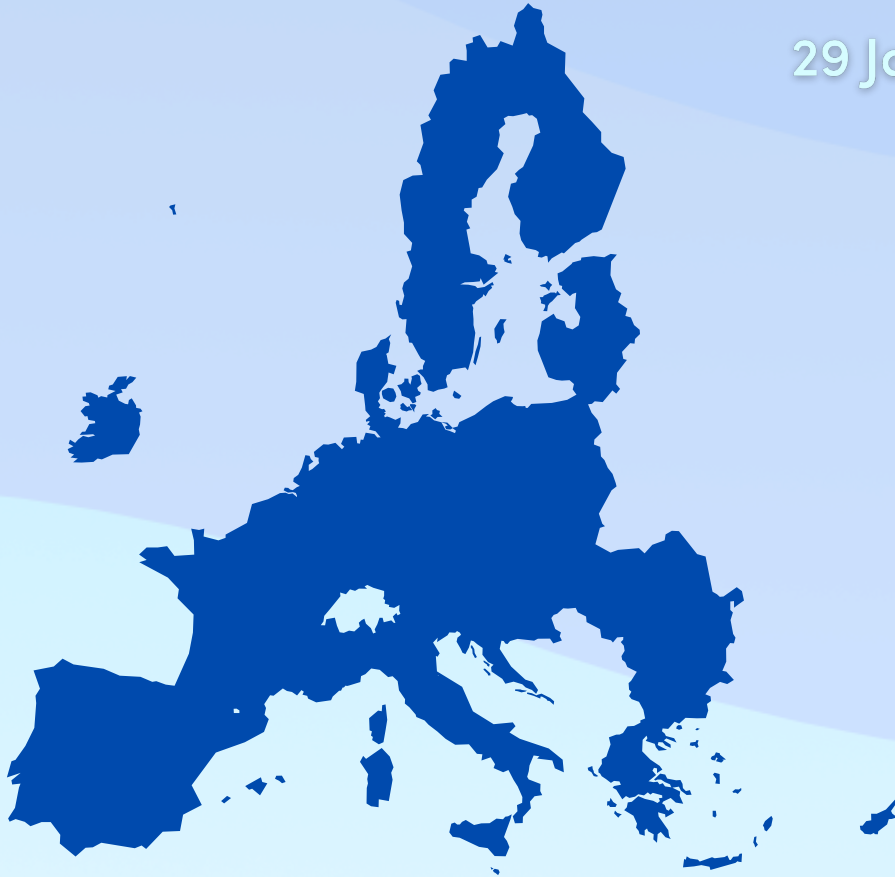


NIS2 TRANSPOSITION OVERVIEW

29 January 2025



Transposed
NIS2 laws:

Draft laws in
legislative
procedures:

Awaiting draft
NIS2 laws:



