
CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2026

Definitive global law guides offering
comparative analysis from top-ranked lawyers

**Greece: Law and Practice
& Trends and Developments**

Orfeas Mavredakis and Evangelos Katsaras
ALG Manousakis Law Firm



GREECE



Law and Practice

Contributed by:

Orfeas Mavredakis and Evangelos Katsaras
ALG Manousakis Law Firm

Contents

1. General Overview of Laws and Regulators p.4

- 1.1 Cybersecurity Regulation Strategy p.4
- 1.2 Cybersecurity Laws p.4
- 1.3 Cybersecurity Regulators p.5

2. Critical Infrastructure Cybersecurity Regulation p.6

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.6
- 2.2 Critical Infrastructure Cybersecurity Requirements p.6
- 2.3 Incident Response and Notification Obligations p.7
- 2.4 State Responsibilities and Obligations p.8

3. Operational Resilience in the Financial Sector p.9

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.9
- 3.2 ICT Service Provider Contractual Requirements p.10
- 3.3 Key Operational Resilience Obligations p.11
- 3.4 Operational Resilience Enforcement p.12
- 3.5 International Data Transfers p.13
- 3.6 Threat-Led Penetration Testing p.14

4. Cyber-Resilience p.15

- 4.1 Cyber-Resilience Legislation p.15
- 4.2 Key Obligations Under Legislation p.16

5. Security Certification for ICT Products, Services and Processes p.17

- 5.1 Key Cybersecurity Certification Legislation p.17

6. Cybersecurity in Other Regulations p.17

- 6.1 Cybersecurity and Data Protection p.17
- 6.2 Cybersecurity and AI p.18
- 6.3 Cybersecurity in the Healthcare Sector p.20

Contributed by: Orfeas Mavredakis and Evangelos Katsaras, **ALG Manousakis Law Firm**

ALG Manousakis Law Firm was established in 2011 by Ioannis and Alexandros Manousakis. Based in Athens, ALG is an international law firm with lawyers qualified in six EU jurisdictions and Switzerland. The firm's team consists of 50 lawyers and 25 paralegals. With deep expertise in corporate and commercial law, it offers tailored solutions across various indus-

tries. Its client base includes 30 pharmaceutical/biotech and five medical device companies. The firm supports them in contracting negotiations, ensuring compliance, and developing robust data privacy frameworks. The firm has a high rate of success, especially in commercial claims, tax and administrative litigation in general.

Authors



Orfeas Mavredakis is an associate at ALG Manousakis Law Firm. He is a Greek-qualified lawyer. His practice focuses on data protection and privacy law, as well as public, civil and medical law. He advises clients

on compliance with the General Data Protection Regulation, represents clients before the Hellenic Data Protection Authority and provides support in data protection-related training initiatives. He also advises on public tenders, administrative procedures and litigation, and assists organisations with contract drafting and regulatory compliance. He holds a postgraduate degree in Law and Information and Communication Technologies from the University of Piraeus.



Evangelos Katsaras is a junior partner at ALG Manousakis Law Firm. He is an EU-qualified attorney at law specialising in privacy, cybersecurity, and AI law, and an IAPP-accredited privacy professional. He holds a Law

and Technology LLM from Tilburg University and is currently a PhD candidate in Law at the National and Kapodistrian University of Athens. His practice focuses on the design and implementation of compliance programmes in the areas of privacy, cybersecurity, and AI, including audits, mapping, third-party risk management, and the development of policies and procedures. He regularly advises on management of cybersecurity incidents and privacy requests.

ALG Manousakis Law Firm

16 Laodikias Str.
Athens
11528
Greece

Tel: +30 210 723 2761
Email: info@alg.gr
Web: www.alg.gr



1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

Greece has established a modern, multi-layered cybersecurity framework that brings together national strategies, legislative measures, sector-specific regulations and directly applicable EU instruments. More specifically, the Greek legislature:

- defines clear national priorities in the National Cybersecurity Strategy 2026–2030, focusing on strengthening resilience, improving governance, enhancing public–private co-operation and developing national cybersecurity skills;
- creates a unified regulatory architecture through Law 5160/2024 (transposing the EU NIS2 Directive), which broadens the range of regulated sectors, sets minimum cybersecurity and incident-reporting requirements, and introduces explicit accountability obligations for top management;
- centralises oversight under the National Cybersecurity Authority (NCSA) as established by Law 5086/2024 – the NCSA acts as the national supervisory authority, issues binding requirements, co-ordinates cyber crisis response and serves as Greece’s EU Single Point of Contact;
- enhances the resilience of critical entities through Law 5236/2025 (transposing the EU CER Directive), extending protection beyond cyber threats to include physical and hybrid risks affecting essential services – this aligns cybersecurity measures with broader operational resilience standards across critical sectors; and
- integrates key EU regulations – including DORA, the Cyber Resilience Act (CRA), and the EU Cybersecurity Act – to ensure harmonised cybersecurity standards across financial services, digital products, ICT supply chains and certification frameworks.

Together, these elements form a cohesive, risk-based regulatory ecosystem that ensures a high and consistent level of cybersecurity across Greece’s critical and emerging sectors, supporting the country’s transition toward a secure and resilient digital future.

1.2 Cybersecurity Laws

Law 5160/2024, which transposes the NIS2 EU Directive, constitutes the core horizontal cybersecurity framework in Greece.

Subject Matter

- Establishes an enhanced framework for cybersecurity risk management, incident reporting, governance obligations, and supervisory/enforcement mechanisms.

Organisations in Scope

- Applies to essential and important entities across the sectors listed in Annexes I and II, including: energy, transport, digital infrastructure, public administration, health, finance, space, water, waste management, food, chemicals, and manufacturing.

Notable Points

- Introduces top-management accountability, stricter incident-reporting timelines, supply-chain security controls, and detailed asset-inventory obligations.
- Requires registration with the National Cybersecurity Authority (NCSA).

Greece has also issued multiple binding and quasi-binding secondary instruments to operationalise the new cybersecurity obligations. The most significant are Joint Ministerial Decisions (JMDs).

JMD 1689/2025 – National Cybersecurity Requirements Framework

This is the primary binding technical and organisational guidance implementing Law 5160/2024 (NIS2). It sets out concrete controls, including:

- cybersecurity policies and procedures;
- risk assessments;
- penetration testing;
- vulnerability management;
- supply-chain security requirements;
- encryption and access control;
- staff training obligations;
- mandatory appointment of a Security/ICS Officer; and
- comprehensive asset inventories.

JMD 1990/2025 – Registration and Data Submission to NCSA

- Governs how entities must register and submit data to the NCSA under Law 5160/2024.

JMD 1899/2025 – Appointment and Duties of the Information and Communication Systems Security Officer (ICSSO)

This JMD details the qualifications and responsibilities of the ICSSO required by Law 5160/2024 and JMD 1689/2025. It establishes:

- ICSSO eligibility and qualification criteria;
- conflict-of-interest rules (eg, ICSSO cannot also serve as DPO or Head of IT);
- integrity and background-check requirements; and
- detailed ICSSO operational responsibilities covering oversight of security, policies, controls, and reporting.

The national framework is complemented by directly applicable EU regulations.

A. Digital Operational Resilience Act (DORA) – Regulation (EU) 2022/2554

Subject matter

- Establishes uniform EU-wide rules on ICT risk management, incident reporting, digital operational-resilience testing, governance, and ICT third-party risk oversight for the financial sector.

Organisations in scope

- Applies to banks, investment firms, insurers, payment institutions, CCPs, CSDs, crypto-asset service providers, and ICT service providers supporting financial entities.

Notable points

- Is directly applicable in Greece and prevails over NIS2 obligations where both frameworks apply.
- Establishes the oversight framework for critical ICT providers, such as cloud service providers.

B. Cyber Resilience Act (CRA) – Regulation (EU) 2024/2847

Subject matter

- Imposes security-by-design and vulnerability-management obligations for digital products and software, covering secure development, life cycle management, patching, and co-ordinated vulnerability disclosure.

Organisations in scope

- Applies to manufacturers, developers, importers, and distributors of digital products placed on the EU market.

Notable points

- Complements NIS2 by regulating product-level security, while NIS2 focuses on service-level resilience.
- Introduces conformity assessment, technical-documentation requirements, and CE marking obligations.

1.3 Cybersecurity Regulators

The NCSA is Greece's central cybersecurity authority, established under Law 5086/2024. It is responsible for developing the national cybersecurity strategy, supervising NIS2 obligations, setting technical cybersecurity requirements, and co-ordinating national cyber incident response.

