end of November, provided there are no unexpected delays in the legislative process.</p>	<p>apply NIS2 to public administration entities at a local level.</p> <ul style="list-style-type: none"> <li>- Similarly, pursuant to Article 2(8) NIS2, Slovakia has opted to use the possibility to exclude the application of NIS2 to specific entities which carry out activities in the areas of national security, public security, nuclear security, defense or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities.</li> <li>- Additionally, there are slight differences regarding Article 3(4) NIS2. Pursuant to NIS2, entities are required to notify changes in the information (specified therein) submitted to the competent authorities within two (2) weeks of the change. However, in Slovakia the Amendment requires this notification obligation to be fulfilled within 30 days of the change.</li> <li>- In the current iteration of the Amendment, we have not identified any notable differences from NIS2 which are not already mentioned above. However, seeing that the Amendment is still in the legislative process and may, rather</li> </ul>			

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
			likely, be subject to further changes, especially during the upcoming two rounds of readings in the Slovak Parliament before it is finally adopted and enacted, it may eventually differ from the interim legislative material available to us during the time of writing this Slovak chapter.			
<b>Slovenia</b>	<b>Ongoing</b>	<p>In February 2024, a proposal of the new Slovenian Information Security Act that shall implement NIS2 into Slovenian legislation was published.</p> <p>The interested public submitted numerous comments to the respective proposal and the responsible government agency is currently preparing a revised proposal of the new Slovenian Information Security Act.</p> <p>No information is currently available when the revised proposal of the new Slovenian Information Security Act shall be available or when the revised proposal shall be submitted to the Slovenian National Assembly for adoption.</p>	<ul style="list-style-type: none"> <li>– (Outdated) currently available proposal of the new Slovenian Information Security Act modelled on the NIS2.</li> <li>– Currently available proposal of the new Slovenian Information Security Act is expected to be amended (with no revised proposal currently available), so it is currently not know what shall be the deviations of the revised proposal of the Slovenian Information Security Act from the NIS2.</li> <li>– Further amendments of the proposal are also possible during the legislative procedure before the Slovenian National Assembly.</li> </ul>	Not clear, but currently expected in Q1 2025.	ŠELIH & PARTNERJI <a href="mailto:bara.hocevar@selih.si">bar- bara.hocevar@selih.si</a>	28-Oct-2024

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
<b>Spain</b>	<b>Ongoing</b>	The NIS2 Directive has not yet been implemented in Spain. Regarding the current status of the implementation, only public consultations have happened in Spain in 2023 and no draft has been made public. In June 2024, a formal written query was made to the Spanish Government regarding the implementation status. The Spanish Government answered to this request on 18 September 2024 but it merely indicated that they are working on the implementation of NIS2 Directive and did not provide any indications or estimation about the implementation deadlines.	N/A	Unclear	Uría Menéndez <a href="mailto:leticia.lopez-lapuente@uria.com">leticia.lopez-lapuente@uria.com</a> and <a href="mailto:martin.montilla@uria.com">martin.montilla@uria.com</a>	30-Oct-2024
<b>Sweden</b>	<b>Ongoing</b>	On 5 March 2024, a Swedish Governmental Official Report entitled 'New rules on cybersecurity' (SOU 2024:18) was published, which proposed adaptations of Swedish law necessary for the NIS2 Directive and the CER Directive to be implemented in Swedish law. Thereafter, several supplementary Swedish	<ul style="list-style-type: none"> <li>- Closely modelled on the NIS2 Directive.</li> <li>- There is some difference in terminology, e.g. that the Act refers to 'operators' rather than 'entities'. However, it is not clear whether such difference in terminology is intended to have any impact on which organizations the Act will apply to.</li> <li>- The Swedish Act introduces similar supervision and sanctioning possibilities</li> </ul>	Unclear, but expected to be summer 2025	Vinge <a href="mailto:Jonatan.Karlsson@vinge.se">Jonatan.Karlsson@vinge.se</a>	30-Oct-2024

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
		<p>Governmental Official Reports relating to the proposed implementation have been published.</p> <p>The Reports propose a new Act, the Swedish Cyber Security Act, as well a supplementary Regulation (the Swedish Cyber Security Regulation).</p> <p>It is proposed in the Reports that the Act and Regulation enter into force on 1 January 2025. However, the Swedish parliament has not yet passed the proposed Act and so a delay is expected.</p>	<p>as those provided for in the NIS2 Directive. However, it is not clear how some of the more specific requirements of the NIS2 Directive, such as the power of competent authorities to suspend certifications, will be implemented in Swedish law.</p>			
Norway	Ongoing	<p>In Norway, the Government recently (September 2024) issued a consultation document, which serves as the foundation for implementing the NIS1 Directive into Norwegian jurisdiction. The NIS1 Directive will be incorporated into Norwegian law in 2025.</p> <p>As of now, Norway has not implemented the NIS2 Directive through national legislation. The Government is working on</p>	N/A	N/A	Thommessen <a href="mailto:egu@thommessen.no">egu@thommessen.no</a>	10-Oct-2024

# LexMundi

Bringing the best together®

Country	Status	Status of the NIS2 implementation act	If available, foreseeable significant deviations of the national implementation act from the NIS2 Directive	Expected date of entry into force of the implementation act	Lex Mundi Member Firm Contact Point (Email)	Date of last change to the table
		<p>drafting a consultation document to address the necessary regulatory changes for implementing both the NIS2 Directive and the CER Directive into Norwegian law. However, the specific timeline for this process remains uncertain.</p>				