ROKAS

Articles for Lexology

ROKAS

Date: February 2025

TOPIC:
Enhancing EU Cybersecurity: Legal provisions under NIS II and Greek Law 5160/2024

Author / Title:
Maria Katsioti
Associate

Andreas Papastathis
Junior Partner

Introduction

On December 27th, 2022, the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union *(known as NIS II)* was published in the Official Journal of the European Union, repealing Directive (EU) 2016/1148 *(known as NIS)*. Compared to its predecessor *(the NIS Directive),* NIS II expands its scope to include more sectors, establishes a more coherent and robust supervision framework, reinforces cross-border collaboration between member states, expands the list of proportional cybersecurity risk management measures and introduces more structured incident notification obligations with specific deadlines. The aim is to enhance the level of cybersecurity in the European Union.

According to NIS II, in line with Regulation (EU) 2019/881 *(EU Cybersecurity Act, establishing ENISA as the permanent EU agency for cybersecurity),* the term *"cybersecurity"* means *"the activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats"* In this framework, NIS II provisions for ensuring a high level of cybersecurity are based on three key pillars: **1)** obligations for entities that fall within its scope, **2)** provisions for member states and the National Cybersecurity Authority, and **3)** cooperation at the EU level.

NIS II Directive requires Member States to transpose its provisions into national law by 17 October 2024. In Greece, the Greek Law 5160/2024 transposing the NIS II Directive was published and entered into force on 27 November 2024. This article presents indicatively provisions of the Greek Law 5160/2024 for each pillar and concludes with a comparison of **a)** NIS II Directive with the DORA Regulation and **b)** NIS II Directive with the GDPR.

Obligations for entities under the scope of Greek Law 5160/2024 (1st pillar)

Greek Law 5160/2024 *(hereinafter "the Greek Law")* encompasses several entities in the private domain and in most of the public domain operating in sectors crucial to the economy and society. These include: **a)** Sectors of high criticality, such as energy, digital infrastructure, transport, space, health, public administration, drinking water, banking, financial markets infrastructure and ICT services management; **and b)** other critical sectors, including the manufacture, production and distribution of chemicals, manufacturing, research, postal and courier services, waste management, production, processing, and distribution of food and digital providers. According to the Greek Law, entities in these sectors are categorized as essential or important *(the criteria of the characterization of an entity as essential or important are analytically presented in article 3 and 4 of the Greek Law)*, with essential entities having slightly more obligations, such as stricter supervisory and enforcement measures and administrative fines.

Essential and important entities *(hereinafter "the Entities")* are required to submit the information specified in article 4 paragraph 3, by the extended deadline of 14 March 2025, according to the recent announcement by the Ministry of Development and the Greek National Cybersecurity Authority. Additionally, specific entities outlined in article 19, such as cloud computing, DNS and TLD service providers, must submit the information specified in article 19 paragraph 1 by the extended deadline of 21 February 2025, according to the same joint announcement. Due to the absence of the relevant digital platform, the required information shall be sent by the provided deadline to the email address register.ncsa@cyber.gov.gr. Upon submission, a protocol number will be assigned.

Furthermore, the administrative bodies of the Entities must implement appropriate and proportionate cybersecurity risk management measures. These measures can be technical, organizational, and business-related, aimed at securing the network and information systems used to provide their services to their clients. The measures, as presented in the next paragraph, should align with

international standards and consider factors such as of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

According to article 15 paragraph 2 of the Greek Law, required cybersecurity risk management measures include policies and procedures for risk analysis and information system security, incident management, business continuity, basic cyber hygiene practices and cybersecurity training for both administrative bodies and employees, policies and procedures regarding the use of cryptography and, where appropriate, encryption and 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.

In addition, the Greek Law requires the Entities to report to CSIRT *(Computer security incident response teams*) of Greek NCA *(National Cybersecurity Authority)* significant incidents, i.e. events compromising the availability, authenticity, integrity or confidentiality of data *(personal or not)* or of the services offered by network and information systems and has caused or could cause severe operational disruption or financial loss or damage to natural or legal persons.