In addition to supervising covered entities, the NCSA serves a co-ordinating and regulatory role. It can issue mandatory cybersecurity requirements and publish guidelines for both essential and important entities.

The NCSA also operates Greece's National Computer Security Incident Response Team (CSIRT) and acts as the country's cyber crisis management authority. It serves as Greece's single point of contact at the EU level for cybersecurity co-operation networks, such as the CSIRTs Network.

Finally, the NCSA is responsible for conducting compliance checks, issuing binding orders to address identified deficiencies, and imposing administrative penalties where necessary.

2. Critical Infrastructure Cybersecurity Regulation

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

Pursuant to Law 5160/2024, entities classified as “essential” or “important” are required to implement specific cybersecurity risk-management measures, incident-reporting obligations, governance processes, and to comply with supervisory and enforcement mechanisms.

The criteria used to classify entities into these two categories are based on the nature and sector of their activity as well as their size. The sectors covered by the regulatory framework include:

- energy;
- transport;
- banking;
- financial markets;
- health;
- drinking water and wastewater management; and
- digital infrastructure.

The framework also encompasses digital providers such as online marketplaces, search engines, and social networking services.

In addition, Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) fall within the scope of Law 5160/2024 when they provide ICT or security services on a large scale and are considered part of the digital infrastructure or ICT services category. This effectively extends compliance requirements across the broader services market.

Law 5160/2024 applies to all medium-sized or large organisations within the above sectors (indicatively, those with more than 50 employees or turnover exceeding EUR10 million). Smaller entities may also be included when they are the sole providers of an essential service or when the disruption of their operations is considered to have a significant social impact.

Furthermore, public administrations that provide critical public services or state functions are explicitly covered – even if they do not meet the size criteria

– with the aim of protecting critical government information systems.

However, several aspects of the law remain open to interpretation or are still awaiting further guidance.

- Definition of “digital infrastructure” – although the law applies to digital infrastructure providers, it does not clearly define which modern digital services qualify as infrastructure as opposed to “online services” or “digital platforms”.
- The “significant impact” exception – neither NIS2 nor Law 5160/2024 sets quantitative thresholds for determining what constitutes a “significant impact”.
- Scope of managed service providers – the law does not clarify which MSP business models are automatically included within its scope.

2.2 Critical Infrastructure Cybersecurity Requirements

Law 5160/2024 establishes requirements for implementing appropriate technical and organisational measures to manage cybersecurity risks. These obligations are further specified in Greece’s National Cybersecurity Requirements Framework, set out in JMD 1689/2025, which provides a detailed checklist for essential and important entities. The main areas of focus are as follows.

Governance and Accountability

A cyber governance plan is required, ensuring that risk oversight is carried out at senior management level and that specific responsible officers are appointed. Notably, organisations must designate an Information and Communications Systems Security Officer (ICSSO – equivalent to a CISO) by name, who must also report to the NCSA. Senior management bears responsibility for compliance, as the legislation explicitly holds CEOs and directors accountable if they fail to ensure adequate measures or proper incident handling. Organisations must maintain an information security policy covering the entire organisation, supported by individual policies, with clearly defined roles and responsibilities. Regular updates to senior management are required, along with submission of an annual cybersecurity report to the NCSA.

Risk Assessment and Asset Management

Organisations must maintain an up-to-date inventory of assets (hardware, software, data and network assets), prioritised according to criticality and risk. Periodic risk assessments must identify threats and vulnerabilities affecting critical processes, applying controls based on a recognised risk management methodology (often aligned with ISO 27005 or similar standards). These assessments must also address supply-chain risks, including those associated with suppliers and service providers.

Basic Technical and Organisational Measures

The National Framework outlines a set of core measures aligned with international best practices. These measures include the following.

- Access controls and identity management – ensuring system access only for authorised users.
- Asset and configuration security – implementing secure configurations, maintaining current software versions, and applying network security controls, including continuous monitoring of network traffic and logs for anomalies.
- Vulnerability management and code updates – establishing procedures for timely remediation of vulnerabilities and co-ordinated vulnerability disclosure.
- Training and awareness – conducting regular security training and awareness activities.

Incident Detection, Response and Recovery

Organisations must maintain an incident response plan with procedures for incident classification, containment, eradication, recovery and reporting – both internally and to the authorities. Periodic testing of these procedures is required.

Business Continuity and Disaster Recovery (BCP/DR)

BCP/DR planning and testing must be carried out to ensure that key services can be maintained or quickly restored following a cyber disruption. Requirements include backup policies and regular recovery testing, particularly to protect against ransomware and data corruption.

Third-Party Due Diligence and Management

Organisations must ensure that third-party contracts include appropriate cybersecurity controls and clauses, such as security obligations, audit rights or independent assessment reports, breach notification requirements, and data-location provisions when applicable. There is also an obligation to oversee sub-contractors, maintain an exit strategy (including data portability, relocation support and transition periods), and manage concentration risks, supported by contingency plans for the failure of a critical supplier.

The National Framework effectively transforms established best practices into mandatory requirements. Compliance is monitored through submissions and audits, and non-compliance may result in enforcement actions, such as fines or corrective orders.

2.3 Incident Response and Notification Obligations

The established incident response and reporting obligations aim to ensure the timely management of incidents and the proper notification of authorities.

Under Law 5160/2024, an incident must be reported if it is classified as a “significant incident”. This includes any security incident that has, or could have, a substantial impact on the provision of an operator’s services or that affects other individuals or entities, causing significant material or non-material damage. In practice, the assessment considers factors such as the number of users affected, the duration of the disruption, the geographical spread, and the severity of the impact (including financial losses or risks to life or health). At EU level, quantitative thresholds have been set (for example, incidents affecting more than 100,000 users or lasting several hours may automatically qualify as significant), and Greece follows these criteria as established in the Commission’s implementing regulation on incident reporting.

The incident reporting process takes place in stages.

- Within 24 hours of becoming aware that a significant incident has occurred, the entity must submit an initial notification (“early warning”) to the authorities. This notification must be provided even if full details are not yet known, as its purpose is to alert

the NCSA (and potentially the EU CSIRT Network) promptly.

- Within 72 hours, the entity must submit a more detailed incident report. This report should include an initial assessment of the nature of the incident, its severity and observable impact, and whether the incident appears to be under control or ongoing. The NCSA may also request interim updates or additional information as the situation develops, and Law 5160/2024 allows it to require progress reports while the incident is being resolved.
- No later than one month after the initial notification, the entity must submit a final report to the NCSA. This report should include a comprehensive analysis of the incident, its root cause, the full extent of its impact, and the remedial measures taken. If the incident is still ongoing after one month, additional progress reports may be required beyond this deadline.

Failure to comply with reporting deadlines may itself lead to penalties, as timely reporting is a legal obligation.

All notifications are submitted to the NCSA's National CSIRT, but relevant sectoral authorities may also be involved.

- Public administration and national security sectors: incidents require co-ordination with the government CSIRT. Law 5160/2024 requires public sector entities to notify the Cyber Security Incident Response Team of the National Intelligence Service (EYP), alongside simultaneous notification to the NCSA.
- Telecommunications sector: significant incidents must be reported both to ADAE and the NCSA. ADAE then shares relevant information with the NCSA and EETT as needed.
- Financial sector: under DORA, institutions report significant ICT incidents to their financial regulator (the Bank of Greece or the Hellenic Capital Market Commission). If the incident also falls under NIS2, these regulators are expected to co-ordinate with the NCSA. The Greek framework (via Law 5236/2025 and cross-sector Memoranda of Cooperation) seeks to avoid duplicate reporting – for example, a bank may report to the Bank of Greece,

which then informs the NCSA, or vice versa – although this mechanism is still maturing.

Certain incidents trigger multiple regulatory notifications. For example, a personal data breach in a hospital qualifies both as a NIS2 incident and a GDPR breach. In such cases, the hospital must notify the NCSA (under NIS2) and the Greek Data Protection Authority within 72 hours (under the GDPR). As there is currently no one-stop-shop mechanism, organisations must comply with each law's separate procedure.