NIS2: BACKGROUND

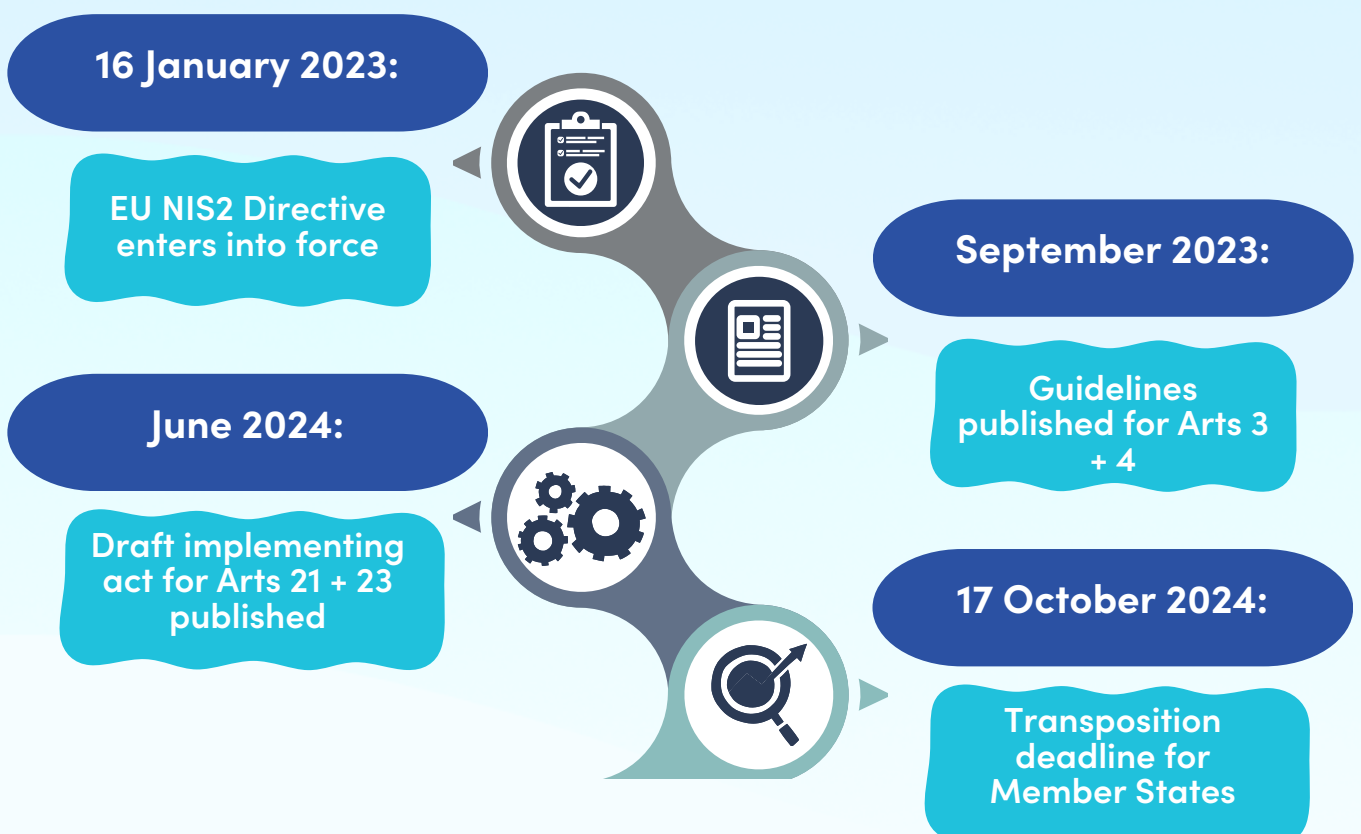
The state of play of the NIS2 Directive

Europe's critical infrastructure faces ever-increasing cyber threats. Examples of serious consequences are the Danish railways coming to a standstill in 2022, or the millions of Ukrainians being cut off from the internet in 2023. To combat these threats, the revised Network and Information Security (NIS2) Directive was adopted in November 2022, and entered into force on 16 January 2023. It aims to increase the common level of cybersecurity of critical infrastructure in the EU and sets out obligations related to Member States' cyber capabilities, risk management and reporting, and cooperation and information exchange for 'essential and important entities'.

The deadline for Member States to transpose the Directive into national law was 17 October 2024. Nevertheless, as of 28 November 2024, the European Commission opened infringement procedures on 23 EU Member States for having failed to transpose the NIS2 Directive. Two months after the deadline, only four Member States had done so.

The ongoing work in the EU Member States and (draft) transposition laws published so far show that there is a real risk of fragmentation across the EU, hampering efficient cybersecurity and competitiveness for the digital industry. Recently, DIGITALEUROPE has published studies on improving the [EU Digital Single Market](#) and on how Europe can lead on [critical technology](#).

This document seeks to provide an overview of the state of NIS2 transposition in the EU Member States, based on details provided by national trade association (NTA) members of DIGITALEUROPE, complemented by desk research. Note that the information found below is non-exhaustive, is based on available information and comprises a snapshot of the current situation that may be subject to change.



