SQUIRE PATTON BOGGS

Are you NIS2 ready?

What You Should Know and What You Should Do

Background

The Network and Information Security (NIS) Directive was the first piece of EU-wide legislation on cybersecurity, aimed to achieve a high common level of cybersecurity across the member states.

However, its implementation proved difficult, and resulted in fragmentation at different levels across the internal market. To respond to the growing threats posed with digitalization and the surge of cyber-attacks, the European Commission submitted a new proposal to replace the NIS Directive: NIS2. The final text was adopted on December 14, 2022 and focused on:

- Responding to cyber-threats by enforcing higher level of common security practices
- Ensuring uniformity in implementation across EU MS
- Expanding scope to cover additional sectors

Impact on other laws

- **DORA** – Specialized cybersecurity regulation to be considered in the financial sector.
- **EECC** – Telecoms providers are covered by the current NIS framework if they provide non-telecoms services that fall within the scope of the directive, i.e. cloud computing services. NIS2 repeals the corresponding EECC security provisions and entirely regulate the security of telecoms providers.

Jurisdiction

MS where it is established, in exception of:

- Providers of public electronic communications network or providers of public electronic communications services: MS where they offer their services.
- DNS providers, registries of top-level domain names, entities offering domain name registration services, cloud computing service providers, managed security service providers, as well as providers of online marketplaces, online search engines or social networking service platforms: MS where they have their main establishment.
- Public administration entities: MS that created them.

Scope

Two main criteria

1. Size:

At least, medium-sized enterprise (**Recommendation 2003/361/EC**) *

To calculate the size of an organization which is part of a group, implies the consolidation of the data of the different components of the group. This may be waived in certain circumstances.

*Exceptions apply.

2. The provided service:

Annex I: High Criticality

- Drinking water
- Energy
- Space
- Transport
- Health
- Digital Infrastructure
- Financial Market Infrastructure
- Banking
- Waste Water
- ICT service management
- Public administration

Annex II: Other Critical Sectors

- Digital Providers
- Waste Management
- Research
- Postal and courier services
- Manufacture production and distribution of chemicals
- Food production and distribution

2 categories:

Essential

- If large enterprise + Service of Annex I

Important

- If medium-sized enterprise + Service of Annex I
- If large or medium-sized enterprise + Service of Annex II

Difference in control and sanction mechanisms

Recommendation 2003/361/EC			
Type	**Staff headcount**	**Financial ceilings**	
		Actual turnover	Annual balance sheet
Large enterprise	> 250 employees	> €50 million	> €43 million
Medium-sized enterprise	> 50 employees	> €10 million	

Key obligations:

Reporting

Essential and important entities to report any significant incident without undue delay to the competent national authorities.

Significant incident:

- Has caused, or is capable of causing serious operational disruption to services in the sectors or subsectors or financial losses to the entity concerned
- Has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage

Steps:

1. **Early warning** – Within **24 hours** of becoming aware à minimal info (sectors/territories affected and if malicious intent)

2. **Complete incident report** – Within **72 hours** of becoming aware

3. (Where applicable) **Notify recipients** of their services potentially affected: **without undue delay**. Also measures or remedies that the recipients are able to take in response to the threat of the incident.

4. **(Possible) interim or progress report** – If requested by authorities

5. **Final report** – **One month** after first warning.

Registration

General registry of essential and important entities:

- Entities under scope shall submit the following information to the competent authorities:
  - Name of the entity
  - The address and up-to-date contact details, including email addresses, IP ranges and telephone numbers
  - Where applicable, the relevant sector and subsector
  - Where applicable, a list of the MS where they provide services falling within the scope of the Directive

  Deadline for MS to have final list – **April 17, 2025**
- DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, to register on the basis of the information received from the single points of contact.

  Information to be provided:
  - Name of the entity
  - Relevant sector, subsector and type of the entity referred to in Annex I or II, where applicable
  - The address on the entity's main establishment and its other legal establishments in the Union (or its representative)
  - MS where the entity provides services
  - The entity's IP ranges

  Deadline for submission: **January 17, 2025**

Security Requirements

Essential and important entities must take appropriate and proportionate measures to manage the risks to the security of their network and information systems, and to prevent or mitigate the effects of incidents on the recipients of their services and on other services.

At minimum, these measures include:

- Risk analysis and information systems security policies
- Incident handling
- Business continuity, such as backup management and disaster recover and crisis management
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers' or service providers' security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Basic cyber hygiene practices and cybersecurity training
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption
- Human resources security, access control policies and asset management
- Use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

Members of governing bodies of entities should undergo **cybersecurity training** and provide similar training to their **employees** on a regular basis.

Supervision:

Entities subject to:

- **Essential entities ex-ante/important entities when provided with evidence, indication or information** that an important entity allegedly does not comply with NIS2
- **On-site inspections and off-site supervision**, including random checks based on risk assessment or risk-related information
- **Security scans** based on objective, non-discriminatory, fair and transparent risk assessment criteria
- **Companies to provide**:
  - Necessary documentation to assess adopted cybersecurity measures including proof the implementation of IS policies
  - Access to data, documents or any information necessary for the performance of their supervisory tasks
  - Evidence of implementation of cybersecurity policies

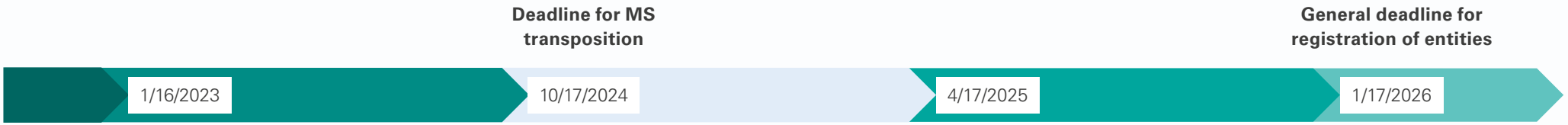
Enforcement:

- **Warning – cease and desist**
- **Public statements**
- **Fines** (administrative an/or personal)
  - For **essential entities** – **Up to €10 million or at least 2%** of the **total annual worldwide turnover** in the previous fiscal year of the company to which the essential entity belongs, whichever is higher
  - For **important entities** – **Up to €7 million or at least 1.4%** of the **total annual worldwide turnover** in the previous fiscal year of the company to which the important entity belongs, whichever amount is higher
- **Liability of management bodies** – Natural persons representing essential entities may be held liable for failure to comply.

Next Steps:

- Confirm your organization's obligations for NIS2.
- Educate and onboard relevant influential individuals for governance obligations.
- Map the NIS2 requirements to a framework that can be used across the organization.
- Conduct a holistic gap assessment across existing controls in place within the organisation.
- Establish the level of effort required to achieve compliance.

Timeline



Key Contacts

Annette Demmel
Partner, Berlin
T +49 30 72616 8000
E annette.demmel@squirepb.com

Bartolomé Martín
Partner, Madrid
T +34 91 426 4867
E bartolome.martin@squirepb.com

Mareike Lucht
Senior Associate, Berlin
T +49 30 72 616 8131
E mareike.lucht@squirepb.com

Claire Murphy
Senior Associate, Madrid
T +34 91 520 0771
E claire.murphy@squirepb.com

66343/09/24