The Greek authorities encourage reporting streamlining to prevent multiple entities from reporting the same incident separately. For instance, if a telecommunications provider submits a report to ADAE, ADAE forwards it to the NCSA so the provider does not need to report twice (supported by a Memorandum of Cooperation between ADAE and the NCSA). Similarly, at the European level, the NCSA – acting as the national single point of contact – shares information with the EU CSIRT Network and, for large-scale incidents, with the European Cyber Crisis Liaison Organisation Network (EU-CyCLONE). Entities do not need to report directly to EU bodies, although they may be asked for further details via the NCSA.

Early warnings are used for immediate alerts and support and are treated as confidential. The NCSA must protect the security, commercial interests, and confidentiality of the information, though it may issue anonymised warnings to other entities. The final report and interim updates form part of the formal post-incident obligations, and the NCSA may request a corrective action plan, follow-up meeting, or audit. Beyond regulatory notifications, entities may also be required to inform service recipients/users if service provision is affected, and the NCSA may issue public notices where necessary to mitigate risks or protect the public interest.

2.4 State Responsibilities and Obligations

The state, through the NCSA, develops the National Cybersecurity Strategy, which outlines the protection of critical sectors, skills development, and investment in secure technologies. The strategy is reviewed every five years, while progress is assessed every two years,

with ENISA support available when required. In parallel, the state establishes the regulatory framework and, through the NCSA, issues binding technical and organisational requirements as well as guidelines. The NCSA also serves as the National Cybersecurity Certification Authority under the EU Cybersecurity Act, overseeing the implementation of certification schemes for ICT services.

The state is responsible for maintaining national prevention, detection, and response capabilities. The NCSA hosts the national CSIRT, and in cases of large-scale incidents, national cyber crisis management procedures and European co-ordination mechanisms (eg, EU-CyCLONE) are activated. In the area of Cyber Threat Intelligence (CTI), the framework encourages and protects the voluntary exchange of information – such as indicators of compromise, vulnerabilities, and incidents – and supports the establishment of Information Sharing and Analysis Center (ISAC) structures. The NCSA facilitates information exchange, issues anonymous warnings to the market when necessary, and participates in EU-level networks (such as the EU CSIRT Network) and international collaborations.

The strategy adopts a public–private partnership model. The state seeks co-operation with the private sector by forming sectoral working groups or ISACs in areas including finance, energy, and telecommunications. It regularly convenes critical infrastructure operators in dedicated forums to discuss emerging threats and jointly develop mitigation measures. Furthermore, the state invests in capacity building and operates a National Coordination Centre within the EU cybersecurity capabilities network (Regulation (EU) 2021/887). Financial incentives for cybersecurity investments and certifications are also under consideration.

In serious cases, the state may mobilise additional resources, including technical assistance from NCSA experts, and involve law enforcement authorities to provide investigative support. Similarly, the development of sectoral ISACs highlights the state’s role as convenor and the industry’s role as the primary channel for day-to-day information exchange.

In summary, the Greek state plays the roles of organiser, regulator, information provider, and supporter in

the field of cybersecurity. It sets strategic direction and regulatory requirements (so private entities understand their obligations), ensures national response capabilities (so the state can intervene during major threats), actively shares threat information (so no organisation confronts risks alone), and builds strong connections with the private sector and international partners (because cybersecurity resilience is a collective effort).

3. Operational Resilience in the Financial Sector

3.1 Scope of Financial Sector Operational Resilience Regulation

DORA applies directly in Greece without requiring national transposition and serves as the primary operational resilience framework for financial entities and critical ICT third-party providers. The following organisations fall within the scope of DORA.

A broad range of financial sector entities, including:

- credit institutions, payment institutions and e-money institutions;
- investment firms, insurers and reinsurers;
- central securities depositories (CSDs), CCPs and trading venues;
- crypto-asset service providers (CASPs); and
- pension funds, credit rating agencies and trade repositories.

Critical Third-Party ICT Providers, meaning ICT service providers that deliver critical or important services to financial institutions, such as:

- cloud computing service providers;
- data analytics or software providers; and
- other ICT outsourcing firms.

DORA is structured around five core operational pillars:

1. ICT Risk Management Requirements

- Asset identification, protection and detection measures, as well as incident response, recovery and backup policies.

2. ICT Incident Reporting Rules

- Classification of ICT incidents and mandatory reporting of major incidents.

3. Digital Operational Resilience Testing

- Regular scenario-based testing and Threat-Led Penetration Testing (TLPT).

4. ICT Third-Party Risk Management

- Contractual obligations, oversight requirements, concentration-risk assessment and exit strategies.

5. Oversight of Critical Third-Party ICT Providers

- ESA-level monitoring and supervisory powers over designated critical ICT providers.

DORA also has significant extraterritorial reach, covering the following.

- Financial entities operating in Greece but headquartered elsewhere – if an institution provides regulated services in any EU Member State, including Greece, DORA applies regardless of where its headquarters are located.
- Non-EU ICT third-party providers serving Greek financial institutions – at the national level, Greece has complemented DORA with Law 5193/2025, which assigns supervisory and enforcement powers. The Bank of Greece supervises banks, insurance companies and payment providers, while the Hellenic Capital Market Commission oversees investment firms, fund managers and related entities. These authorities have the power to impose administrative fines of up to 10% of turnover, in accordance with national law.

3.2 ICT Service Provider Contractual Requirements

DORA defines ICT services as encompassing “a broad range of offerings, extending beyond traditional out-

sourced IT services”. This includes third-party service providers, cloud and software vendors, and fintech providers. Under DORA, entities qualify as ICT service providers when they supply any of the following to financial institutions:

- digital or data services;
- data processing;
- software;
- data centre services;
- cloud computing services; or
- any outsourced ICT-related function.

ICT service providers may be designated as critical based on several criteria:

- the provider’s systemic importance;
- the scale and complexity of services offered to the financial sector;
- the potential impact on the stability, continuity, and quality of financial services in the event of disruption; and
- the degree of concentration within the provider’s market segment.

This designation is carried out by the European Supervisory Authorities (ESAs), not by national authorities.

Financial institutions must embed binding contractual and supervisory requirements into their agreements with all ICT service providers. In particular, contracts must address the following areas.

Full description of services:

A clear and comprehensive description of all services and the provider’s obligations.

Subcontracting:

Explicit provisions governing subcontracting, including notification and approval requirements, as well as the obligation to ensure that subcontractors receive equivalent security, control, and co-operation commitments (“chain outsourcing”).

Data location:

Specification of the countries or regions where services are delivered and data are stored, along with an obligation to provide prior notice – and, where required, obtain consent – for any changes.

Security and confidentiality:

Clauses describing ICT security and confidentiality measures, including resilience and business continuity plans, as well as the provider's obligation to support the financial institution in meeting its regulatory requirements.

Incident notification:

An obligation for the provider to immediately inform the financial institution of any circumstances that may have an impact on it, and to fully co-operate with both the institution and relevant supervisory authorities.

Control:

Clear service-level targets and monitoring procedures, allowing the institution to maintain active oversight and undertake timely corrective actions.

Audit:

Rights for on-site inspections by both the financial institution and competent supervisory authorities (and, for critical ICT third-party providers, by the designated lead supervisor).

Exit strategy:

Clauses ensuring that, in cases of termination, cancellation, insolvency, or cessation of activity, data remains accessible and is returned in a usable format, accompanied by transition support and secure deletion once the process is complete.

Termination options:

Defined conditions and notice periods, including the option to terminate the arrangement when requested

by a supervisory authority or when the provider's risk profile becomes unacceptable.

Concentration risks:

Requirements for institutions to assess concentration risks and third-country or jurisdictional risks, particularly where local regulations may hinder access or control.

Through Law 5193/2025, these obligations become enforceable by the Bank of Greece or the Hellenic Capital Market Commission. Institutions are expected to review existing significant contracts, and authorities may impose corrective measures where necessary.

3.3 Key Operational Resilience Obligations

DORA sets out obligations for governance, risk management, incident management, and incident reporting.

Governance (Tone From the Top and Accountability)

Financial entities must ensure clear management body accountability for ICT risk. This includes the responsibility to approve and oversee the ICT risk management framework, allocate appropriate roles, resources, and expertise, and ensure directors receive adequate training.

Policies and controls must cover all phases of the ICT risk life cycle: identification, protection, detection, response, recovery, and backup/restore, along with periodic review and board-level reporting.

ICT Risk Management (End-to-End)

Organisations must maintain comprehensive asset and dependency mapping, including business services, ICT assets, and third-party dependencies.

They must establish and maintain controls for protection, prevention, and detection of ICT risks.

