KYBERX

NIS2 | NETWORK AND INFORMATION SECURITY

EU Regulation
2022/2555

Compliance is required
from 17 October 2024

Non-sector-specific: Aiming to achieve a high common level of cybersecurity across the European Union.

Original NIS 2016 (EU Regulation 2016/1148) – 1st EU-wide cybersecurity law

GOAL:

Ensure high and constant level of cybersecurity in important industries

- Operators of essential services
- Digital services providers (search engines, online marketplaces, cloud operators)

CHALLENGES:

- Insufficient monitoring of implementation (supervision)
- Unclear definitions (industries covered)
- Too narrow scope (industries covered)
- Different starting levels
- Different reporting requirements

AS SECURE AS THAT.

HISTORY:

- 2016 – NIS
- Dec-2022 – NIS2 signed
- Jan-2023 – enters into force
- 17-Oct-2024 – compliance enforcement begins

SUMMARY:

- Critical industries (50 people, 7M EUR Revenue) in essential or important industries – directive lists
- Sec min requirements: 13 main areas – NIS2 article 21 & 23

Industries (Different fines essential vs important)

Essential:

- Energy
- Transport
- Bank
- Health
- Water
- IT infra
- ICT services
- Public administration
- Space

Important:

- Postal
- Waste
- Chemicals
- Food
- Manufacturing
- Digital Providers

13 key areas

- Risk Management and Information Security Policies
- Incident Management
- Logging & Detection
- Business Continuity, Backups & Disaster Recovery
- Third-Party Risk
- Secure Development
- Cyber Resilience Testing
- Cyber Hygiene & Cybersecurity Training
- Encryption & Secure Communications
- Human Resource Security
- Access Control
- Asset Management
- Multi-Factor Authentication (MFA)

15-step Checklist to Compliance

1. Understanding the scope
2. Risk assessment
3. Information security policies and procedures
4. First-party risk management
5. Incident response plan
6. Continuous monitoring for potential threats and risks
7. Business continuity plans (incl. backups and DR)
8. Third-party risk management
9. Secure Development
10. Regular testing of cyber resilience
11. Encryption
12. Human Risk Management
13. Access Control
14. Asset Management
15. Multi-Factor Authentication (MFA)

Non-compliance consequences:

Binding instructions

Administrative fines:

- 10M EUR or 2% global annual turnover (essential) whichever is greater
- 7M EUR or 1.4 % global annual turnover (important) whichever is greater

Coverage (up to) by other cybersecurity frameworks:

ISO27001 – extensively 80 %

NIST CSF – quite extensively 75 %

Cyber Essentials – quite extensively 50 %

SOC2 – somewhat 20 %