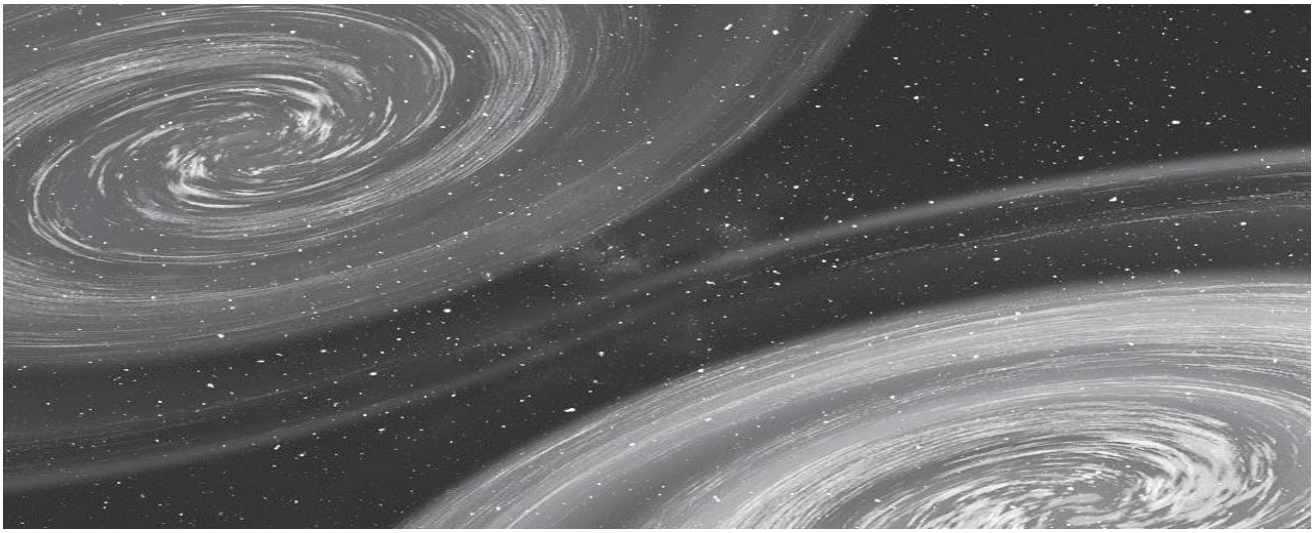

Greece transposes Directive (EU) 2022/2555 re Cybersecurity – Are you Compliance Ready?

Introduction

The Greek Parliament has finally voted Law 5160/2024 (Government Gazette A'195/27.11.2024) entitled "*Transposition of the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*"

NIS 2 (and consequently the respective new Law voted last week in Greece) modernizes the existing legal framework to keep up with increased digitization and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole (ar. 2 L. 5160/2024).

Scope of application

The new legislation applies to public or private entities of a type referred to in Annex I (High criticality sectors) or II (Other critical sectors) which 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 which provide their services or carry out their activities within the Greek territory (ar. 3 L. 5160/2024).

High criticality sectors (Annex I L. 5160/2024)

Energy
Transport
Finance
Financial market infrastructures
Public Administration
Health
Space
Water supply (drinking & wastewater)
Digital Infrastructure

Other critical sectors (Annex II L. 5160/2024)

Postal Services
Waste Management
Chemicals
Research
Foods
Manufacturing
Digital Providers

Regardless of their size, the law also applies to entities of a type referred to in Annex I or II as aforementioned, where (ar. 3 par. 2 Law 5160/2024):

(a) services are provided by:

i. providers of public electronic communications networks or of publicly available electronic communications services;

ii. trust service providers;

iii. top-level domain name registries and domain name system service providers;

(b) the entity is the sole provider of a service which is essential for the maintenance of critical societal or economic activities;

(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;

(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;

(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in Greece;

(f) the entity is a public administration entity:

i. of central government; or

ii. Local government organization of 1st or 2nd Degree.

Regardless of their size, the Law also applies to entities identified as critical entities under Directive (EU) 2022/2557.

Regardless of their size, the Law further applies to entities providing domain name registration services.

Essential and Important entities (ar. 4 Law 5160/2024)

Essential entities

Entities:

(a) in high criticality sectors which exceed medium size threshold;

(b) qualified trust service providers and top-level domain name registries, as well as DNS service providers, regardless of their size;

(c) providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC;

(d) public administration entities of central government.

Important entities

(a) Entities in high criticality sectors of small or medium size;

(b) Entities in other critical sectors which exceed medium size threshold

The Greek National Cybersecurity Authority

The Authority establishes a list of essential and important entities, as well as entities providing domain name registration services based on

respective declarations to take place through an online platform (ar. 4 par. 3 Law 5160/2024) and is further responsible to provide for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity (ar. 7 par. 1 Law 5160/2024).

As part of the national cybersecurity strategy, the Authority is entitled to adopt policies:

- addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services;
- promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures;
- promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities;
- supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure;
- promoting active cyber-protection.