Business continuity and disaster recovery (BCP/DRP) plans must be in place, regularly tested, and reviewed for lessons learned.

Third-party risk management (TPRM) requirements include:

- a TPRM strategy;
- risk assessments;
- a register of all third-party arrangements; and
- contractual clauses covering access, audit and information rights, sub-outsourcing, exit, and data reversibility.

Incident Management and Reporting

Entities must maintain an end-to-end incident management process covering detection, triage, containment, eradication, recovery, and post-incident review.

Incidents must be classified using defined criteria such as service downtime, number and criticality of users affected, data loss, geographic spread, economic impact, and other material indicators.

DORA delegates specific thresholds and evidence requirements to the Regulatory Technical Standards (RTS). Classification of an incident as “major” is based primarily on its scale and criticality – for example, disruption to critical services, high user impact, long duration, significant data loss, or systemic implications. Materiality is assessed based on factors such as:

- impact on critical functions;
- number of affected customers or users and extent of disruption;
- duration and severity of availability degradation;
- geographical spread;
- impact on the confidentiality, integrity, or availability of data;
- operational or financial damage; and
- potential systemic or chain-reaction effects.

Reporting Timelines

Major ICT-related incidents must be reported to the competent financial authority (Bank of Greece or HCMC). Reporting follows a staged model.

- Initial notification – within 4 hours of classification as “major”, and no later than 24 hours after detection.

- Interim report – within 72 hours of the initial notification.
- Final report – within one month of the interim report, providing full root-cause analysis and corrective measures.

Additional updates are required when the situation materially changes or when requested by the authority.

The reports must enable supervisors to understand what happened, the areas affected, and how the incident is being managed. Initial notifications should provide essential information, followed by more detailed impact assessments and status updates, and finally a comprehensive root-cause analysis, damage assessment, remediation plan, and preventive actions.

Third-Party Providers and Cross-Regime Considerations

DORA brings third-party ICT providers into the same operational framework. If an incident occurs at an ICT provider (eg, cloud or outsourcing provider), the financial entity must report it as its own major incident and co-ordinate with the provider based on contractual obligations for co-operation and information sharing.

Providers designated as CTPPs (Critical Third-Party Providers) fall under a dedicated EU-level oversight regime. This does not limit national obligations for Greek financial institutions regarding TPRM, testing, and full incident reporting.

Financial entities may also report significant cyber threats, even before they develop into incidents, and may participate in threat-information-sharing arrangements consistent with the framework’s safeguards.

For entities also subject to NIS2, DORA incident reporting to financial sector supervisors exists alongside NIS2 reporting obligations to the NCSA.

3.4 Operational Resilience Enforcement

DORA establishes a new EU-level oversight framework under which designated ICT providers (eg, cloud service providers, software vendors) are subject to direct supervisory monitoring by the European Supervisory Authorities (ESAs – EBA, ESMA and EIOPA). At

the same time, national supervisors (such as the Bank of Greece) continue to supervise financial entities that rely on those ICT services.

Once an ICT provider is designated as critical, the ESAs may exercise the following powers.

Information and Access Powers

- Request any information relevant to operational resilience.
- Access, inspect, and audit ICT systems, premises, and security processes.
- Interview staff and request incident reports, test results, or any other relevant documentation.

On-Site Inspections

- Conduct planned or unannounced on-site inspections.
- Examine configuration settings, logging practices, security controls, resilience measures, and subcontracting arrangements.

Oversight Recommendations and Binding Instructions

- Issue remediation recommendations.
- Impose mandatory corrective actions.
- Require improvements to risk management, incident handling, or resilience testing frameworks.

Testing and Validation Requirements

- Require participation in threat-led penetration testing (TLPT).
- Request evidence of resilience controls, backup capabilities, and incident detection mechanisms.

Sanctioning Powers

- Supervisory (non-financial) measures:
 - (a) Compliance orders
 - (b) Public statements
 - (c) Suspensions or restrictions of activities
 - (d) Penalties for natural persons or officials
- Financial penalties:
 - (a) Recurring penalty payments until compliance is achieved
- Fines for violations of oversight requirements (up to 10% of annual turnover or EUR5 million for serious infringements)

Although DORA introduces a central EU-level supervisory regime for critical third-party providers (CTPPs) through the ESAs acting as Lead Overseers, national authorities continue to enforce requirements on providers indirectly. This is achieved through mandatory obligations imposed on financial entities – such as contractual clauses, oversight mechanisms, auditing and testing obligations, and exit strategies. National supervisors may also require institutions to modify or terminate outsourcing arrangements if the associated risk is deemed unacceptable.

The Bank of Greece conducts supervision via both off-site monitoring (submitted data reports, incident reporting, information on critical assignments, and testing results) and on-site audits focused on ICT risk and resilience. Audits typically examine:

- governance structures;
- policies and procedures;
- technical evidence (logs, monitoring data, security controls, test results); and
- third-party risk management practices (assignment registers, risk assessments, SLAs, audit/inspection rights, provider participation in testing, data exit and portability plans).

Greek authorities may require a financial entity to mitigate third-party risks or, if risks remain unacceptably high, to suspend or terminate a critical outsourcing arrangement.

3.5 International Data Transfers

The operational resilience rules for the financial sector in Greece operate alongside European data transfer law and the supervisory requirements that apply to outsourcing in third countries. Although these rules do not impose a general obligation to localise data, in practice financial entities must select providers that do not impede supervision, allow effective control and access, and ensure that international data transfers remain lawful.

At the DORA level, the key issue is not a “prohibition” on data transfer but the need for transparency and control. Contracts with ICT providers must clearly specify the locations (regions/countries) where services are delivered and where data is processed or

stored, as well as the conditions under which these locations may change. This transparency enables both the financial entity and competent authorities to assess the risks associated with different jurisdictions.

In parallel, supervisory expectations for outsourcing require that both the financial entity and the competent authorities retain full access, inspection, and audit rights. They also require that risks arising from third-country involvement be specifically assessed. The EBA Guidelines on Outsourcing address these requirements explicitly, covering both access/control obligations and risk management considerations related to third-country arrangements.

From a data protection perspective, Greece operates fully within the EU's GDPR framework. When personal data is transferred outside the EEA, the transfer must rely on an appropriate GDPR mechanism. Following Schrems II, organisations must evaluate whether the chosen transfer tool functions effectively in practice and, where necessary, adopt additional technical and organisational measures in line with the EDPB's guidance on "supplementary measures".

In practice, the combined effect of DORA, GDPR, and supervisory obligations often leads organisations to adopt operational strategies that resemble a form of soft data localisation. This typically results in a preference for EU/EEA data regions, the use of technical measures that ensure encryption keys remain within the EU, and contingency planning that allows critical functions to continue or be recovered without reliance on a third country that poses regulatory or operational difficulties.

3.6 Threat-Led Penetration Testing

Greece does not maintain its own national threat-led penetration testing (TLPT) framework. Instead, TLPT obligations for Greek entities stem directly from DORA and the TIBER-EU Framework, which functions as the official methodology for conducting TLPT under DORA.

DORA TLPT adopts the TIBER-EU intelligence-led methodology.

Threat Intelligence (TI) Requirements

- TI must reflect real threat actors targeting an entity's critical or important functions (CIFs).
- Under TIBER-EU, tests must simulate the tactics, techniques, and procedures (TTPs) of advanced real-world attackers.

Scenario Selection

- Scenarios must be based on bespoke, entity-specific TI.
- They must focus on CIFs and vulnerabilities across systems, processes, and people.
- The DORA TLPT RTS aligns closely with TIBER-EU scenario design requirements.

Mandatory Documentation Timeline

Following notification by supervisory authorities:

Within 3 months:

Submit initiation documents (project plan, control team lead details, communication plan).

Within 6 months:

Submit the detailed Scope Specification Document (CIFs, systems, test flags).

Red Team Testers (RTTs) Requirements

RTTs must:

- be independent from the entity's operations;
- meet strengthened competence and ethical requirements introduced under TIBER-EU (2025 update); and
- demonstrate experience in advanced threat-simulation techniques.

Threat Intelligence Providers (TIPs) Requirements

TIPs must:

- produce high-quality bespoke TI reports;
- meet strict selection criteria aligned with the updated TIBER-EU rules; and
- be subject to supervisory restrictions if they lack sufficient qualifications.

