The NIS2 Directive is the 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 EU cybersecurity rules introduced in 2016 were updated by the NIS2 Directive that came into force in 2023. It modernised the existing legal framework to keep up with increased digitisation and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

The Directive on measures for a high common level of cybersecurity across the Union (the NIS2 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 network and information systems (NIS) authority,
- cooperation among all the Member States, by setting up a Cooperation Group

- 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 Directive.

**NIS 2 Directive (Directive (EU) 2022/2555)**

(https://eur-lex.europa.eu/eli/dir/2022/2555)

Questions & answers
NIS2 Guidelines - application of Article 3 (4) of Directive (EU) 2022/2555
Follow the latest progress and learn more about getting involved.
Follow the Commission's work on cybersecurity @CyberSec_EU (https://twitter.com/cybersec_eu?lang=en)

Latest News

PRESS RELEASE | 31 January 2024

The EU and the United States took an important step to further strengthen their mutual cyber resilience and foster a secure global cyberspace.

PRESS RELEASE | 31 January 2024
First EU-wide cybersecurity certification scheme to make European digital space safer
The Commission has today adopted the first-ever European cybersecurity certification scheme, in line with the EU Cybersecurity Act. The scheme offers a Union-wide set of rules and procedures on how to certify ICT products in their lifecycle and thus make them more trustworthy for users.

DIGIBYTE | 30 January 2024
European Chips Act: Commission publishes guidance on the application process for the status of integrated production facility and open EU foundry

Today the Commission published the guidance document on the application process for “first-of-a-kind” facilities to request the status of integrated production facility and/or open EU foundry, under the second Pillar of the European Chips Act.

PRESS RELEASE | 18 December 2023
The Digital Europe Programme makes €84 million available to strengthen AI and cybersecurity

The Commission has published a series of new calls for proposals for the Digital Europe Programme. A dedicated budget of €84 million is available for activities supporting Security Operation Centres with novel applications of AI and other enabling technologies, for the implementation of cybersecurity EU legislation such as the Cyber Resilience Act, as well as for the European transition to post-quantum cryptography.

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.

**Dig deeper**

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.


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

See Also


On the 18 April 2023, the European Commission proposed the EU Cyber Solidarity Act, to improve the preparedness, detection and response to cybersecurity incidents across the EU.


New EU cybersecurity rules ensure safer hardware and software.


Operators of Essential Services (OES), National Cybersecurity Certification Authorities (NCCAs) and National Competent Authorities (NCAs) for cybersecurity are among the selected applicants that will receive €11 million in funding by the Connecting Europe Facility cybersecurity...


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


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

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

**Source URL:** [https://digital-strategy.ec.europa.eu/policies/nis2-directive](https://digital-strategy.ec.europa.eu/policies/nis2-directive)