ENISA shall assist the Authority, upon its request, in the development or the update of a national cybersecurity strategy and of key performance indicators for the assessment of that strategy, in order to align it with the requirements and obligations laid down in this Directive. The Authority is responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities) and participates in the European cyber crisis liaison organisation network (EU-CyCLONe). The Authority further establishes CSIRTs (Computer Security Incident Response Team)

By 17 April 2025 and every two years thereafter, the Authority shall notify:

(a) the Commission and the Cooperation Group of the number of essential and important entities listed for each sector and subsector referred to in Annex I or II; and

(b) the Commission of relevant information about the number of essential and important entities identified pursuant to Article 2(2), points (b) to (e), the sector and subsector referred to in Annex I or II to which they belong, the type of service that they provide, and the provision, from among those laid down in Article 2(2), points (b) to (e), pursuant to which they were identified.

Until 17 April 2025 and upon request of the Commission, the Authority may notify the Commission of the names of the essential and important entities (ar. 4 §§5, 6 Law 5160/2024).

Organizational (entities') Obligations and Requirements

The legislation at stake introduces new requirements and obligations for organizations in four overarching areas: risk management, corporate accountability, reporting obligations, and business continuity (ar. 14-16 Law 5160/2024).

Governance

The management bodies of essential and important entities must approve the cybersecurity risk-management measures taken by those entities in order to comply with the law within 3 months from the publication of the law, oversee its implementation and can be held liable for infringements by the respective entities.

The members of the management bodies of essential and important entities are further required to follow training, and shall encourage

3, Stadiou str., 105 62 Athens, Greece llf@lambadarioslaw.gr +30 210 3231135 www.lambadarioslaw.gr

essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

The law also mandates the appointment of an Officer responsible for the Security of Information and Communications Systems. This officer is tasked with ensuring compliance with the requirements of the Greek Cybersecurity Law and managing communications with the National Cybersecurity Authority.

Cybersecurity risk-management measures

Essential and important entities must take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services.

These measures shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the 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.

Reporting obligations

Essential and important entities notify, without undue delay, the authority of any incident that has a significant impact on the provision of their services. The mere act of notification shall not subject the notifying entity to increased liability.

Essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.

An incident shall be considered to be significant if:

(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;

3, Stadiou str., 105 62 Athens, Greece llf@lambadarioslaw.gr +30 210 3231135 www.lambadarioslaw.gr

(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

For the purpose of the above notifications, the entities concerned submit to the competent authority:

(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

(b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

(c) upon the request of the competent authority, an intermediate report on relevant status updates;

(d) a final report not later than one month after the submission of the incident notification under point (b), including the following:

i. a detailed description of the incident, including its severity and impact;

ii. the type of threat or root cause that is likely to have triggered the incident;

iii. applied and ongoing mitigation measures;

iv. where applicable, the cross-border impact of the incident;

(e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

By way of derogation from the aforementioned, a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident.

Registry of entities (ar. 19 Law 5160/2024)

All 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 must mandatorily submit, until, the latest, the 17th of January, 2025, before the National Cybersecurity Authority, the following information:

(a) the name of the entity;

(b) the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable;

(c) the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative;

(d) up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative;

(e) the Member States where the entity provides services; and

(f) the entity's IP ranges.

The entities referred to in the above paragraph must notify the competent authority about any changes to the information they submitted under aforementioned without delay and in any event within three months of the date of the change.

3, Stadiou str., 105 62 Athens, Greece llf@lambadarioslaw.gr +30 210 3231135 www.lambadarioslaw.gr

Penalties for Violations

The law sets out specific penalties for non-compliance, these include:

– Non-monetary remedies (warnings, recommendations, security audit implementation orders etc.);

– Administrative fines;

These penalties can be imposed on essential entities and important entities for infraction such as failure to meet security requirements and failure to report incidents.

General conditions for imposing administrative fines on essential and important entities

The administrative fines imposed through a justified decision by the National Authority on essential and important entities must be effective, proportionate and dissuasive, taking into account the circumstances of each individual case. Said decisions may be issued solely following the hearing of the involved entities according to the provisions of the Code of Administrative Proceedings.

In case of failure to implement risk management measures and report significant incidents, essential entities may incur fines of up to €10m or 2% of their total worldwide annual turnover, while important entities can be fined up to €7m or 1.4% of their total worldwide annual turnover. Lower ceilings apply for other infringements of the Law.

Last but not least, the authority is competent to hold organization managers personally liable if gross negligence is proven after a cyber-incident. This includes:

– Ordering that organizations make compliance violations public;

– Making public statements identifying the natural and legal person(s) responsible for the violation and its nature;

– If the organization is an essential entity, temporarily ban an individual from holding management positions in case of repeated violations.

Steps To Prepare For Compliance

Taking into consideration the aforementioned, applicable organizations must take steps to prepare for compliance. These include:

– **Determine if they fall under the law's scope** and which units are impacted;

– **Evaluate security measures**, amend security policies and plan for the legislation compliance;

– **Incorporate new security measures** and incident reporting obligations in supply chain.

Author:

Litigation & White Collar Crime
Arbitration & Dispute Resolution
Harry Karampelis
Partner

C.Karampelis@lambadarioslaw.gr