Skadden

Cybersecurity and Data Privacy Update

October 11, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., NW
Washington, DC 20005
202.371.7000

320 S. Canal St.
Chicago, IL 60606
312.407.0700

Navigating the New Cybersecurity Landscape: Key Implications of the EU's NIS 2 Directive

Executive Summary

- The deadline for EU countries to transpose the expanded cybersecurity directive, NIS 2, into national law is 17 October 2024, but the implementation status varies significantly from country to country. Some of the member states will miss the deadline. In others, the new regulation is expected shortly.
- NIS 2 significantly expands the scope of NIS 1 and revises how companies are classified. The directive addresses the security of information and communication technology (ICT) supply chains and supplier relationships, imposes direct obligations on "management bodies" regarding an entity's compliance with NIS 2, and amends the incident reporting requirements.
- Like other EU regimes, NIS 2 applies extraterritorially, to companies located outside the EU if they provide services within the EU.
- Companies — including those based outside the EU — must therefore assess whether NIS 2 applies to them. Supervisory authorities are already calling on companies to take preparatory measures, as certain obligations will apply shortly.

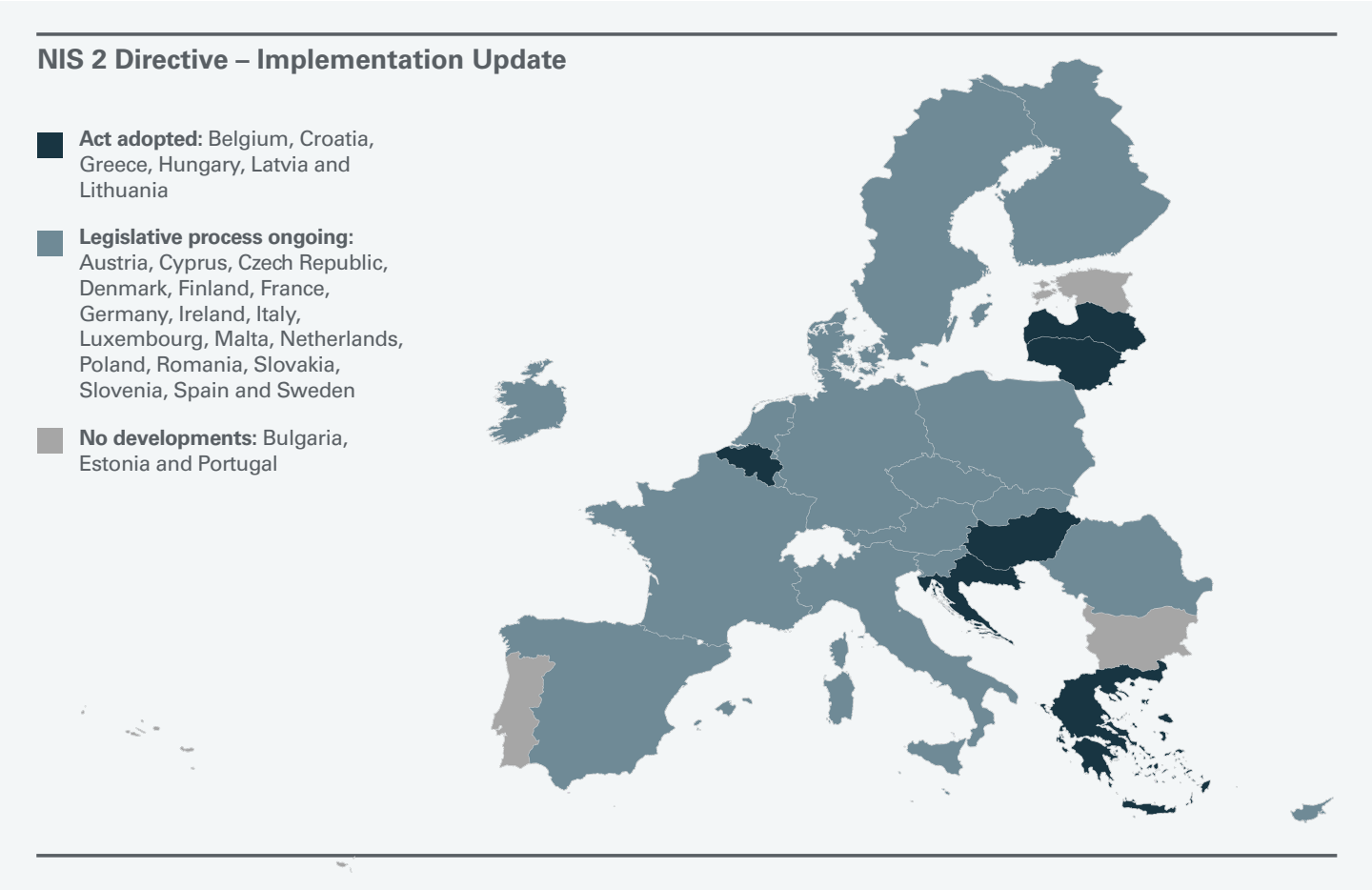
Background and Implementation Status

The EU is increasingly subject to cyberattacks, including by nation state actors. Such attacks affect all economic participants — individuals, companies and public institutions. That is why one of the main priorities on the EU-wide agenda is cybersecurity. On 10 November 2022, the European Parliament voted to adopt the NIS 2 Directive (NIS 2), which forms a key part of the EU's cybersecurity strategy and aligns with the European Commission's priority to prepare Europe for the digital age.

NIS 2 came into force in 2023. Yet, as a directive, it has to be transposed into national law by the member states to apply to companies. The deadline for the implementation into national laws, 17 October 2024, is now approaching.

Progress towards implementation has been uneven, however. While there are currently no developments in some countries, such as Bulgaria, Estonia and Portugal, other member states are already in the legislation process, *e.g.*, Germany, France, and Luxembourg. In six countries, namely Belgium, Croatia, Greece, Hungary, Latvia, and Lithuania, national transposition legislation has already been adopted. Based on the current implementation status, some of the member states will not implement NIS 2 by 17 October.