Cross-Jurisdictional Recognition

The TIBER-EU framework is explicitly designed to avoid duplication where multiple EU jurisdictions require TLPT. A TIBER-EU test conducted in any EU member state can satisfy DORA TLPT requirements, provided the entity also meets the formal TLPT obligations set by its competent authority.

Entities Subject to Mandatory TLPT Under DORA

Only “significant” financial entities fall under DORA’s mandatory TLPT requirement. These are defined by impact, risk, and systemic-relevance criteria set out in the RTS. Examples include:

- significant banks;
- insurance undertakings;
- systemically important payment and e-money institutions; and
- CCPs, CSDs, and major trading venues.

Indicative (non-exhaustive) thresholds include:

- banks with total assets exceeding EUR30 billion;
- institutions with very large customer bases or transaction volumes; and
- entities operating across at least five EU member states.

Frequency of TLPT Under DORA

TLPT must be carried out at least once every three years. Supervisors may mandate more frequent testing based on identified risk.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

There is currently no autonomous, unified Greek “cyber-resilience law” that horizontally covers all ICT products and services. Instead, Greece follows a multi-layered cybersecurity and cyber-resilience framework aligned with EU legislation. This framework combines the following.

- NIS2 (Law 5160/2024) – establishes horizontal cybersecurity obligations for essential and important entities, including governance, risk management, and incident reporting requirements.

- DORA (Reg. 2022/2554) – Defines digital operational resilience obligations for financial entities, covering ICT risk management, incident response, and threat-led penetration testing (TLPT).
- CRA (Reg. 2024/2847) – Introduces product-based security-by-design requirements for ICT products and connected devices.
- EU Cybersecurity Act – Provides voluntary and mandatory certification schemes for ICT products and cloud services.

The core product-focused obligations now derive from the Cyber Resilience Act (CRA), which is already in force and will be fully applicable from 11 December 2027, with some requirements taking effect earlier. NIS2 (Law 5160/2024) and DORA complement the CRA.

- NIS2 imposes horizontal cybersecurity duties across sectors, including digital infrastructure and managed service providers.
- DORA imposes operational resilience requirements specifically for financial entities.

Together, these frameworks cover most risks arising in cloud and SaaS environments, even when a service does not strictly qualify as a “product” under the CRA.

The CRA applies to any hardware or software product with digital components (PDE), and its scope is intentionally broad. It includes:

- IoT and connected consumer products (any device that connects to a network, directly or indirectly);
- industrial controllers and embedded systems;
- networking equipment;
- operating systems and security software;
- standalone software; and
- cloud/SaaS components that support the functionality of a PDE.

In addition, the CRA introduces mandatory notification obligations for actively exploited vulnerabilities and for serious cybersecurity incidents, with strict reporting timelines.

4.2 Key Obligations Under Legislation

Pursuant to the CRA, manufacturers and distributors of PDE in Greece must comply with a set of baseline cybersecurity obligations designed to ensure product security throughout its life cycle. The key obligations for manufacturers are outlined below.

Vulnerability Management and Reporting Obligations

- Identify, document, and continuously monitor vulnerabilities in all software and hardware components.
- Design products with security by design and security by default principles, including eliminating default passwords, minimising attack surfaces, enforcing authentication and encryption, and ensuring security throughout the life cycle.
- Ensure the resilience of essential product functions even during cyberattacks (eg, DoS hardening, watchdog systems).
- Maintain and provide a complete Software Bill of Materials (SBOM) that tracks vulnerabilities in all components, including open-source elements.
- From 11 September 2026, report actively exploited vulnerabilities and severe cybersecurity incidents via the CRA Single Reporting Platform to the competent CSIRT:
 - (a) Within 24 hours: initial notification.
 - (b) Within 72 hours: update with available information.
 - (c) No later than 14 days after notification: final report including mitigation measures and corrective actions.

Patching and Update Obligations

- Provide free security updates without undue delay for the full duration of the declared support period (minimum expected product lifetime).
- Ensure ongoing life cycle support.

Post-Market Surveillance Obligations

Actively monitor PDEs after market release for:

- exploited vulnerabilities;
- security incidents; and
- weaknesses observed in deployment environments.

Documentation Duties

Maintain secure and up-to-date:

- development documentation;
- life cycle security evidence;
- vulnerability logs; and
- update histories, to support market surveillance activities and potential audits.

Co-operation With Authorities

Manufacturers, importers, and distributors must co-operate with market surveillance authorities – including those in Greece – by providing technical information and remediation plans when requested.

Conformity Assessments

- Classify their PDE based on the technical criteria outlined in Implementing Regulation (EU) 2025/2392 to determine whether it is a:
 - (a) standard product;
 - (b) important product (Class I or Class II); or
 - (c) critical product.
- Conduct self-assessments for non-critical products with lower cyber risk.
- Co-ordinate a notified-body assessment for critical products where cybersecurity failure could have significant systemic impact.
- Issue an EU Declaration of Conformity (DoC) confirming the PDE complies with CRA requirements.

Marking and Certification

- Apply the CE mark to CRA-compliant products before they are sold in Greece or any EU member state.
- Non-compliant products cannot be placed on the EU market beginning 11 December 2027.

Importers and distributors also have responsibilities: they must not make available products that clearly fail to meet the requirements, must co-operate in corrective actions, and must support traceability. Where non-compliance or serious risks are identified, corrective measures may include market withdrawal or recall, with mandatory co-operation and notification to the competent market surveillance authorities.

Enforcement

Enforcement will be carried out by national market surveillance authorities (Greece must designate its authority by 11 June 2026). These authorities may:

- request technical documentation;
- conduct checks; and
- impose corrective measures or restrict market placement.

Under the CRA, if PDEs fail to meet requirements, authorities may:

- order product recall or market withdrawal;
- prohibit placement on the EU market; and
- impose fines of up to EUR15 million or 2.5% of global revenue, whichever is higher.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

The EU Cybersecurity Act establishes an EU-wide cybersecurity certification framework for ICT products, services, and processes. Under this framework, Greece designates the National Cybersecurity Authority (NCSA) as the National Cybersecurity Certification Authority.

The European framework operates through certification schemes tailored to specific technology categories. A key example is the European Cybersecurity Certification Scheme on Common Criteria (EUCC), which consolidates Common Criteria certification at the European level for defined product categories. The EUCC has been in force since 27 February 2025, making it the most clearly active European scheme at the implementation level.

EU certification schemes may define three levels of assurance.

- Basic – fundamental requirements and controls, typically based on lighter assessment.
- Substantial – enhanced assessment offering greater security assurance.

- High – the most rigorous assessment, appropriate for particularly critical use cases.

Although the Cybersecurity Act originally envisioned these schemes as voluntary, in practice they can become effectively mandatory in three key ways.

- Public procurement – tenders may require compliance with a specific scheme or assurance level.
- Sectoral regulatory compliance – frameworks such as NIS 2 or DORA may promote certification as evidence of due diligence.
- Market access/CE-type logic – for certain “critical” product categories, certification may serve as proof of conformity or become necessary if mandated by secondary legislation.

In addition, some sectors operate under their own established certification schemes, including the following.

- Automotive – vehicle cybersecurity requirements are embedded in type-approval regulations, effectively serving as a prerequisite for market entry.
- Payments – standards such as PCI DSS and PCI PTS act as industry-mandated requirements for participation in the payment ecosystem.
- Identity solutions – historically, Common Criteria (and now EUCC) has played a major role in the certification of smart cards, secure elements, and digital identity systems, where High assurance is a prerequisite for trust and security.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

In Greece, cybersecurity and personal data protection are closely interconnected, as the security of personal data is both a legal compliance requirement and a fundamental cybersecurity objective. The core framework is the GDPR, together with the Greek implementing law 4624/2019, which impose preventive security measures as well as strict obligations for managing and reporting data breaches.

A key security obligation is that controllers and processors must implement “appropriate technical and

organisational measures” that are proportionate to the level of risk. In practical terms, this requires a risk-based approach: the more sensitive or critical the data, the stronger the expected safeguards. Although the GDPR does not prescribe specific security controls, demonstrating due diligence is often supported through recognised standards – such as ISO 27001 – though these are not legally mandatory. Alongside this, the GDPR embeds the principle of privacy by design and by default. This means that systems and processes handling personal data must be designed from the outset to incorporate secure defaults. In practice, any application or platform operating in Greece must collect only what is necessary, avoid exposing data through default settings, enforce role-based isolation, and integrate risk-reducing techniques wherever feasible.

