

NIS2 Directive: A Gap in the EU's Cybersecurity Policy

Role: European Parliament Policy Analyst

Audience: Members of the European Parliament (MEPs)

Summary

As vital sectors such as energy, transportation, healthcare, and public administration have become increasingly reliant on digital systems, cybersecurity has become a significant part of the European Union's (EU) security strategy. The NIS2 Directive was adopted to establish a high, common level of cybersecurity across the EU. This brief asks: To what extent does the varying implementation of NIS2 by Member States create a gap in the EU's common cybersecurity policy? The findings show that, although NIS2 provides a common legal framework, its implementation has not progressed at the same level across all Member States. The European Commission launched infringement proceedings against 23 Member States in November 2024, issued reasoned opinions to 19 Member States in May 2025, and referred Ireland, Spain, France, and the Netherlands to the Court of Justice in July 2026. The EU should therefore enhance monitoring, provide technical support, and foster cooperation among national authorities to eliminate differences in implementation.

KEY POINTS

- 1. NIS2 creates a common EU framework for a high level of cybersecurity.**
- 2. Differing levels of national implementation pose a significant enforcement challenge.**
- 3. The EU should strengthen oversight, ENISA's support, and cooperation among Member States.**

1. Cybersecurity as an EU Security Issue

Digital technologies are becoming an indispensable component of economic, social, and political life in the EU. Energy, transportation, healthcare, public administration, and communications services increasingly rely on digital networks. Cyber incidents can therefore jeopardize not only individual organizations but also the continuity of vital services. From the EU's perspective, cybersecurity is not merely a technical issue but an integral part of security and resilience policy.

The NIS2 Directive is one of the EU's key tools in this regard (European Parliament & Council of the European Union, 2022). Aiming to achieve a high, common level of

cybersecurity across the Union, it requires Member States to establish national cybersecurity strategies, competent authorities, and incident response structures. It also imposes cybersecurity risk management and reporting requirements on organizations in important and critical sectors, including energy, transportation, healthcare, digital infrastructure, public administration, and manufacturing. This breadth highlights the strong link between cybersecurity and the functioning of European society.

However, a common EU law does not guarantee that it will be applied in the same way in every Member State. This discrepancy between EU-level rules and national implementation is the central issue examined in this brief.

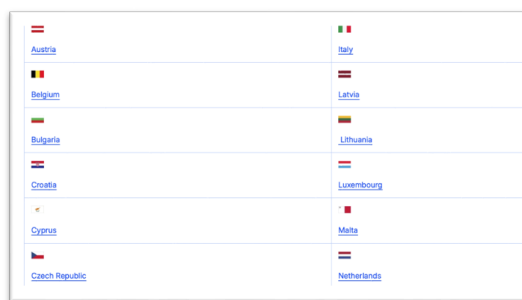
2. The NIS2 Directive and Its Implementation

The NIS2 Directive entered into force in January 2023, and Member States were required to transpose it into national law by 17 October 2024 (European Parliament & Council of the European Union, 2022). It obliges Member States to establish competent authorities and Computer Security Incident Response Teams (CSIRTs), while requiring covered entities to implement cybersecurity risk management measures and report certain incidents.

The European Union Agency for Cybersecurity (ENISA, 2025) supports this process through technical guidance and cooperation with Member States, providing practical information on implementing NIS2 requirements.

Implementation, however, is not progressing uniformly. On 28 November 2024, the European Commission (2024) initiated infringement proceedings against 23 Member States for not fully transposing NIS2 into national law. On 7 May 2025, it issued reasoned opinions to 19 Member States that had not yet reported full transposition (European Commission, 2025). These events show a difference between adopting unified EU rules and ensuring their full and timely implementation nationally.

Figure 1
NIS2 Directive Transposition in EU Member States



Note. Adapted from European Commission (2024).

3. The Implementation Gap and EU Cybersecurity

The main gap lies between NIS2's fundamental objective and the pace and scope of its implementation at the national level. Member States must incorporate the Directive into their legal systems and establish the relevant institutions. Variations in administrative capacity, national legislation, and implementation processes therefore affect when the common rules will fully take effect.

The Commission's enforcement measures provide concrete evidence of this issue. Following the 2024 infringement procedures and the 2025 reasoned opinions, the Commission referred Ireland, Spain, France, and the Netherlands to the Court of Justice of the European Union in July 2026 for failing to notify measures ensuring full transposition (European Commission, 2026). The Commission has emphasized that full implementation is crucial for strengthening resilience and incident response capabilities in critical sectors.

This situation should not be interpreted as a failure of NIS2. Rather, it shows that the effectiveness of an EU policy also depends on how consistently it is implemented nationally. From the perspective of a European Parliament policy analyst, the EU should place greater emphasis on implementation: common legal frameworks matter, but their impact may remain limited if Member States implement them at varying paces.

4. Policy Recommendations

4.1 Strengthen the EU's Monitoring Role

The European Commission should regularly monitor the implementation of NIS2 and report to the European Parliament. Monitoring should cover not only transposition into national law but also the

functioning of national authorities and procedures.

4.2 Strengthen ENISA's Practical Support

ENISA should provide more technical guidance, training, and best practices, particularly for Member States and organizations with limited technical capacity (ENISA, 2025).

4.3 Enhance Cooperation Among National Authorities

The EU should encourage information sharing, joint exercises, and joint enforcement actions among national cybersecurity authorities.

4.4 Prioritize Implementation Before Creating New Rules

The EU must first ensure the full and effective implementation of NIS2. Strengthening the existing framework would be more beneficial than continually introducing new requirements before current implementation gaps are addressed.

Conclusion

NIS2 is a significant initiative aimed at establishing a comprehensive EU cybersecurity framework. However, the implementation process has shown that common laws alone are not sufficient. The EU must support them with stronger monitoring, technical assistance, and cooperation. This will help reduce disparities among Member States and contribute to a more consistent level of cybersecurity across the Union.

References

European Commission. (2024, November 28). *The Commission calls on 23 Member States to fully transpose the NIS2 Directive*. <https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive>

European Commission. (2025, May 7). *Commission calls on 19 Member States to fully transpose the NIS2 Directive*.

https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1499

European Commission. (2026, July 8).

Commission refers Ireland, Spain, France and the Netherlands to the Court of Justice for failing to transpose the rules on cybersecurity.

https://ec.europa.eu/commission/presscorner/detail/bg/ip_26_1499

European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. *Official Journal of the European Union*, L 333, 80–152. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555>

European Union Agency for Cybersecurity.

(2025). *NIS2 technical implementation guidance*. ENISA. <https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance>

Author: Sümeyye Cerit (2023173039), European Parliament Policy Analyst.

This policy brief has been prepared as part of the POLLEN policy brief exercise. Its content reflects the author's analysis and not the official opinion of any EU institution.