Navigating the New Cybersecurity Landscape: Key Implications of the EU's NIS 2 Directive



The Commission is also tasked to adopt an implementing act to define the technical and methodological requirements for cybersecurity risk management measures for certain entities in the areas of digital infrastructures, digital providers and ICT service management (business-to-business). Once adopted, that can also serve other regulated entities as guidance for sufficient security risk management measures. The adoption is planned for the third quarter 2024.

Key Changes

The NIS 2 Directive brings many innovations and tightens the current regulations under NIS 2's predecessor, the NIS Directive.

Extended Scope

NIS 2 significantly expands the scope of application compared to the original NIS Directive According to estimates, around 300,000 institutions are now covered by the rules, compared to 20,000 companies previously.

This is the result of a significant expansion of the sectors regulated under NIS 2 due to their degree of digitalization or their importance for the economy and society. Those sectors now include aerospace, public administration, wastewater disposal, postal and courier services, chemicals, food, mechanical engineering, digital services and research.

Furthermore, companies that belong to a regulated sector are now categorized as "essential" or "important" based on the sector and size of the company:

- A company qualifies as essential if (i) it operates in a highly critical sector and (ii) has more than 250 employees or an annual turnover of more than €50 million.
- All other entities in regulated sectors with more than 50 employees or an annual turnover of more than €10 million qualify as important entities.

This classification primarily affects the supervisory and enforcement powers[1] of the supervisory authorities.

- Important companies are subject to ex post supervision, *i.e.*, audits and inspections only take place in the event of reasonable suspicion of violations.
- Essential entities are also subject to ex ante monitoring, *i.e.*, they will have to undergo regular and targeted security audits as well as on-site inspections and off-site supervision including random checks conducted by trained professionals.