NIS2: BACKGROUND

Summary of the state of play

The revised Network and Information Security (NIS2) Directive stipulates that it must be transposed into national law by 17 October 2024, and apply from 18 October 2024. Roughly three months after the official application date, only nine countries have adopted national laws transposing the NIS2 Directive: Belgium, Croatia, Greece, Hungary, Italy, Latvia, Lithuania, Romania and Slovakia.

NIS2 will greatly impact the companies in scope. Especially for those that did not yet prepare for a high level of cybersecurity, the cost of compliance will be high, and significant changes to their cybersecurity management may be needed. This necessitates a sufficient period for the private sector to prepare for compliance with the NIS2 transposition laws, also bearing in mind the potential discrepancies between the requirements that Member States set out, and the different timelines they adhere to.

To give an idea: the expected number of companies impacted by the NIS2 Directive in Romania is 12,000, in Germany 30,000 and in Italy 50,000.

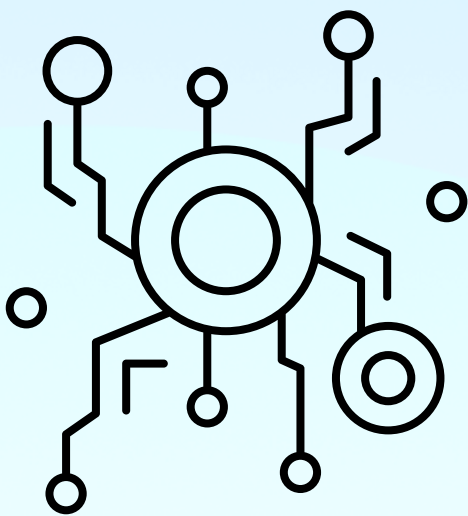


EU national governments work hard to transpose the NIS2 Directive, resulting in a rapidly increasing number of countries adopting their relevant national laws. That notwithstanding, there are still 16 countries where transposition laws are undergoing national legislative procedures and two that have not yet published their draft transposition laws. Amongst those are countries in difficult political situations, such as Germany, France and Ireland where snap elections are taking, or have taken place.

This results in significant fragmentation across the EU27 block, and not only due to greatly diverging timelines. Member States sometimes go beyond the requirements the Directive sets out.

For instance, in Italy, the NIS authority has stated that all Italian branches of international organisations can be subject to Italian rules depending on circumstances, hampering the concept of a 'main establishment'. Belgium established requirements that are more comprehensive than required by the European level, while Poland's draft NIS2 law includes the possibility to exclude 'High Risk Vendors' in particular instances. In Germany, the possibility of self-assessment resulting in a presumption of conformity can be examined for non-consumer products, while government entities are excluded from the scope.

DIGITALEUROPE recently flagged fragmentation issues, hampering European cybersecurity and competitiveness, in a [joint statement co-signed by 20 national trade associations](#).



ADOPTED NIS2 LAWS

Belgium



Timeline: Belgium's NIS2 transposition law has been adopted and published on 17 May 2024.

Key elements of the Belgian transposition law

The scope of the Belgian law does not deviate from the EU Directive, but could be expanded through a Royal Decree. The measures are almost identical to the EU Directive. The Coordinated Vulnerability Disclosure (CVD) policy is mandatory and needs continuous improvement. Presumption of compliance for entities can be derived through third party conformity assessments based on ISO 27001 or the Belgian Cyberfundamentals. The alternative is an inspection by the authorities against these two frameworks. The responsible authority is the Centre for Cybersecurity Belgium (CCB).



Romania

Timeline: The Romanian transposition law was formally adopted towards the end of December 2024.

Key elements of the Romanian transposition law

The law is expected to impact 12,000 companies. The specifics of the self-registration for entities in scope will be specified in secondary legislation, after which the National Cybersecurity Directorate (DNSC) will decide if entities are indeed essential (within 60 days) or important (within 150 days). The evaluation methodology is inspired by the Belgian model and will be specified in secondary legislation. The DNSC is the responsible authority.