In cases of personal data breaches, clear notification rules apply. Notification to the Hellenic Data Protection Authority (HDDPA) must be made “without undue delay and, where feasible, within 72 hours” whenever the breach is likely to pose a risk to the rights and freedoms of individuals. The notification should include, in a practical and well-documented manner:

- the nature of the breach;
- the categories and approximate number of individuals and records affected;
- the potential consequences for the individuals;
- the measures taken or planned to address and mitigate the breach; and
- the contact details of the controller, where required.

Notification to affected individuals is required only when the breach is likely to result in a high risk to their rights and freedoms, unless standard exceptions apply – for example, when individual notification would involve a disproportionate effort. This communication must be written in clear, accessible language and should focus on practical steps individuals can take to protect themselves, without unnecessary technical detail.

6.2 Cybersecurity and AI

In the Greek legal system, there is no standalone national “AI law” that horizontally regulates the security of AI systems. The primary framework is Regulation

(EU) 2024/1689 (the EU AI Act), published on 12 July 2024 and being implemented gradually. The main date of application is 2 August 2026, although some provisions take effect earlier (eg, from 2 February 2025).

At the core of the AI Act, cybersecurity obligations apply to high-risk AI systems, alongside requirements relating to governance, monitoring, transparency, and the reporting of serious incidents.

For high-risk AI systems, the AI Act requires providers or manufacturers to design and develop systems with an appropriate level of accuracy, robustness, and cybersecurity. In particular, they must ensure:

- protection against adversarial inputs;
- prevention of data poisoning;
- model and parameter integrity checks; and
- secure update and change-management mechanisms to prevent unauthorised “hidden” modifications.

A second layer concerns the security of the AI supply chain. Many AI systems incorporate pre-trained models, third-party libraries, and other external components. Regulatory expectations therefore emphasise documentation, traceability, and controls that mitigate the risks of backdoors, vulnerabilities, dependencies, and supply-chain attacks. This resembles a secure development life cycle, but adapted to the specific characteristics of machine learning (ML).

Furthermore, the AI Act requires notification of serious incidents to competent authorities. For high-risk systems, such reports must generally be submitted within 15 days of the provider or user (depending on the scenario) becoming aware of the incident. This may overlap with other regulatory reporting frameworks, meaning organisations need an operationally unified incident-management process capable of addressing multiple reporting obligations within the correct timeframes.

In practice, compliance in Greece will be multi-layered, because the AI Act does not replace general cybersecurity or data-protection frameworks – it complements them.

- If an AI system processes personal data, the GDPR continues to apply.
- If the organisation falls under regimes such as NIS2 (and/or DORA for the financial sector), an AI-related incident affecting availability, integrity, or confidentiality may simultaneously trigger obligations under those frameworks.

Thus, the AI Act adds the AI-specific layer: integrity of model behaviour, protection against ML-specific attacks, and reporting of serious incidents associated with AI-related risks.

Overall, the “cyber resilience” of AI systems in Greece will be assessed on three simultaneous levels:

- infrastructure and operational security (classical cybersecurity);
- personal data security (GDPR where applicable); and
- security and resilience of the AI model and its behaviour (AI Act).

Organisations that develop or use high-risk AI systems therefore need a documented risk assessment that addresses ML-specific threats, technical defence measures, and incident-reporting procedures covering all parallel regulatory obligations.

AI-Related Cybersecurity Obligations in Greece

AI-related cybersecurity requirements in Greece stem from a combination of national law and EU legislation. Primarily, the following are relevant.

Law 4961/2022 – Emerging Technologies Law (AI, IoT, Blockchain)

This national law established Greece’s earliest horizontal framework for AI governance. It includes obligations relating to responsible use, risk management, and data governance, applying across sectors. It also introduces risk-control requirements relevant to cybersecurity.

EU AI Act (Regulation 2024/1689)

Applicable directly in Greece, the AI Act imposes mandatory obligations on high-risk AI systems, including cybersecurity-specific requirements.

Under the EU AI Act, high-risk AI systems must include cybersecurity by design, encompassing:

Robustness, accuracy, and resilience

High-risk systems must be resilient to:

- adversarial attacks;
- data poisoning;
- model manipulation;
- model extraction; and
- malicious inputs or “hallucination attacks”.

Secure development life cycle requirements

The AI Act requires:

- secure coding practices;
- logging and monitoring;
- model traceability and version control; and
- testing for robustness and security failures.

Supply chain security

AI operators must evaluate the security of:

- datasets;
- pre-trained models;
- embedded components (libraries, frameworks); and
- remote data-processing elements.

Technical documentation and risk assessment

Providers must maintain:

- risk-management documentation;
- logs that enable incident reconstruction; and
- security-testing results.

Under Greek Law 4961/2022, organisations using AI systems that affect employees or users must also:

- maintain registers of AI systems; and
- take measures to mitigate risks such as misuse, bias, and system vulnerabilities.

Common requirements under both the EU AI Act and Greek Law 4961/2022

Dataset integrity and provenance

High-risk AI systems must undergo validation of:

- training-data quality;
- vulnerability to poisoning or tampering; and
- potential biases and statistical weaknesses.

Model security

Both legal frameworks expect:

- secure model deployment;
- controlled access to the model (API security, rate limiting); and
- robustness testing aligned with standards (eg, ISO/IEC AI testing guidance referenced in Greek advisory documents).

Third-party components

Where AI systems rely on:

- pre-trained models;
- open-source components; or
- external AI APIs,

the operator is still responsible for:

- verifying their security characteristics; and
- ensuring they do not introduce vulnerabilities.

6.3 Cybersecurity in the Healthcare Sector

Cybersecurity in the Greek healthcare sector is governed by a multi-layered framework that combines:

- horizontal cybersecurity rules (NIS2, GDPR);
- sector-specific regulation for medical devices (MDR/IVDR reinforced by MDCG guidance); and
- practical obligations arising from procurement processes and system-integration requirements.

Under NIS2, healthcare providers – such as hospitals, clinics, and diagnostic centres – are categorised as essential entities. This designation entails enhanced security and reporting duties. At a minimum, such entities must implement risk-management measures including security policies, vulnerability management, monitoring, access controls, incident-response processes, and supply-chain assurance.

A defining sector-specific element of healthcare cybersecurity is the security of medical devices, especially as they become increasingly connected and software-driven. Under the EU Medical Device Regulation (MDR 2017/745), which applies directly in Greece, medical devices are subject to mandatory cybersecurity-by-design and life cycle-security obligations, established through the General Safety and Performance Requirements (GSPRs) in Annex I.

Incident reporting is one of the most operationally demanding obligations, as many cybersecurity incidents simultaneously trigger GDPR requirements. Furthermore, if a cybersecurity incident affects a medical device, MDR vigilance obligations may also apply. This means that a single incident may generate parallel reporting obligations, such as the following.

- A significant cybersecurity incident must be reported to the NCSA/CSIRT following NIS2 timelines: an early warning within 24 hours, an incident notification within 72 hours, and a final report within one month.
- In the healthcare sector, there is an additional national layer: incidents must also be reported to IDIKA (ΗΔΙΚΑ), which operates central Greek eHealth infrastructures such as the national ePrescription system and the EHR ecosystem.
- IDIKA must be notified whenever a local incident (eg, ransomware in a hospital) could affect interconnected national systems.
- A health data breach requires a risk assessment and, in many cases, notification to the Hellenic Data Protection Authority (HDPa) within 72 hours.
- A cybersecurity incident involving a medical device that creates or risks causing serious harm to patient safety must be reported to the competent market surveillance authority.

Trends and Developments

Contributed by:

Alexandros Choimes and Evangelos Katsaras
ALG Manousakis Law Firm

ALG Manousakis Law Firm was established in 2011 by Ioannis and Alexandros Manousakis. Based in Athens, ALG is an international law firm with lawyers qualified in six EU jurisdictions and Switzerland. The firm's team consists of 50 lawyers and 25 paralegals. With deep expertise in corporate and commercial law, it offers tailored solutions across various indus-

tries. Its client base includes 30 pharmaceutical/biotech and five medical device companies. The firm supports them in contracting negotiations, ensuring compliance, and developing robust data privacy frameworks. The firm has a high rate of success, especially in commercial claims, tax and administrative litigation in general.

