

New sectors

Important entities

NIS1 sectors

Essential Entities



Research



Digital Providers



Food



Chemicals



Manufacturing



Postal services



Waste Management

# NIS2

## EU Directive on Measures for a High Common Level of Cybersecurity Across the Union



Energy



Public Administration



ICT service Management



Waste water



Digital infrastructure



Drinking water



Health



Financial Market Infrastructures



Transport



Banking



Space

### Timeline



On **16 January 2023**  
-  
**Enters into force**

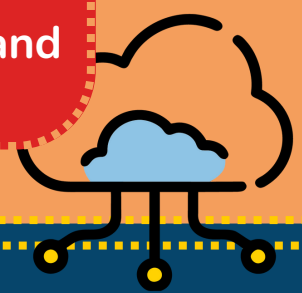
Additional guidelines adopted by the EU

By **17 October 2024**  
-  
**Enforceable**

### Requirements for Companies

Adopt appropriate and proportionate technical, operational and organisational cybersecurity risk-management measures to prevent or minimise the impact of cyber incidents, incl.

Sanctions include **binding instructions, order to implement the recommendations of a security audit, order to bring security measures in line with NIS requirements, and administrative fines.**



Risk analysis



Risk management



Cryptography



HR security



Security in network and information systems acquisition



Incident handling



Cybersecurity training



Supply chain security



Cyber hygiene



MFA



Information system security



Business continuity

### Incident Notifications

72 hours for incident reporting

24 hours for early warning of a significant incident

without undue delay, communicate any measures or remedies to service recipients potentially affected by a significant cyber incident

One month for a final report



### Attention points

- Possible **prohibition or suspension of certification or authorisation**, or C-level function in case of non-compliance.
- **Administrative fine**: €10M or 2% of the worldwide annual turnover (essential entities) and € 7M or 1,4% of the worldwide annual turnover (important entities).
- **Essential entities** have regular or ad hoc audits
- **Important entities** have ad hoc audits, following information on potential NIS2 infringement.
- **National authorities** appointed for large-scale cybersecurity incidents and crises management, supported by the cyber crisis liaison organisation network (CYCLONE)

### What does CYEN do?

Supports you understand and implement NIS2 requirements, taking due consideration of the specificities of your sector and organisation.

Contact us at [info@cyen.eu](mailto:info@cyen.eu) to get a free consultation and learn more!

Follow us on LinkedIn and subscribe to our Youtube channel.

CYEN

