



European Commission

# HITTING THE REFRESH BUTTON ON CYBERSECURITY RULES

## NIS2: DIRECTIVE ON MEASURES FOR A HIGH COMMON LEVEL OF CYBERSECURITY ACROSS THE UNION

16 January 2023  
#DigitalEU

The first EU-wide law on cybersecurity, [the NIS Directive](#), came into force in 2016 and helped achieve a higher and more even level of security of network and information systems across the EU. In view of the unprecedented digitalisation, new rules now ensure stronger cybersecurity.

### How?

#### NIS



#### Greater capabilities

EU Member States improve their cybersecurity capabilities.

More stringent supervision measures and enforcement are introduced.



#### Cooperation

Increased EU-level cooperation.

Establishment of European Cyber crises liaison organisation network (EU- CyCLONe) to support coordinated management of large scale cybersecurity incidents and crises at EU level



#### Cybersecurity risk management

Operators of Essential Services (OES) and Digital Service Providers (DSP) have to adopt risk management practices and notify significant incidents to their national authorities.

Strengthened security requirements with a list of focused measures including incident handling and crisis management, vulnerability handling and disclosure, policies and procedures to assess the effectiveness of cybersecurity risk management measures, basic computer hygiene practices and cybersecurity training, the effective use of cryptography, and human resource security, access control policies and asset management.

#### NIS2

A list of administrative sanctions, including fines for breach of the cybersecurity risk management and reporting obligations is established.

Increased information sharing and cooperation between Member State authorities with enhanced role of the Cooperation Group.

Coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU is established.

Cybersecurity of supply chain for key information and communication technologies will be strengthened.

Accountability of the company management for compliance with cybersecurity risk-management measures.

Streamlined incident reporting obligations with more precise provisions on the reporting process, content and timeline.

# SECTORS COVERED BY THE NIS DIRECTIVE

## NIS



## NIS2

Expanded scope to include more sectors and services as either essential or important entities.