Authors



Alexandros Choimes is a senior associate at ALG Manousakis Law Firm. He is a Greek-qualified attorney at law. He graduated from the Law School of the National and Kapodistrian University of Athens and

holds an LLM in Innovation, Technology and the Law from the University of Edinburgh, as well as a minor degree in Business Administration from the American College of Greece. Prior to joining ALG, he completed an internship with the Hellenic Data Protection Authority. His practice focuses on data protection and privacy law, advising clients on GDPR compliance and related regulatory matters.



Evangelos Katsaras is a junior partner at ALG Manousakis Law Firm. He is an EU-qualified attorney at law specialising in privacy, cybersecurity, and AI law, and an IAPP-accredited privacy professional. He holds a Law

and Technology LLM from Tilburg University and is currently a PhD candidate in Law at the National and Kapodistrian University of Athens. His practice focuses on the design and implementation of compliance programmes in the areas of privacy, cybersecurity, and AI, including audits, mapping, third-party risk management, and the development of policies and procedures. He regularly advises on management of cybersecurity incidents and privacy requests.

ALG Manousakis Law Firm

16 Laodikias Str.
Athens
11528
Greece

Tel: +30 210 723 2761
Email: info@alg.gr
Web: www.alg.gr



AI Threats, New Laws, and Expanding Obligations: The Future of Cybersecurity in Greece

Introduction

Cybersecurity in Greece is entering a defining period. By early 2026, the country will have implemented a new generation of legislative and strategic reforms. These developments go beyond routine legal updates and signal a broader shift in the maturity of Greece's cybersecurity ecosystem. At the same time, the rapid adoption of emerging technologies – particularly artificial intelligence (AI) – combined with increasingly sophisticated and complex cyber-attack methods, is fundamentally reshaping the risk landscape. Together, these factors significantly affect the obligations of both public and private sector organisations. This article examines the most important cybersecurity trends and regulatory developments expected in 2026, focusing on issues that are particularly relevant for organisations doing business in Greece or operating digital infrastructure connected to the Greek market.

The regulatory landscape

Since the start of the decade, the Greek regulatory landscape saw the adoption of numerous laws relating to the emergence of new and innovative technologies as well as to the rise of an increasingly complex cybersecurity framework. What makes 2026 particularly significant is that several of these legislative initiatives are now advancing to a new stage of implementation.

NIS2: Full enforcement, registration, and rising scrutiny

Greece's transposition of the EU NIS2 Directive through Law 5160/2024 has moved decisively from being merely "on the books" to being fully in force and actively enforced. A key feature of the Greek approach is the emphasis on registration and post-registration scrutiny. In-scope entities are required to register with the National Cybersecurity Authority (NCSA) and submit specific data sets via the Authority's digital platform. This registration is not a purely formal or declaratory step. Once an entity becomes visible to the NCSA, it is subject to ongoing supervisory engagement, which may include requests for documentation, desk-based reviews, and on-site or remote audits.

These supervisory powers are reinforced by binding secondary measures, such as national requirements on cybersecurity policies, asset inventories, supplier and third-party oversight, and staff training. In practice, this "register-then-supervise" continuum is already being applied and is shaping how compliance is assessed and enforced in Greece.

CER: Enforcement and the knock-on effect for NIS2 scope

Although the Critical Entities Resilience (CER) Directive is not a cybersecurity framework, its transposition into Greek law through Law 5236/2025 is expected to have one of the most significant indirect impacts on the scope of NIS2 in the coming years. CER establishes a new national regime for the identification and supervision of critical entities across key sectors, including energy, transport, health, water, digital infrastructure, banking, public administration, and others. Its focus is on resilience against physical, natural, technological, and hybrid threats.

The relevance of CER for cybersecurity practitioners lies in the designation process. By 17 July 2026, Greece will be required to formally designate all critical entities and record them in a national register. In practice, once an organisation is designated as a "critical entity" under CER, it will almost invariably fall within the highly critical or critical sectors already covered by NIS2. As a result, CER designation effectively operates as an additional trigger for NIS2 applicability. Organisations not previously captured by the cybersecurity regulatory framework will be brought into full NIS2 scope under such designation – not because of changes to cyber rules themselves, but because of their classification as critical entities under CER.

In this way, CER is set to significantly expand the NIS2 compliance perimeter in Greece from 2026 onwards, subjecting a broader range of organisations to cybersecurity oversight through the interplay between resilience and cybersecurity regulation.

CRA: Gradual enforcement and product security obligations coming into focus

The EU Cyber Resilience Act (CRA) is the Union's first horizontal product security regulation for products with digital elements (PDE), a category that includes

almost all connected hardware and software, from IoT devices and embedded systems to firmware, operating systems, standalone applications and cloud-supported digital components. Although, the CRA became legally binding on 10 December 2024, its obligations are intentionally phased in. Starting from September 2026, manufacturers selling PDEs into Greece must begin reporting actively exploited vulnerabilities and severe incidents to national CSIRTs/ENISA.

The digital landscape

In relation to the emergence of these technologies, the digital environment of Greece has been marked by the following trends and observations.

Rapid development of technologies using AI

The relationship between AI and cybersecurity is quite tight considering that the rise in cyber threats is becoming increasingly associated with the capabilities of AI systems such as Large Language Models (LLMs), which, while becoming popular for day-to-day as well as commercial uses, may also serve the purposes of cybercrime groups (eg, for cyber-espionage or for financial gains). AI-enhanced malicious activities are also significant for malware attacks, which are quite common in Greece compared to other EU member states, particularly due to the country's geographical location.

Rise of cyber threats

In 2025, the most significant types of cyber-attacks related to cybercrime activities such as DDoS (distributed denial of service attack) and ransomware, especially impacting public administration bodies, digital providers as well as entities operating in the health sector. Research suggests that the evolution of cybercrime in Greece shows distinctive national characteristics, primarily in cases of fraud (predominantly in the form of ransomware and business email compromise) as well as AI-enhanced attacks, although systematic annual monitoring and available datasets for cybercrime activities (as compiled by the Cyber Crime Division of the Hellenic Police) remain fragmented. Nevertheless, the nature of these threats considering the divergence in national statistics compared to global trends showcase the vulnerability of Greece's SME-heavy economy and the lower digital maturity among local businesses. Based on recent data, Greece ranks

6th worldwide for malware detected in incoming email and 1st in Southern Europe for attacks on industrial systems of high criticality.

Lack of preparedness and online safety

Greek small and medium-sized enterprises (SMEs) remain underprepared for cyber threats, given their limited access to security expertise or infrastructure. Specifically, although Greek SMEs make up 99.9% of all businesses, they have emerged as the weakest link in the European Union with regards to cybersecurity, ranking last in terms of protective measures and comprehensive policies against cyber-attacks. In addition, Greece is among the most dangerous online environments, with ransomware and malware attacks surging more than tenfold in 2024 alone, targeting more than one in five Greeks at least once (22%).

Increase in cybersecurity investments

The cybersecurity market in Greece is expected to gain more than 50% and to exceed USD270 million in total value by 2031. Such gains are foreseen due to a number of factors, primarily regarding the increased interest of the Greek private sector in the protection of their digital infrastructure (considering their vulnerability against cyber threats, as described above), rising investments from the EU Recovery and Resilience Facility, as well as foreign investments, such as the USD1 billion investment from Microsoft for the creation and activation of three data centres on Greek territory by 2028. Such continuing digitalisation, which will affect both the private and public sectors, is expected to have a significant impact on the implementation of the NCSA's action plan and to place cybersecurity among Greece's top national priorities moving forward.

The strategic landscape

In parallel to the enactment of the laws mentioned in "The regulatory landscape" above, the NCSA recently published its updated National Strategy on Cybersecurity (2026–2030) in December 2025 by virtue of the Ministerial Decision No 2563/16-12-2025 (the "Strategy"). The updated Strategy came to replace the previously adopted National Strategy (2020–2025) which had been established in light of the older NIS Directive and its transposing Law 4577/2018, stressing the need for institutional changes in response to the

rapid digital development as well as the emergence of novel cybersecurity threats which called for more robust cybersecurity governance systems as well as for advanced organisational readiness.

In formulating its five-year plan, the NCSA focused heavily on the report that was published in March 2024 by the European Union's Agency for Cybersecurity (ENISA), titled "Foresight Cybersecurity Threats for 2030." According to the report, the top ten cybersecurity threats from now to 2030 and beyond (based on total impact and likelihood) are the following.

