Platis - Anastassiadis
& Associates
the associate law firm of EY Greece

February 2025
Law Alert

L.5160/2024: Transposition of Directive NIS 2 on measures for a high common level of cybersecurity across the Union

The better the question. The better the answer. The better the world works.

Law 5160/2024 (Government Gazette A'/195/27-11-2024) incorporates the NIS 2 Directive into Greek legislation. This legislation establishes a comprehensive framework of obligations, measures, and rules designed to achieve a high common level of cybersecurity across the European Union. By doing so, it aims to strengthen the internal market and enhance the overall resilience of cybersecurity systems within Greece and the Union.

On November 27, 2024, Law 5160/2024, entitled 'Implementation of Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022, on measures to achieve a high common level of cybersecurity throughout the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) and other provisions' (Government Gazette A'/195/27-11-2024), hereinafter referred to as the 'Law,' was published in the Government Gazette.

According to the explanatory report of the Law, the new provisions aim to harmonize national law with Directive (EU) 2022/2555 to ensure a high common level of cybersecurity across all Member States of the Union. The Law transposes Directive NIS 2, which replaces the previous Directive NIS 1.

The NIS 2 Directive significantly broadens the scope of liable entities by introducing additional sectors subject to its cybersecurity measures.

Furthermore, it establishes new requirements for cybersecurity risk and incident management, enhances incident reporting obligations, and intensifies the oversight and sanction regime.

Notably, the NIS 2 Directive imposes accountability obligations on top management in cases of non-compliance and introduces more stringent reporting requirements for entities falling under its scope.

1. Purpose & Subject Matter

The purpose of the Law is to achieve a high level of cybersecurity by incorporating the NIS 2 Directive into the Greek legal framework.

In this context, the subject matter of the Law includes:

- Defining the competent national authority responsible for the supervision and implementation of the Law at technical, operational, and strategic levels.
- Enforcing the adoption of measures to enhance the cybersecurity of essential and important entities.
- Strengthening cooperation among all stakeholders.
- Establishing an effective, proportionate, and dissuasive supervisory mechanism to ensure compliance with the obligations set forth in the Law.

2. Scope

The scope of the Law includes highly critical areas as well as all sectors essential for the protection of socio-economic life in cyberspace.

In particular, a single criterion with quantitative characteristics is established to identify entities that fall within the scope of the Law. It is specified that all entities providing services or engaging in activities in Greece are covered if they meet the following cumulative criteria:

- Qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article and,
- They operate in the sectors and provide the types of services or engage in activities specified in Annex I or II of the Law.

Additionally, certain entities operating in the sectors listed in Annexes I or II of the Law, regardless of their size, fall within its scope if they meet specific qualitative criteria that highlight their key role in society, the economy, or specific sensitive sectors. For example, an entity may be included if it is the sole provider of such services in the country or is deemed critical due to its significant importance at the national or regional level.

3. Classification into essential and important entities

The entities falling within the scope of the Law are classified into two (2) categories as follows:

- Essential entities include:
  - Any company or organization that exceeds the thresholds for medium-sized enterprises and operates in the following sectors listed in Annex I of the Law: energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure (including telecommunications service providers, cloud service providers, data center providers, etc.), and ICT service management (Managed Service Providers and Managed Security Service Providers - MSSPs).
  - Public administration entities.
  - Providers of DNS services, TLD name registries, and trust services, regardless of their size.
  - Entities identified in Annexes I and II of the Law based on specific criteria.
  - Organizations falling within the scope of Directive (EU) 2022/2557.
  - Organizations recognized under Article 4 of Law No. 4577/2018 and Article 16 of the Minister of State's decision No. 1027/4.10.2019, prior to January 16, 2023, as operators of essential services.
- Important entities include:
  - Any company or organization that exceeds the thresholds for medium-sized enterprises and operates in the following sectors listed in Annex II of the Law: postal and courier services; waste management; manufacturing; production and distribution of chemicals; production, processing, and distribution of food; manufacturing of equipment (including medical, electronic, and mechanical equipment); digital providers (such as online marketplaces, search engines and social media platforms); and research organizations.
  - Any undertaking or organization listed in Annexes I and II that does not meet the size criterion but is recognized by Member States as an essential entity based on specific criteria.

It is important to note that the provisions of the Law regarding cybersecurity risk management, incident reporting, and supervisory obligations do not apply to financial entities governed by Regulation (EU) 2022/2554 (DORA Regulation), which establishes stricter requirements specific to financial services. In this context, the DORA Regulation serves as a lex specialis in relation to the NIS 2 Directive
According to the Law, the National Cybersecurity Authority is required to establish a list of essential and important entities, as well as entities providing name registration services, which will include essential information for each entity.

