European Commission - Press release

New rules to boost cybersecurity of EU's critical entities and networks

Brussels, 17 October 2024

The Commission has adopted today the first implementing rules on cybersecurity of critical entities and networks under the Directive on measures for high common level of cybersecurity across the Union (NIS2 Directive). This implementing act details cybersecurity risk management measures as well as the cases in which an incident should be considered significant and companies providing digital infrastructures and services should report it to national authorities. This is another major step in boosting the cyber resilience of Europe's critical digital infrastructure.

The implementing regulation adopted today will apply to specific categories of companies providing digital services, such as cloud computing service providers, data centre service providers, online marketplaces, online search engines and social networking platforms, to name a few. For each category of service providers, the implementing act also specifies when an incident is considered significant.*

Today's adoption of the implementing regulation coincides with the deadline for Member States to transpose the NIS2 Directive into national law. As of tomorrow, 18 October 2024, all Member States must apply the measures necessary to comply with the NIS2 cybersecurity rules, including supervisory and enforcement measures.

Next Steps

The implementing regulation will be published in the Official Journal in due course and enter into force 20 days thereafter.

Background

The first EU-wide law on cybersecurity, the NIS Directive, came into force in 2016 and helped to achieve a common level of security of network and information systems across the EU. As part of its key policy objective to make Europe fit for the digital age, the Commission proposed the revision of the NIS Directive in December 2020. After entering in force in January 2023, Member States had to transpose the NIS2 Directive into national law by 17 October 2024.

The NIS2 Directive aims to ensure a high level of cybersecurity across the Union. It covers entities operating in sectors that are critical for the economy and society, including providers of public electronic communications services, ICT service management, digital services, wastewater and waste management, space, health, energy, transport, manufacturing of critical products, postal and courier services and public administration.

The Directive strengthens security requirements imposed on the companies and addresses the security of supply chains and supplier relationships. It streamlines reporting obligations, introduces more stringent supervisory measures for national authorities, as well as stricter enforcement requirements, and aims at harmonising sanctions regimes across Member States. It will help increase information sharing and cooperation on cyber crisis management at a national and EU level.

For More Information

Implementing Act

Factsheet on the Directive on measures for high common level of cybersecurity across the Union (NIS2)

Questions and Answers on NIS2: New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient

**Updated on 17/10/2024 15:05*

IP/24/5342

Quote(s):

"Cybersecurity is one of the main building blocks for the protection of our citizens and our infrastructure. In today's cybersecurity landscape, stepping up our capabilities, security requirements and rapid information sharing with up-to-date rules is of paramount importance. I urge the remaining Member States to implement these rules at national level as fast as possible to ensure that the services which are critical for our societies and economies are cyber secure."
Margrethe Vestager, Executive Vice-President for a Europe Fit for the Digital Age - 17/10/2024

Press contacts:

Thomas Regnier (+32 2 29 9 1099)
Roberta VERBANAC (+32 2 298 24 98)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email