- Supply chain compromise of software dependencies.
- Skill shortage.
- Human error and exploited legacy systems within the cyber-physical ecosystems.
- Exploitation of unpatched and out-of-date systems within the overwhelmed cross-sector tech ecosystem.
- Rise of digital surveillance authoritarianism/loss of privacy.
- Cross-border ICT service providers as a single point of failure.
- Advanced disinformation/influence operations (IO) campaigns.
- Rise of advanced hybrid threats.
- Abuse of AI.
- Physical impact of natural/environmental disruptions on critical digital infrastructure.

Eventually, the Strategy aims to support the Greek state as well as its enterprises and citizens in navigating the new digital landscape by focusing on four main strategic goals, with each one of them broken down to further specifications and considerations.

Goal #1: Developing skills and raising awareness

With this goal, the NCSA focuses on the following.

- Boosting cyber resilience within the private sector by identifying the specific cybersecurity needs of SMEs, promoting the implementation of European and international cybersecurity standards and developing a cybersecurity readiness toolkit for SMEs as well as for self-employed professionals.

- Bridging the skills gap in cybersecurity matters by building related training platforms, preparing a national action plan for education and awareness in cybersecurity, implementing a comprehensive cybersecurity training programme for managers in public administration, building targeted awareness programmes for senior management in the public and private sectors and implementing specific reskilling and upskilling programmes for information security officers in the public sector.
- Fostering investment and innovation by enhancing the role and functions of the National Coordination Centre (NCC-EL ScaleUP), ensuring continuous co-operation with academic and research institutions on cybersecurity issues, developing financial incentives for investment in cybersecurity services and tools, and establishing a Cybersecurity Investment Observatory as well as a National Cybersecurity Reserve for the financial support of cybersecurity-related projects and initiatives.
- Enhancing readiness and response strategies in cybersecurity incidents by developing a National Communication and Awareness Plan, building a comprehensive exercise programme (especially on crisis management) within the scope of the NIS2 Directive and the CER Directive, preparing information and training materials, establishing a communication management framework in case of cybersecurity incidents, conducting awareness-raising campaigns in primary and secondary education, optimising the function of cybersecurity operation centres (gSOC and mini-SOC), conducting vulnerability scans and vulnerability analyses as well as establishing supporting functions such as the Cybersecurity Testing and Research Analysis Laboratory (LAB), the Unified Cybersecurity Reporting Centre (EL-SOC), as well as the Computer Security Incident Response Teams (CSIRTs).

Goal #2: Strengthening of national, European and international co-operation

This goal focuses on the following.

- Strengthening mechanisms for preventing and combating cybercrime by taking advantage of modern tools, techniques and collaboration processes, developing and implementing cybercrime-related training programmes for law enforcement

officials (such as police officers, prosecutors and judges) and updating policies and action plans for dealing with ransomware and deepfake-driven attacks.

- Enhancing European and international co-operation by establishing a Strategy for International Cooperation on Cybersecurity Issues, promoting the NCSA's public and international presence and strengthening the co-operation in the context of shaping a European Cybersecurity Policy.
- Establishing reliable mechanisms for exchange of information through the creation of a threat intelligence sharing platform.
- Establishing procedures for mutual assistance through the enhancement of cyber resilience among Greek local authorities.

Goal #3: Systemising cybersecurity governance

This goal promotes the following.

- The development of cybersecurity management frameworks by strengthening business continuity and disaster recovery mechanisms as well as developing a crisis management national plan.
- Secure digital identities and trust in public digital services by upgrading the protection of government websites.
- The establishment of a national cybersecurity risk assessment framework by preparing threat landscape reports, developing and maintaining a register to include hardware, software, and intangible information assets in critical sectors (public sector and critical infrastructure) and conducting a national cybersecurity risk assessment.
- The improvement of national cybersecurity governance by establishing a Cybersecurity Coordination Committee for Public Administration, developing and implementing a unified co-ordination framework for information security officers in Public Administration, formulating an operational framework for Organic Cybersecurity Units of Central Administration Bodies, adopting and implementing secondary legislation under Law 5160/2024, developing and publishing sectoral cybersecurity policies and standards, developing audit mechanisms on the implementation of cybersecurity requirements, building a cybersecurity governance manual for public bodies, creating of a training and

certification framework for cybersecurity inspectors as well as cyber insurance providers, and developing a policy framework related to the security of submarine communications cables.

- The implementation of cybersecurity risk management measures by implementing a comprehensive cybersecurity framework for 5G networks as well as a framework of measures and actions for AI, Cybersecurity and the Internet of Things (IoT), establishing secure design principles for new ICT systems in the public sector, developing a national framework for the secure transition of services to cloud computing, and conducting NCSA audits (eg, on essential and important entities under the NIS2 Directive).
- The enhancement of cybersecurity incident reporting mechanisms through the creation of a central mechanism for co-ordinated reporting of cybersecurity incidents as well as a cyber hotline.

Goal #4: Bolstering regulatory compliance / updating cybersecurity policies and procedures

The last goal aims to achieve the following.

- Balancing cybersecurity and the protection of privacy by developing a national framework on privacy and security by design, as well as a plan on cybersecurity and privacy compliance with both Data Protection Officers (DPOs) and Chief Information Security Officers (CISOs) as target audiences.
- Bolstering cybersecurity in the supply chain by establishing a framework for secure ICT procurement as well as supply chain security.
- Protecting and strengthening cyber resilience among critical sectors by creating and updating a dedicated list relating to critical infrastructure, developing specific system guidelines and security standards for particular categories such as ICS, SCADA and IIoT, adopting a sectoral strategy and action plan for cyber resilience in the field of civil aviation and strengthening the cyber resilience of the “.gr” and “.ελ” domain name registries.
- Establishing a national policy to co-ordinate disclosure of vulnerabilities (CVD Policy) by developing a dedicated national mechanism as well as a national incentive framework for responsible vulnerability disclosure (Bug Bounty GR).

- Promoting active protection in cyberspace by creating a framework of requirements for the development of a register of recommended cybersecurity service providers, upgrading and operationalising the National Cybersecurity Certification Authority, establishing an institutional certification framework in line with Regulation (EU) 2019/881 (“EU Cybersecurity Act”) and strengthening of cyber prevention capabilities in the national defence sector.

Practical considerations

Drawing together the regulatory, digital and strategic landscapes above, the following focus areas can help organisations operating in Greece calibrate their 2026 plans.

A. Prepare for deep NIS2 supervision

- Treat NIS2 registration as the start of ongoing regulatory engagement rather than a formal requirement.
- Conduct internal or third-party audits to verify readiness.
- Maintain up-to-date documentation and records to support potential desk-based audits or on-site inspections.
- Implement mandatory secondary measures, including comprehensive policies, asset inventories, supplier oversight programmes, and staff training.

B. Monitor CER designation of critical entities

- Identify whether or not the organisation falls within CER’s scope and track the official designation process.
- Re-assess NIS2 applicability immediately after CER designation to ensure full regulatory compliance.
- Integrate CER and NIS2 requirements into internal compliance monitoring frameworks.

C. Accelerate CRA readiness

- Establish CRA compliance workstreams ahead of 2026 obligations.
- Prepare to provide CRA-aligned product security evidence for procurement processes.
- Ensure market access readiness by implementing CRA-aligned practices before 2027 deadlines.

D. Strengthen defences against AI-enabled and hybrid cyber threats

- Deploy detection capabilities to identify AI-generated threats and abnormal behavioural patterns.
- Upgrade endpoint, identity, and email security controls to mitigate advanced attacks.
- Implement technical and procedural measures to prevent deepfake-driven fraud and hybrid cyber incidents.

E. Address SME weakness in the supply chain

- Conduct comprehensive vendor risk assessments and define minimum-security baselines for suppliers.
- Perform periodic verification of supplier compliance with cybersecurity standards.
- Provide SMEs with practical support, including templates, awareness training, and secure configuration guidance.
- Request all critical suppliers to comply with NIS2-aligned security provisions.

F. Invest in cyber skills, training, and governance

- Recruit cybersecurity professionals proactively to address talent shortages.
- Develop and upskill existing employees through targeted training programmes.
- Strengthen internal governance by clearly defining cybersecurity roles, responsibilities, and escalation procedures.

G. Enhance incident response capabilities across multiple regulatory regimes

- Map all relevant reporting channels and timelines across NIS2, GDPR, CRA, CER, and sector-specific frameworks.
- Develop unified incident response playbooks to ensure consistent handling of multi-regime obligations.
- Establish a central incident response function to triage, manage, and report incidents efficiently across all applicable regulations.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com