

Cybersecurity and Data Privacy Update

March 27, 2026

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

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

European Commission Announces Potential NIS2 Cybersecurity Reform With Implementation Well Underway

Executive Summary

- **What’s new:** As the EU’s NIS2 Directive is implemented by more member states, the European Commission has published a proposal to reform the law, adding new ransomware reporting obligations, expanding representative appointment requirements and amending the law’s scope.
- **Why it matters:** The proposed amendments introduce additional requirements for regulated entities, including potential ransomware reporting obligations.
- **What to do next:** As NIS2 is adopted into more member states’ laws, the regulatory focus will shift from implementation to enforcement. Companies can continue to move forward with their NIS2 compliance efforts while considering the proposed amendments.

The implementation of the NIS2 Directive is advancing across the European Union, with the European Commission (Commission) proposing further reforms that would introduce additional requirements for regulated entities, such as potential ransomware reporting obligations.

The NIS2 Directive imposes minimum cybersecurity requirements, including registration and incident reporting obligations, on providers of “critical infrastructure” in the EU (e.g., data centers and energy distribution or manufacturing businesses). See our client alerts of August 14, 2025, “[NIS2 Update: EU Cyber Authority Sets Out Compliance Expectations, but Implementation Is a Work in Progress](#),” and October 11, 2024, “[Navigating the New Cybersecurity Landscape: Key Implications of the EU’s NIS 2 Directive](#).”

Proposed Changes to NIS2 Directive

On January 20, 2026, the Commission announced [a proposal to amend certain provisions of NIS2](#). This proposal builds upon the Commission’s November 2025 announcement that it plans to amend other EU digital laws, and its proposal to revise the EU Cybersecurity Act, announced together with the proposed NIS2 changes on January 20, 2026. See our November 21, 2025, client alert “[Commission Proposes Significant Changes to EU Digital Rules – First Impressions](#).”

European Commission Announces Potential NIS2 Cybersecurity Reform With Implementation Well Underway

With this proposal, the Commission aims to amend certain aspects of the NIS2 Directive, including:

Scope. Under the new proposal, operators of submarine data transmission infrastructure will be brought within scope, while entities involved in the distribution of chemicals are removed (though manufacturers and producers of chemicals would still be in scope). The proposal would also tweak the size thresholds for entities to be subject to NIS2’s broader requirements for “essential entities.”

Ransomware reporting. Under NIS2, organizations must report “significant incidents.” The proposal would add a requirement for companies reporting significant incidents linked to ransomware to provide additional ransom-related details (*e.g.*, whether a ransom demand has been requested, whether it was paid and to whom) if requested to.

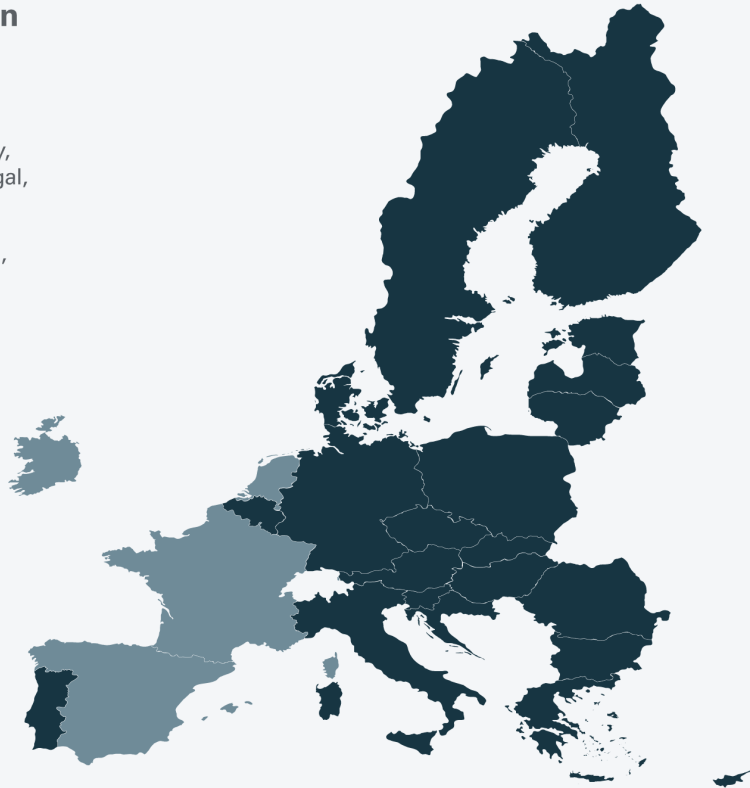
Representatives. Under the current NIS2 Directive, providers of digital services in the EU that do not have an establishment in the EU are required to appoint a representative in one of the EU countries where they provide such services. The proposal would expand this requirement to all companies offering NIS2-regulated services in the EU (*e.g.*, credit institutions and manufacturers of certain products).

NIS2 Implementation Update

The announcements from the Commission comes as the law has been implemented by more European member states in recent months. Twenty-two out of 27 EU countries have now implemented NIS2 into national law and, of the countries that are yet to implement, several have advanced draft legislation that outlines national frameworks.

EU NIS2 Directive – Transposition

- **Act adopted:** Austria, Bulgaria, Belgium, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Malta, Poland, Portugal, Romania, Slovakia, Slovenia and Sweden
- **Legislative process ongoing:** France, Ireland, Luxembourg, Netherlands and Spain



European Commission Announces Potential NIS2 Cybersecurity Reform With Implementation Well Underway

Approaches to key implementation elements vary between countries. For example, reporting obligations under NIS2 vary significantly between countries, creating a fragmented compliance landscape. For example, entities in Germany must immediately inform individuals of an incident if instructed to do so by regulators. This divergence in national rules increases administrative and compliance burdens for organizations operating across multiple EU jurisdictions.

Given this uncertainty, companies may find it best to take a phased approach to compliance, focused on addressing core compliance obligations that are consistent across countries, while leaving flexibility to address jurisdiction-specific quirks once more countries complete their implementations.

What to Do Now

While the implementation process remains at the early stages in many EU countries, 2026 is set to be the year when the first enforcement actions under NIS2 begin, so companies should assess their readiness to comply with NIS2 obligations.

Specific steps companies may want to take:

- Continue to progress NIS2 compliance programs, focusing on systems (*e.g.*, operationally critical systems) and documentation (*e.g.*, incident response plans) that present the greatest enforcement risk.
- Ensure that management bodies (*e.g.*, boards) are updated on NIS2 compliance progress, as those management bodies can be held personally liable for NIS2 noncompliance.
- Consider guidance from EU and national agencies (*e.g.*, the European Union Agency for Cybersecurity/ENISA) that map expectations for NIS2 compliance onto existing international and national standards, such as ISO 27001.
- Continue to track NIS2 implementation status in the jurisdictions in which they operate and identify areas where compliance efforts can be advanced before local implementation is complete.

Contacts

David A. Simon

Partner / Washington, D.C.
202.371.7120
david.simon@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

Susanne Werry

Counsel / Frankfurt
49.69.74220.133
susanne.werry@skadden.com

Aleksander J. Aleksiev

Associate / London
44.20.7519.7212
aleksander.aleksiev@skadden.com

Alex Smallwood

Associate / London
44.20.7519.7202
alex.smallwood@skadden.com

Alberto F. Vogel

Associate / London
44.20.7519.7104
alberto.vogel@skadden.com