KYRIAKIDES GEORGOPOULOS
LAW FIRM

DATA PRIVACY, CYBERSECURITY AND TECHNOLOGY LAW

Cybersecurity Regulatory Developments in Greece - Key Updates of the Implementation of the NIS2 Directive

February 17, 2026

Cybersecurity Regulatory Developments in Greece - Key Updates of the Implementation of the NIS2 Directive

BY IRENE KYRIAKIDES, VICTORIA MERTIKOPOULOU, NATALIA SOULIA, VASILIKI ANGELOPOULOU, EVGENIA CHATZISTRATI

Introduction

Recent regulatory and policy developments in Greece reinforce the national cybersecurity governance framework following the transposition of Directive (EU) 2022/2555 (NIS2) through Law 5160/2024. Below we summarize the most significant recent initiatives introduced by the Hellenic Cybersecurity Authority (NCSA), which are of particular relevance to essential and important entities, as well as to organisations operating in critical sectors.

NIS2 Gap Analysis Tool

With regard to cybersecurity obligations imposed on entities under Law 5160/2024 as well as Ministerial Decision 1689/2025, in mid-September the NSCA published a dedicated Gap Analysis Tool, developed in cooperation with the European Union Agency for Cybersecurity (ENISA).

The tool is designed as a comprehensive assessment framework enabling essential and important entities to systematically evaluate their level of compliance with the applicable regulatory requirements.

As emphasized by the NSCA, the systematic use of the Gap Analysis Tool should be viewed not merely as a compliance exercise, but as a strategic investment in operational continuity, digital resilience, and corporate governance.

Mandatory Use of Multi-Factor Authentication (MFA) for Microsoft Entra ID

The NSCA mandates the immediate activation and enforcement of Multi-Factor Authentication (MFA) for all Microsoft Entra ID users.

MFA significantly reduces the risk of unauthorized access, as the majority of cybersecurity incidents originate from password theft or compromise.

Launch of Significant Incident Notification Mechanism

The NSCA has launched a new mechanism for the submission of cybersecurity incident notifications.

Essential and Important entities are required to notify the CSIRT of the NSCA, without undue delay, of any incident having a significant impact on the provision of their services. To support this obligation, NSCA has introduced two standardized submission forms:

- The Simple Submission Form, to be used for the early warning notification within 24 hours of becoming aware of a significant incident. This form may also be used voluntarily by any organization in Greece to report cyber threats or near-miss incidents.
- The Detailed Submission Form, to be used for the 72-hour incident notification, for intermediate updates upon request by

NSCA, and for the final report, which must be submitted within one month of the incident notification. This form may also be used voluntarily by any organization to report actual cybersecurity incidents.

All incident notifications must be submitted via email to incident@cyber.gov.gr.

Publication of the National Cybersecurity Strategy 2026–2030

The NSCA has published the National Cybersecurity Strategy 2026-2030, Greece's comprehensive policy framework for addressing cyber threats and strengthening national digital resilience over the next five years. The Strategy was formally approved in December 2025 by the Ministry of Digital Governance and establishes the country's overarching roadmap for cybersecurity governance, prevention, preparedness, and response.

Launch of the Web-Based Cybersecurity Self-Assessment Tool

The NSCA has launched a web-based version of its Cybersecurity Self-Assessment Tool for organisations.

The tool is designed to support organisations in evaluating their overall cybersecurity posture, identifying weaknesses, and improving their level of preparedness against cyber threats. It comprises a total of 234 control points, structured across 19 thematic areas, and is designed to assist organizations in identifying gaps, strengthening cybersecurity controls, and enhancing their overall cybersecurity maturity.

It is primarily addressed to medium- and large-sized organizations in both the public and private sectors that constitute essential and important entities for Greece.

Conclusion

Taken together, these initiatives demonstrate the continued consolidation of Greece's cybersecurity governance framework under NIS2 with emphasis on proactive risk management, enhanced supervisory mechanisms, and increased accountability of management bodies.

Organisations falling within the scope of Law 5160/2024 are encouraged to closely monitor these developments and integrate the relevant tools and controls into their internal governance and compliance frameworks.

Early alignment with these initiatives is expected to play a key role in mitigating regulatory risk and strengthening long-term operational resilience.

Contact Us

Irene Kyriakides
PARTNER
i.kyriakides@kglawfirm.gr

Victoria Mertikopoulou
PARTNER
v.mertikopoulou@kglawfirm.gr

Natalia Soulia
COUNSEL
n.soulia@kglawfirm.gr

Follow Us

ATHENS OFFICE

28, Dimitriou Soutsou Str.,
115 21 Athens

T +30 210 817 1500
E kg.law@kglawfirm.gr

THESSALONIKI OFFICE

31, Politechniou Str.,
551 34 Thessaloniki

T +30 2310 441 552
E kg.law@kglawfirm.gr

www.kglawfirm.gr