NIS Directive

The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

The Directive on security of network and information systems (the NIS Directive) provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,
- cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States,
- a culture of security across sectors that are vital for our economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

Businesses identified by the Member States as operators of essential services in the above sectors will have to take appropriate security measures and notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the new Directive.
A 'NIS Toolkit'

As the cybersecurity threat landscape evolves at a fast pace, it was necessary to implement the NIS Directive quickly. The Commission adopted a Communication to support Member States in their efforts to implement the Directive.

The Communication, dubbed the 'NIS toolkit', provides practical information to Member States on the Directive. For example, it presents best practices on implementing the Directive from other Member States, with explanation and interpretation of specific provisions to clarify how the NIS Directive should work in practice.

Report assessing the consistency of the approaches in the identification of operators of essential services

Operators of essential services are responsible for notifying national authorities of serious cyber incidents. This report provides an overview of how Member States have identified operators of essential services. It assesses whether the methodologies for identifying such operators are consistent across Member States.

Review of the Directive

Article 23 of the Directive requires the European Commission to review the functioning of this Directive periodically. As part of its key policy objective to make Europe fit for the digital age as well as in line with the objectives of the Security Union, the Commission announced in its 2020 work programme that it would conduct the review by the end of 2020.

As part of this process, a consultation opened on 7 July 2020, with as deadline 2 October 2020. The results of this consultation were used for the evaluation and impact assessment of the NIS Directive.

Proposal for a revised NIS Directive (NIS2)

As a result of the review process, the new legislative proposal was presented on 16 December 2020.

The proposal is part of a package of measures to further improve the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole. It covers the field of cybersecurity and critical infrastructure protection. The proposal is in line with the Commission’s priorities to make Europe fit for the digital age and to build an economy ready for a future that works for the people.

The proposal builds on and repeals the current NIS Directive. It modernises the existing legal framework taking account of the increased digitisation of the internal market in recent years and an evolving cybersecurity threat landscape.

The proposal for a revised Directive on security of network and information systems was accompanied by an impact assessment, which was submitted to the Regulatory Scrutiny Board (RSB) on 23 October 2020 and received a positive opinion with comments by the RSB on 20 November 2020.

A political agreement was reached on 13 May 2022.

Revision of the NIS Directive: Questions and answers
Follow the latest progress and learn more about getting involved.
Follow the Commission's work on cybersecurity @CyberSec_EU

**Latest News**

**DIGIBYTE | 30 September 2022**
Launch of the 10th anniversary of the European Cybersecurity Month

The 10th edition of the European Cybersecurity Month, this year titled “Think Before U click – I choose to be safe online”, starts today.

**PRESS RELEASE | 15 September 2022**
New EU cybersecurity rules ensure more secure hardware and software products
The Commission presented yesterday a proposal for a new Cyber Resilience Act to protect consumers and businesses from products with inadequate security features.

DIGIBYTE | 20 June 2022
Team Europe - Winners of the 1st International Cybersecurity Challenge

ENISA, the EU agency for Cybersecurity, has organized for the first time an International Cybersecurity Challenge (ICC) for young cyber players.

PRESS RELEASE | 08 June 2022
Executive Vice-President Vestager and Vice-President Schinas at the International Cybersecurity Forum in Lille

Margrethe Vestager, Executive Vice-President for a Europe Fit for the Digital Age, and Margaritis Schinas, Vice-President responsible for the Security Union are participating in the International Cybersecurity Forum that is taking place in Lille, France until tomorrow 9 June.

Browse Cybersecurity
The European Union works on various fronts to promote cyber resilience, safeguarding our communication and data and keeping online society and economy secure.

State-of-play of the transposition of the NIS Directive
The Commission, together with European Union Agency for Network and Information Security, works closely with the Member States to ensure the NIS Directive's transposition into national legislation.

NIS Cooperation Group

The Network and Information Systems Cooperation Group was established by the NIS Directive to ensure cooperation and information exchange among Member States.

See Also

EU Cyber Resilience Act

New EU cybersecurity rules ensure safer hardware and software.

European Cybersecurity Competence Network and Centre

The European Cybersecurity Network and Cybersecurity Competence Centre help the EU retain and develop cybersecurity technological and industrial capacities.

Stakeholder Cybersecurity Certification Group

The Stakeholder Cybersecurity Certification Group was established to provide advice on strategic issues regarding cybersecurity certification.

The EU Cybersecurity Act

The Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.

The EU cybersecurity certification framework

The EU cybersecurity certification framework for ICT products enables the creation of tailored and risk-based EU certification schemes.

Source URL: https://digital-strategy.ec.europa.eu/policies/nis-directive