ADOPTED NIS2 LAWS

Hungary



Timeline: On January 1, 2025, the new Cybersecurity Act and its corresponding implementing government regulation came into force. Although this completes the transposition of the core NIS2 Directive into Hungarian law, for full applicability and legal certainty a few remaining details are still to be nailed in ministerial and supervisory decrees. Organisations subject to the new legal framework have already registered with the designated cybersecurity supervisor by June 2024, as mandated by a temporary act now repealed by the Cybersecurity Act.

Key elements of the Hungarian transposition law

- **Structural Alignment with NIS2:** The legislation closely follows the framework of the NIS2 Directive but introduces deeper obligations. For instance, a significantly broader segment of public administration is now subject to ex-ante supervision.
- **Data Residency Requirements:** The new regulations mandate in-country residency for a significant part of the data estate of government institutions, government-owned entities and certain other companies, reflecting a stricter approach to data sovereignty.
- **Unified Cybersecurity Framework:** Hungarian legislators used the opportunity provided by NIS2 to overhaul and unify cybersecurity regulations across both public and private sectors.
- **Enhanced Private Sector Requirements:** Private organisations are now required to undergo biannual cybersecurity audits conducted by registered auditors. The security measures align with the robust standards of NIST 800-53.



Lithuania

Timeline: The Lithuanian transposition law was adopted by Parliament in July 2024, and entered into force on 17 October 2024.

Key elements of the Lithuanian transposition law

In April 2025, the relevant authorities have to publish a list of critical and important entities. From that date onwards, these entities have 12 months to comply with the obligations imposed on them.

ADOPTED NIS2 LAWS



Italy

Timeline: The Italian transposition law was adopted and published in the Italian Official Journal in October 2024.

Key elements of the Italian transposition law

The law stays relatively close to the NIS2 Directive. Many aspects are to be defined through implementing acts. The designated NIS authority is the National Cybersecurity Agency (ACN), and expects around 50,000 companies to fall into scope. The deadline for self-registration is 28 February 2025. Incident reporting measures apply from 1 January 2026. Basic and advanced (sector-specific) risk management measures will be adopted in April 2025 and April 2026, respectively. This may constitute an element of fragmentation. The key concerns for the Italian NIS2 transposition law are resource constraints, shortage of cyber professionals, a high risk of paper compliance, and support and guidance to NIS2 entities.

One particular concern is that the ACN's interpretation of Art. 26 of the NIS2 Directive constitutes that all Italian branches of international groups, if they are national legal entities, are subject to the Italian rules, provided they are not only reselling services or products from their headquarters.

Latvia



Timeline: The Latvian transposition law was adopted on 20 June 2024, and entered into force on 1 September 2024.

Key elements of the Latvian transposition law

Further specifications are to be included in so-called Cabinet Regulations, which are still under development. Entities in scope need to register with the authorities by 1 April 2025. By 1 October 2025, they need to appoint a 'cybersecurity manager', and submit their first self-assessment report.

ADOPTED NIS2 LAWS



Slovakia

Timeline: The Slovakian draft transposition law was approved by Parliament on 28 November 2024, and entered into force on 1 January 2025.

Croatia



Timeline: Croatia's NIS2 transposition law has been adopted and entered into force on 15 February 2024.



Greece

Timeline: The Greek draft NIS2 transposition law was published on 19 October 2024 for a two-week public consultation. It was subsequently adopted and has been in force since 27 November 2024.

DRAFT NIS2 LAWS

Germany



Timeline: The German draft NIS2 transposition law was published in May 2024. The Parliament may pass it before the national elections, however, this will likely happen later in 2025, once a new government is in place.

