KYRIAKIDES GEORGOPOULOS
LAW FIRM

DATA PRIVACY, CYBERSECURITY AND TECHNOLOGY LAW

Data, Cybersecurity & AI | Key Developments

September 1, 2026

Data, Cybersecurity & AI | Key Developments

National Developments

New rules on malicious websites: What companies need to know

As of 1 August 2026, companies and individuals may consult the National Blocklist of Malicious Websites published on the website of the Greek National Cybersecurity Authority (‘**NCSA’**).

The Blocklist, established by virtue of Article 33 of Law 5305/2026, includes **domain names** and **IP addresses** associated with phishing, social engineering and other deceptive practices. The designation of a website or electronic link as unsafe, and its inclusion in the Blocklist, is made by decision of the Governor of NCSA.

The Hellenic Police Cybercrime Directorate and the Hellenic Telecommunications and Post Commission (‘EETT’) may also notify malicious websites to the NCSA.

Listed websites shall remain on the List for three months, subject to reassessment.

New obligations for ISPs and intermediary service providers

Internet service providers (ISPs) and intermediary service providers established or operating in Greece are required, upon listing of a malicious website on the National Blocklist, without undue delay, to:

a) redirect users attempting to access listed websites to a warning page, or

b) block access to the website through appropriate technical means where such access is attempted from Greek IP addresses.

Review and Appeal Mechanisms for NSCA’s Decisions

The NCSA Governor’s decision may be revoked where a website has been erroneously included in the Blocklist and/or following a successful appeal. Domain name and IP address owners, administrators and other persons with a legitimate interest may challenge the decision within ten days of the website's inclusion in the National Blocklist. However, such challenge does not suspend the effectiveness of the listing decision or any associated access-blocking measures.

Rejected decisions may subsequently be challenged before the competent Administrative Court of Appeal, with a further appeal available before the Council of State.

New National Strategy for Resilience of Critical Entities

The General Secretariat for the Protection of Critical Entities (‘GGPKO’), under the Minister of Citizen Protection, prepared the National Strategy for the Resilience of Critical Entities (‘the Strategy’) pursuant to Article 5 of Law 5236/2025, which transposes the Critical Entities Resilience Directive into Greek law.

The Strategy was subject to public consultation from 14 to 20 July 2026 and was subsequently approved by KYSEA, according to an announcement by the Greek Government.

Main elements of the Strategy

The National Strategy for the Resilience of Critical Entities establishes the overarching framework for implementing Greece's critical-entity resilience regime. It sets out the strategic priorities,

governance arrangements and key implementation measures, including:

- **Six (6) strategic objectives:** enhancing risk awareness and prevention; protection; response; recovery and continuity; governance and coordination; and capabilities, resources and financing.
- **Sectoral priorities:** Energy, digital infrastructure and transport are placed in the first tier; health, drinking water, food, wastewater and urban waste in the second; and public administration, space infrastructure, financial markets and the banking sector in the third.
- **Horizontal resilience priorities:** The Strategy identifies cross-sectoral priorities, namely supply chain security, emerging technologies and threats, climate adaptation and Natech risks, economic resilience, foreign direct investment screening and infrastructure lifecycle management.
- **Governance framework**: KYSEA, the Ministry of Citizen Protection, GGPKO and the sectoral competent authorities are central to the Strategy's implementation. GGPKO acts as the national competent authority and single point of contact, alongside the sectoral competent authorities designated for each sector listed in the Annex to Law 5236/2025, including the Regulatory Authority for Energy, Waste and Water (RAAEY), the Ministry of Health's General Directorate for Health Services and the Hellenic Food Authority (EFET).
- **Designation of critical entities:** The Strategy outlines a three-stage designation process consisting of information collection, assessment against statutory criteria, and designation and registration in the National Register of Critical Entities.
- **Support tools and capacity building:** The Strategy provides for guidance, methodologies, standards, training, preparedness exercises, incident reviews and support to critical entities. The National Register will function as a digital portal, central database, supervisory tool and coordination mechanism.

What businesses should expect next

Implementation will take place in four phases, with the designation of critical entities and the launch of the National Register expected in the second phase. The Strategy does not itself impose direct legal obligations; further operational requirements will follow through an Implementation Plan and the administrative acts required by Law 5236/2025.

EU Developments

AI Act implementation

Guidelines on transparency obligations for providers and deployers of certain AI systems

The European Commission has published new Guidelines on the transparency obligations, providing practical clarification on requirements that became applicable on 2 August 2026. The Guidelines clarify when users must be informed that they are interacting with AI, how AI-generated or manipulated content should be marked, and the transparency requirements applicable to deepfakes, emotion recognition systems, biometric categorisation tools, and AI-generated text on matters of public interest. They also offer detailed explanations and examples, to help organisations assess whether their systems fall within scope and demonstrate compliance.

The General-Purpose AI Code of Practice (GPAI)

The European Commission has published the General-Purpose AI (GPAI) Code of Practice, a voluntary compliance framework designed to help providers of GPAI models meet their obligations under the AI Act. The Code, endorsed by both the

European Commission and the AI Board as an adequate means of demonstrating compliance, is structured around three key pillars: **transparency, copyright, and safety and security**. While the transparency and copyright chapters are relevant to all GPAI model providers, the safety and security chapter applies specifically to providers of the most advanced models that present systemic risks.

Commission started enforcing AI Act rules

The EU AI Act entered a significant new phase on **2 August 2026**, with the European Commission's AI Office commencing enforcement of key AI Act obligations. The date marks the application of the Act's transparency requirements under article 50, as well as the start of enforcement of rules applicable to general-purpose AI models.

EDPB's new guidelines

EDPB Issues New Guidance on Anonymisation, Web Scraping and Blockchain Technologies

The EDPB has taken an important step in clarifying the application of EU data protection rules to emerging technologies by adopting new guidelines on anonymisation and web scraping in the context of generative AI, while also finalising its guidelines on the processing of personal data through blockchain technologies.

The Guidelines on Anonymisation aim to bring greater certainty to one of the most challenging concepts under EU data protection law. Taking into account recent CJEU case law, the EDPB clarifies when data can be regarded as genuinely anonymous and therefore fall outside the scope of the GDPR. The guidelines introduce a practical assessment framework based on three key risks, namely record isolation, linkage and inference, and provide organisations with methodologies for evaluating whether anonymisation measures are sufficiently robust in a given context.

The Guidelines on Web Scraping in the Context of Generative AI address the growing use of publicly available online information for AI training purposes. The EDPB emphasises that the public availability of information does not remove GDPR obligations where personal data is involved and examines key compliance requirements, including lawful basis, transparency, purpose limitation, data minimisation and the processing of special categories of personal data. The guidance also highlights technical and organisational measures that may help reduce privacy risks throughout the AI training lifecycle.

In addition, the EDPB has adopted the final version of its Guidelines on the Processing of Personal Data through Blockchain Technologies. The guidelines are intended to assist organisations using blockchain-based solutions in complying with the GDPR and explain how different blockchain architectures may affect data protection obligations. They provide guidance on key issues such as the allocation of roles and responsibilities, the application of data protection principles, and the challenges associated with exercising data subject rights in decentralised environments.

While the blockchain guidelines have now been adopted in final form, the anonymisation and web scraping guidelines have been published for consultation, with stakeholders invited to submit comments until **30 October 2026**.

Contact Us

Irene Kyriakides
PARTNER
i.kyriakides@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