4. Risk Management Measures

Essential and important entities are required to implement proportionate technical, operational, and organizational measures to manage the security risks associated with the network and information systems used in their activities and services. These measures aim to prevent or minimize the impact of incidents on service recipients and other organizations.

Such measures must at least include the following:

- policies and procedures on risk analysis and information systems security;
- incident handling;
- business continuity, such as backup management and disaster recovery, and crisis management;

- supply chain security measures;
- security in network and information systems acquisition, development and maintenance;
- policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- basic cyber hygiene practices and controls;
- policies for the use of cryptography in collaboration with the national CRYPTO authority;
- human resource security and access control policies;
- use of multi-factor authentication and secure communication systems.

Furthermore, essential and important entities are required to:

- Designate a competent executive as the Information and Communication Systems Security Officer (I.A.S.P.E.), who will serve as the primary point of contact with the National Cybersecurity Authority and oversee compliance with the requirements of the Law;
- Maintain a unified cybersecurity policy, subject to annual approval by the National Cybersecurity Authority;
- Maintain a comprehensive inventory of all information and communication assets, both tangible and intangible, categorized by criticality.

5. Reporting obligations

Under the Law, essential and important entities must report any significant incidents to the Computer Security Incident Response Team (CSIRT) of the National Cybersecurity Authority. An incident is deemed significant if it results in a serious disruption of services or financial loss to the entity or other individuals or organizations.

Incident reporting follows a multi-stage approach. Within 24 hours of detecting an incident, an initial warning must be submitted to the National Cybersecurity Authority. A more detailed notification follows within 72 hours, with interim updates provided upon request. Finally, a comprehensive report containing all legally required details must be submitted no later than one month after the initial notification.

6. Supervision and Enforcement

The Law designates the National Cybersecurity Authority as the competent authority responsible for overseeing its implementation and serving as the single point of contact for cross-border cooperation.

For essential entities, the National Cybersecurity Authority has the power to conduct regular, ad hoc, and targeted security audits, on-site inspections, and off-site supervision. It may also request information, access data, issue binding instructions, and impose non-monetary administrative sanctions, such as the suspension of certifications or service authorizations.

Additionally, individuals holding managerial roles, including managing directors and legal representatives, may be temporarily prohibited from exercising their functions.

For important entities, supervisory measures include preventive oversight both on- and off-premises, targeted security assessments, on-site inspections, security scans, spot checks, and the issuance of binding instructions. The Law also establishes administrative fines of up to €10,000,000 or 2% of global annual turnover for essential entities and up to €7,000,000 or 1.4% of global annual turnover for important entities.

7. Compliance deadlines and submission of information to the registry

The Law requires the management of liable entities to implement organizational and technical cybersecurity measures, ensure staff training, and foster a strong cybersecurity culture within the entity. In this regard, management bodies must approve the necessary measures within three (3) months of the Law's entry into force and ensure their effective implementation. Furthermore, in order to establish the relevant Registry, essential and important entities, as defined in Article 4(3) of the Law, must submit the required information by April 11, 2025. Certain categories of providers, including DNS service providers, TLD registries, domain name registration service providers, cloud computing service providers, data centers, content distribution networks, managed security service providers, as well as operators of online marketplaces, search engines, and social media platforms, must submit their information by March 28, 2025. The creation of a digital platform and the details regarding the submission of the required information are specified in Joint Ministerial Decision 1381/2025 – Government Gazette B' 463/10.2.2025.

Until the designated platform becomes operational, entities must submit the required data via email to register.ncsa@cyber.gov.gr. Upon submission, they will receive a confirmation email with a protocol number.

The Law is available here.

About Platis – Anastassiadis & Associates

Platis - Anastassiadis & Associates is part of the EY Law network operating in 90 countries globally and is comprised of 3,500+ people.

We are an independent law office with a core team of 45 lawyers. Our office provides high quality legal services across the full range of commercial and financial transactions.

Especially in our geographical area, we have established an ongoing cooperation with the respective law firms which are associated with EY, in order to offer seamless and consistent regional services to our clients that have cross country operations.

Our experience allows us to better understand our clients' needs and offer them integrated multidisciplinary solutions in the fields of accounting, tax and financial advisory services. Platis – Anastassiadis & Associates law office is solution focused. We work closely with our clients to seek innovative and practical ways of dealing with their issues. Our priority is to help our clients meet their business objectives. Our expertise, commitment and enthusiasm has resulted in the build up of a client base which includes local and international listed, state and private sector companies and financial institutions.

For more information on digital law issues, please contact:

Eirinikos Platis
Partner
eirinikos.platis@gr.ey.com

Antonios Broumas
Senior Manager
antonios.broumas@gr.ey.com

at the
Platis - Anastassiadis & Associates Law Partnership
Tel.: +30 210 2886 512
legaloffice@gr.ey.com

ey.com

EY EY Greece eygreece @EY_Greece EY Greece