Key elements of the German draft transposition law

The German government may issue technical guidelines with requirements and specifications to carry out self-assessments of conformity for entities manufacturers or providers of products, services or processes that are not consumer products. The biggest concern is various legal uncertainties for businesses - it is difficult to assess how a company is affected by NIS2, particularly for SMEs and it is unclear whether a company's entire ICT infrastructure is covered, or just those that are used directly for relevant services. Moreover, municipalities and federal institutions are exempted from the NIS2 requirements, shifting the burden to the private sector alone, leaving institutions vulnerable. The German government has also published a tool for companies to assess their vulnerability under NIS2 [here](#). The responsible authority is the Federal Agency for Information Security (BSI).



Sweden

Timeline: The Swedish draft NIS2 transposition law has been published in 2024. It is expected to enter into force by the summer of 2025.

Key elements of the Swedish draft transposition law

There seem to be deviations from the EU NIS2 Directive, mainly pertaining to a stricter implementation. There are various concerns, revolving around single businesses being subject to many supervising authorities, a short implementation timeline, the fact that costs are not fully investigated and how liability for Board Members is set out.

DRAFT NIS2 LAWS



The Netherlands

Timeline: The Dutch draft NIS2 transposition law was published on 21 May 2024. Whilst work has been ongoing, the government expects the law to enter into force in Q3 2025.

Key elements of the Dutch draft transposition law

The Dutch transposition law initially seemed to include several discrepancies with the EU Directive and other national transposition laws, but these have been part of ongoing discussions and could be ironed out. In the Netherlands, specific ministries are responsible for specific sectors, which could be slowing things down, whilst introducing concerns about a harmonised application of the transposition law, even within the country.

Poland



Timeline: The Polish draft NIS2 transposition law has been published. It is expected to be voted on by the Parliament in April 2025.

Key elements of the Polish draft transposition law

Poland's draft law transposing NIS2 is the most restrictive in the entire EU and goes far beyond the NIS2 directive. The Polish government justifies this as they are the most vulnerable and most cyber-attacked country in the EU. It proposes to use the 5G Toolbox mechanism to exclude vendors in 18 sectors, including other critical infrastructure sectors using ICT, not just in 5G telecommunications. Polish NTAs have proposed a different approach to regulation in the telecom and energy and other critical sectors. The bill is currently at the inter-ministerial consultation stage.

DRAFT NIS2 LAWS



Finland

Timeline: The Finnish draft transposition law was published on 23 May 2024, and is currently with the Parliament. The law is expected to be passed and come into force in Q2 2025.

Key elements of the Finnish draft transposition law

The Finnish draft law transposes the EU Directive in a fairly straightforward manner. It is fully aligned, apart from minor details in its scope. The measures are levelled with the Directive - there are no additional requirements, nor requirements for standard certifications (e.g., ISO series). The draft law is estimated to directly affect 5,000 entities.

Austria



Timeline: The Austrian draft transposition law was sent to Parliament (Nationalrat) in April 2024, but is being revised after negative feedback. The timeline is unclear.

DRAFT NIS2 LAWS



Denmark

Timeline: The Danish draft transposition for most sectors was published on 5 July 2025. The NIS2 Directive is expected to be fully transposed by February 2025 and enter into force on 1 July 2025.

Key elements of the Danish draft transposition law

The Danish transposition law is divided in various sector-specific laws and one general law for all sectors without sector-specific legislation. All drafts (separate ones for the finance, energy and telecommunication sectors, as well as the general transposition law) have been published.

The biggest concern identified in Denmark is the insufficient guidance for companies to achieve compliance, complicated by the short deadline. Another concern is the lack of harmonisation across sectors and Member States, but also regarding the authorities' supervision of Danish and European companies.

Bulgaria



Timeline: The Bulgarian draft transposition law has been tabled in July 2024, and has been delayed in part due to the political situation in the country. The timeline going forward is unclear.



Portugal

Timeline: Portugal's draft transposition law is expected to be approved by the Parliament by April 2025.