The reporting timeframe of Entities is divided into three stages: **a)** without undue delay and within 24 hours of becoming aware of the significant incident, an early warning must be submitted to the Greek NCA. This warning should indicate whether the incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact, if applicable; **b)** without undue delay and within 72 hours of becoming aware of the significant incident, an incident notification must be submitted, which, where applicable, shall update the information referred to the early warning and include an initial assessment of the incident, its severity and impact, and, where available, the indicators of compromise **and c)** a final report must be submitted no later than one month after the incident notification. This report should provide a detailed description of the incident, the type of threat, the mitigation measures applied and ongoing, and, where applicable, the cross-border impact.

Finally, Entities must maintain a cybersecurity policy and designate an Information Systems Security Officer (ISSO). The ISSO must be a different person from the Data Protection Officer, as specified in Article 37 of the GDPR, and must be autonomous in decision-making. The ISSO is responsible for all relevant

communication with the Greek NCA and ensuring the entity complies with cybersecurity risk management measures and incident reporting obligations.

In case of infringement of the cybersecurity risk management measures and reporting obligations, the Greek NCA imposes proportionate and sufficiently justified fines to the Entities. Essential Entities are subject to administrative fines of a maximum of 10 000 000 € or of a maximum of 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher. While, important Entities are subject to administrative fines of a maximum of 7 000 000 € or of a maximum of at 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.

Provisions for National Cybersecurity Authority of Greece (2nd pillar) and cooperation at EU Level (3rd pillar)

The competent Greek authority responsible for supervising and monitoring the compliance of Entities with the Greek Law is the National Cybersecurity Authority (*NCA*), which operates within Greek Ministry of Digital Governance. The NCA imposes supervisory or enforcement measures on Entities. Additionally, NCA is the Greek single point of contact for the implementation of NIS II and the Greek Law, receiving information for the registration of the Entities and incident reports, managing large-scale cyber crisis in Greece and cooperating with authorities from other Member-States and the European Union.

Within the NCA, the Computer Security Incident Response Team *(CSIRT)* is established, responsible for handling incidents related to computer security. Under the framework of the 3rd pillar of NIS II and the Greek Law, the Greek CSIRT may cooperate with national computer security incident response teams from third countries or equivalent bodies, sharing information and providing cybersecurity assistance.

The relation between DORA Regulation and NIS II Directive

Regulation (EU) 2022/2554 on digital operational resilience for the financial sector *(DORA- application from 17 January 2025)* is relevant to NIS II Directive, as it sets out uniform rules on the security of network and information systems of financial entities, such as banks, insurance and investment companies. In relation to financial entities under the scope of NIS II Directive such as credit institutions, DORA is considered sector-specific union legal act *(lex specialis)* for the purposes of article 4 of NIS II Directive. As a consequence, the provisions of NIS II Directive

regarding reporting obligations, cybersecurity risk management and its supervision and enforcement do not apply to financial entities covered at the same time by DORA.

The relation between GDPR and NIS II Directive

The aim of the GDPR is to safeguard exclusively the personal data of individuals processed by the private sector and most of the public sector. Among other obligations, it requires data controllers *(or data processors)* to ensure the security of personal data. In contrast, the NIS II Directive focuses on strengthening and ensuring the security of network and information systems, which may or may not store personal data, of specific entities *(characterized as essential or important)* and the continuous provision of their services.

When essential or important entities are also data controllers processing personal data, they must comply with both legal acts, ensuring the security of personal data *(e.g. personal data of their clients or employees)* and the security of their information systems. Finally, in the event of a breach of both legislations, different provisions and obligations are applied. If the Greek Personal Data Protection Authority imposes administrative fines on an entity for GDPR violations on personal data security, the Greek NCA cannot impose additional fines for breach of NIS II, arising from the same conduct, but it can impose other enforcement measures.