

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.



© iStock by Getty Images -1169999045 aismagilov

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 a 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.

Follow the latest progress and learn more about getting involved.

Follow the Commission's work on cybersecurity @CyberSec_EU

Latest

PRESS RELEASE | 30 September 2021

Trade and Technology Council: Inaugural meeting
agrees on important deliverables and outlines
areas for future EU-US cooperation

At the first meeting of the Trade and Technology
Council (TTC) in Pittsburgh, the EU and the US
agreed on concrete deliverables and outlined the

future scope of work. Notably, the EU and the US committed to cooperating closely on shared priorities such as export controls, foreign investment screening, critical and emerging technology standards including Artificial Intelligence, and secure supply chains including on semiconductors. They also agreed to work together on important global trade issues, such as the challenges posed by non-market economies and trade-related climate and environment

PRESS RELEASE | 30 September 2021

The European Cybersecurity Month is kicking off: 'Think Before U Click'

The ninth edition of the European Cybersecurity Month has kicked off and will run for the entire month of October under the motto 'Think Before U Click'. This is an annual awareness campaign organised by the Commission, the European Union Agency for Cybersecurity (ENISA) and over 300 partners in the Member States, including local authorities, governments, universities, think tanks, NGOs and professional associations.

PRESS RELEASE | 28 June 2021

The European Cybersecurity Competence Centre and Network is now ready to take off

The regulation establishing a new Cybersecurity Competence Centre and a Network of National Coordination Centres has entered into force this week. The Cybersecurity Competence Centre, which will be located in Bucharest, will contribute to strengthening European cybersecurity capacities and to boosting research excellence and the competitiveness of the Union's industry in the cybersecurity field.

PRESS RELEASE | 23 June 2021

EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents

The Commission has laid out a vision to build a new Joint Cyber Unit to tackle the rising number of serious cyber incidents impacting public services, as well as the life of businesses and citizens across the European Union. Advanced and coordinated responses in the field of cybersecurity have become increasingly necessary, as cyberattacks grow in number, scale and consequences, impacting heavily our security. All relevant actors in the EU need to be prepared to respond collectively and exchange relevant information on a 'need to share', rather than only 'need to know', basis.

[Browse Cybersecurity](#)

Related Content

Big Picture

Cybersecurity Policies

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

Dig deeper

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

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>