DRAFT NIS2 LAWS

Luxembourg



Timeline: The Luxembourgish draft transposition law, dealt with under 'projet de loi 8364', is currently with the Parliament. On 9 December 2024, a Rapporteur was appointed to lead the file.



Slovenia

Timeline: The Slovenian draft transposition law was published in February 2024, but is yet to be adopted.

Cyprus



Timeline: Amendments have been proposed to national law 89(I)/2020, to reflect the NIS2 transposition. The timeline going forward is unclear.

DRAFT NIS2 LAWS

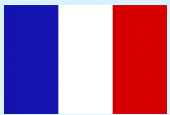
Czech Republic



Timeline: The Czech draft transposition law is still undergoing the legislative procedure.

Key elements of the Czech draft transposition law

There are indications that it may be stricter than the Directive, mostly when it comes to supply chain monitoring requirements and executive action, with a potential ban on suppliers. This ban is publicly announced to be tied to concerns over certain high-risk suppliers, but its impact may go far beyond that. The biggest concern is legal uncertainty.



France

Timeline: The French draft transposition law has been delayed due to the political situation in the country. The Senate is expected to start examining the draft law towards the end of Q1 2025.

Key elements of the French draft transposition law

There are still uncertainties on what the scope will be, but it is expected to generally align with the NIS2 Directive. The number of companies, including SMEs, falling into scope was estimated by the French Cybersecurity Agency (ANSSI) to be 10,000-15,000.

The requirements on self-registration will be specified through decrees, not the legislation itself. Reporting obligations may emerge as an area of concern, as well as information exchange between public authorities.

DRAFT NIS2 LAWS

Ireland



Timeline: The Irish transposition of NIS2 will be included in the 'National Cyber Security Bill', of which the draft was published on 30 August 2024. Its progress has been delayed by snap elections in November 2024. The timeline going forward is unclear.

Preparation of the Irish transposition law

Supervision and enforcement of the NIS2 Directive in Ireland is expected to be divided between the Irish National Cybersecurity Centre (NCSC) and sectoral regulators. The NCSC has, in the meantime, issued a public consultation on risk management measures, broadly pertaining to Arts 20, 21 and 23 of the NIS2 Directive.



Malta

Timeline: The Maltese draft transposition law was published on 6 September 2024 and was open for public consultation until 7 October 2024. It is still undergoing the legislative procedure.

Estonia



Timeline: The Estonian draft transposition law was published on 9 December 2024, and is currently undergoing public consultation, closing on 31 January 2025. For more information, please click [this link](#).

COUNTRIES AWAITING DRAFT NIS2 LAWS



Spain

Timeline: There is no draft transposition law yet in Spain, in part due to discussions of responsibility division within the government. The timeline going forward is unclear.

DIGITALEUROPE'S NETWORK OF NATIONAL TRADE ASSOCIATIONS



About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 113 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE'S NETWORK OF NATIONAL TRADE ASSOCIATIONS

- Aavit (CZ)
- Abelia (NO)
- adigital (ES)
- AFNUM (FR)
- AGEFE (PT)
- Agoria (BE)
- Ametic (ES)
- ANIS (RO)
- Anitec-Assinform (IT)
- APSI (LU)
- ATIC (MO)
- bitkom (DE)
- CITEA (CY)
- HGK (HR)
- Dansk Erhverv (DK)
- DI Digital (DK)
- Digital Turkey Platform (TR)
- ECID (TR)
- FIAR (NL)
- GZS (SI)
- Infobalt (LT)
- IOÖ (AT)
- IT Ukraine (UA)
- ITAS (SK)
- IT-Branchen (DK)
- ITL (EE)
- IVSZ (HU)
- KIGEiT (PL)
- NLdigital (NL)
- Numeum (FR)
- PIIT (PL)
- SECIMAVI (FR)
- SEPE (GR)
- Swico (CH)
- TIF (FI)
- TechSverige (SE)
- techUK (UK)
- Technology Ireland (IE)
- Teknikföretagen (SE)
- Zipsee (PL)
- ZVEI (DE)