Applicability to Entities Outside the EU

Like other EU regimes such as the General Data Protection Regulation (GDPR) and the Digital Services Act, NIS2 has an extraterritorial effect applying the marketplace principle: It applies to essential or important entities that provide their services or carry out their activities within the EU, regardless of whether the entity has an establishment in the EU.[2]

Although not defined in the directive, NIS 2 lists specific factors to be considered in determining whether services are offered within the EU. Those include the use of a language or a currency generally used in one or more member states with the possibility of ordering services in that language, or the mentioning of customers or users who are in the EU in marketing material.[3]

Key Obligations for Entities in Scope

- **Incident reporting:** NIS 2 specifies the information to be reported and timing. Companies must submit an early warning within 24 hours of learning of a significant incident. In addition, they must submit an incident notification within 72 hours, as well as a final report not later than one month after submitting the incident notification.
- **Management responsibility:** The directive imposes obligations on "management bodies" of regulated entities. The responsibilities of the board and senior management at C-suite level include, for example, participation in cybersecurity training, assessment and approval of the cybersecurity risk management measures implemented by the institutions and monitoring the implementation process of these measures. Management bodies shall be accountable and liable for non-compliance with NIS 2.
- **Supply chain management:** Given the significant number of cyberattacks on service providers, NIS 2 obliges organizations to secure their supply chains and reinforces supply chain cybersecurity for key ICT. When evaluating the appropriateness of their ICT supply chain security policies, entities must consider vulnerabilities associated with each service provider and supplier. They are also obligated to assess the overall quality of products and cybersecurity practices employed by third parties. To help mitigating those risks, entities are advised to integrate cybersecurity risk management measures into their agreements with their suppliers and service providers.
- **Registration obligation:** Certain in-scope entities (including providers of cloud computing services, data center services, content delivery networks, managed services, online marketplaces, online search engines and social networking services platforms) must register with and submit specific information to competent supervisory authorities.

Fines

NIS 2 transfers to member states the authority to establish administrative fines for violations of the directive by covered entities. These fines are similar to the GDPR's and may amount up to €10 million or 2% of the total annual worldwide turnover in the previous fiscal year, whichever is higher.

To-Dos for In-Scope Entities

- **Check applicability:** Companies must assess whether they are likely to fall within the scope of NIS 2 and determine if they will be classified as important or essential entities.
- **Registration:** NIS 2 poses registration obligations on in-scope companies. In some countries, such as Hungary and Belgium, registration requirements are already in place or will be shortly. In Hungary, regulated entities have to send certain information to the competent authority within 30 days after commencing their operation. Entities that commenced operations before 1 January 2024 had to send such information to the supervisory authority by 30 June 2024. In Belgium, regulated entities must register with the national cybersecurity authority within five months of the act coming into force, *i.e.*, at the latest by 18 March 2025.
- **Review policies and procedures:** Regulated entities need to evaluate their obligations under NIS 2, particularly regarding cybersecurity risk management and incident reporting. Companies should consider necessary updates to their existing policies and procedures.

[1] Art. 32 and 33 NIS 2.

[2] Art. 2 (1) NIS 2.

[3] Recital 116 NIS 2.

- **Supply chain management:** Given to the risks posed by suppliers and third-party service providers, companies should actively manage and mitigate the risks within their supply chain.
- **Monitor implementation status:** Entities within the scope are advised to stay informed on the implementation progress in the member states. As the transposition deadline approaches, more countries will adopt implementing legislation with varying requirements.
- **Management responsibility:** Regulated entities should ensure that the board and senior management participate in cybersecurity training, assess and approve cybersecurity risk management measures and monitor their implementation.

Contacts

Susanne Werry
Counsel / Frankfurt
49.69.74220.133
susanne.werry@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Kata Éles
Associate / Frankfurt
49.69.74220.143
kata.eles@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Nicola Kerr-Shaw
Counsel / London
44.20.7519.7101
nicola.kerr-shaw@skadden.com