Network and Information Security (NIS) Directive 2
Make 'Europe fit for the digital age'

The Directive

- Will become LAW 17th October 2024 in all EU Member States
- Three General Objectives
  1. Increase Cyber-Resilience across EU Relevant Sectors
  2. Reduce Inconsistencies across EU
  3. Improve the level of joint situational awareness and the collective capability to prepare and respond
- NIS2 expanded on NIS1 to include not just Critical infrastructure but also 5G

Seven key elements that all companies must address or implement as part of the measures they take, including incident response, supply chain security, encryption and vulnerability disclosure. In addition, the proposal envisages a two-stage approach to incident reporting.

1. Affected companies have 24 hours from when they first become aware of an incident to submit an initial report
2. Followed by a final report no later than one month later.

These sanctions include binding instructions, an order to implement the recommendations of a security audit, an order to bring security measures into line with NIS requirements, and administrative fines (up to €10 million or 2 % of the entities' total turnover worldwide, whichever is higher).

**Directive does not apply to entities carrying out activities in areas such as defence and national security, public security, law enforcement and the judiciary. Parliaments and central banks are also excluded from the scope

THE SOLUTION

Certes protects the data not matter where it travels through its Patented strong encryption. The addition of detailed meta data / Observability engine and API functionality allow Certes to integrate into security reporting solutions.

NIS 2

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

- PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR SERVICES
- WASTE WATER AND WASTE MANAGEMENT
- MANUFACTURING OF CERTAIN CRITICAL PRODUCTS (SUCH AS PHARMACEUTICALS, MEDICAL DEVICES, CHEMICALS)
- FOOD
- DIGITAL SERVICES SUCH AS SOCIAL NETWORKING SERVICES PLATFORMS AND DATA CENTRE SERVICES
- SPACE
- POSTAL AND COURIER SERVICES
- PUBLIC ADMINISTRATION

NIS

EU Member States improve their cybersecurity capabilities.

Increased EU-level cooperation.

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

Greater capabilities

More stringent supervision measures and enforcement are introduced.

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

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.

NIS 2

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.

CERTES = Simplifying NIS2 Compliance through Patented Data Protection

Contact Certes Networks

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

www.certesnetworks.com

Tel: 1 (888) 833-1142
Fax: 1 (412) 262-2574

sales@certesnetworks.com
info@certesnetworks.com

CERTES NETWORKS