Greece transposes NIS2 Directive on Cybersecurity

Long-awaited **Law 5160/2024** transposed NIS2 Directive 2022/2555 which aims to establish a high common level of cybersecurity across the EU. The Law **strengthens security requirements**, addresses supply chain security, streamlines reporting obligations, and introduces more stringent supervisory measures and enforcement requirements; notably, it also introduces **personal liability** for members of the management of entities within the scope of the Law.

Entities within scope

Law 5160/2024 (the "Law") affects both public and private sector entities established or operating in Greece, that provide their services or carry out activities in critical and highly critical sectors; the applicability depends on their size, type of service or criticality of the activity.

Indicative sectors within scope include:

- Energy
- Banking
- Digital infrastructure
  (cloud computing service providers, data centre service providers, providers of public electronic communications services/networks, etc.)
- Postal and courier services
- Manufacture, production and distribution of chemicals
- Manufacturing
- Transport
- Health
- Space
- Waste management
- Production, processing and distribution of food
- And others

Obligations

Cybersecurity risk-management measures:

Must take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems based on an all-hazards approach, indicatively including:

- policies on risk analysis and information system security
- incident handling
- business continuity
- supply chain security
- basic cyber hygiene practices and cybersecurity training
- policies and procedures regarding the use of cryptography and encryption
- human resources security, access control policies and asset management
- the use of multi-factor authentication or continuous authentication solutions

Communication and Information Systems Security Officer:

Must appoint a Communication and Information Systems Security Officer (CISO).

Cybersecurity policy & asset inventory:

Must have in place a unified cybersecurity policy (to be approved by the National Cybersecurity Authority) and maintain a comprehensive inventory of tangible and intangible information and communication assets.

Registry of entities:

Certain entities (e.g., cloud computing service providers, data centre service providers, content delivery network providers, providers of online marketplaces, entities providing domain name registration services, etc.) must register with the National Cybersecurity Authority (exceptions and timelines apply).

Reporting obligations:

Must notify significant cybersecurity incidents to the CSIRT of the National Cybersecurity Authority and inform affected service recipients (exceptions and timelines apply).

Management duties and liability

Management of essential and important entities must:

- **Approve** the cybersecurity risk-management measures taken by those entities (until 27.02.2025)
- **Oversee** the implementation of said measures and are liable for infringements by the entities of relevant obligations
- Follow **training** and arrange for similar training to be provided to employees (at least on an annual basis)

Management *essential* entities (for instance, legal representatives) are responsible to ensure compliance with the Law and may be held liable for breach of their duties to ensure compliance with the Law; monetary fines may be imposed on the member of the management for breach of relevant provisions.

Under certain circumstances, the National Cybersecurity Authority may prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the *essential* entity from exercising managerial functions in that entity.

Sanctions

Non-compliance can result in significant sanctions, ranging from EUR 100,000 to EUR 10,000,000, depending on the nature and severity of the breach.

What we can do for you

Navigating the complexities of the Law can be a challenging exercise, requiring careful attention to both legal and technical requirements. As trusted partner to numerous organisations operating in critical sectors in Greece, we are well-positioned to support your compliance journey.

Our comprehensive services include:

- **Legal guidance** on interpreting and complying with the NIS2 Directive and Law 5160/2024
- **Collaboration with IT partners** to implement robust cybersecurity measures and risk management strategies
- **Assistance with the appointment of a CISO** and the development of your cybersecurity policy
- **Help with registering** with the National Cybersecurity Authority and fulfilling reporting obligations
- **Management training and awareness programs** tailored to your organisation's needs
- **Guidance on liability risks** and ensuring your management team is fully prepared for compliance requirements

We offer a **holistic approach**, combining legal expertise with practical IT solutions to help you meet your obligations efficiently and effectively. Please contact us for a tailored consultation on how we can help ensure your organisation's compliance with the new cybersecurity requirements.

Contact us

Theodore Konstantakopoulos
Partner | Head of TMT & Data

t.konstantakopoulos@zeya.com

Iliana Papantoni
Associate

i.papantoni@zeya.com