KARATZAS & PARTNERS

Data Protection, AI & Cybersecurity

Brief

June 2026

KARATZAS & PARTNERS

At a glance

EDPB Adopts Common Data Breach Notification Template

€176,000 Fine for Unlawful Retention of Former Employee's Corporate Email Account

Greek DPA Warns Hotels Against Copying IDs and Payment Cards

EU-Wide Cyber Exercise Tests Response to Attacks on Critical Transport Infrastructure

European Commission Proposes Tech Sovereignty Package

Greece Opens Public Consultation on National AI Act Implementation Framework

Commission Publishes Final Code of Practice on Marking and Labelling AI-Generated Content

Thomson Reuters v. ROSS Intelligence – First US Appeals Court to Review Fair Use in AI Training

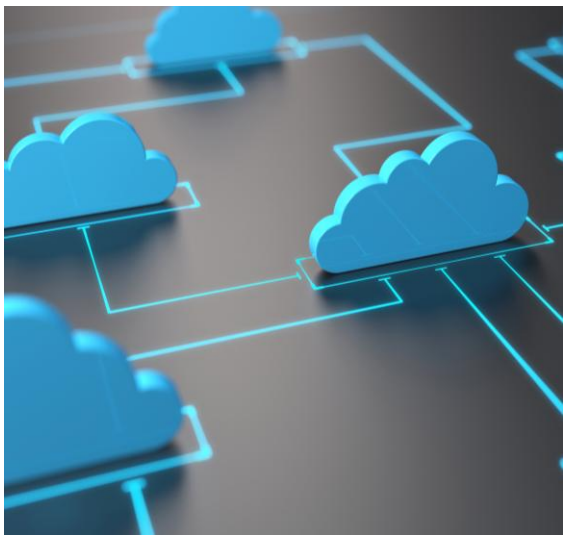
EDPB Adopts Common Data Breach Notification Template

On **8 June 2026**, the European Data Protection Board (EDPB) adopted a common template for personal data breach notifications under Article 33 GDPR. The template is designed to help organisations and Data Protection Authorities (DPAs) to structure, harmonise and unify their data breach notification processes.

The template ensures notifications contain all the information required under Article 33 GDPR, making it easier for organisations to submit a timely notification and facilitating the assessment by the competent DPAs. It provides predefined options to choose from, along with guidance on how to fill in the fields and is expected to help organisations save time and costs.

The template is subject to public consultation until **5 August 2026**. Following the public consultation, the EDPB will decide on the timeline for the practical implementation of the template by all DPAs.

Why it matters: The harmonised template has the potential to significantly reduce compliance burdens for organisations operating across multiple EU jurisdictions. DPOs and compliance professionals should familiarise themselves with the proposed template and consider submitting feedback during the public consultation.



€176,000 Fine for Unlawful Retention of Former Employee's Corporate Email Account

A recent decision by the Belgian Data Protection Authority (APD) sends a clear message to employers across the EU regarding corporate email accounts after an employee leaves.

Key Takeaways

a) A professional email mailbox contains personal data of the former employee and third parties, not just business information.

b) Keeping or accessing a former employee's mailbox is ongoing personal data processing under the GDPR.

c) A short transitional retention period may be allowed for operational reasons, usually up to one month and exceptionally up to three months if clearly documented.

d) Simply disabling the account is not enough if the data remain stored and technically accessible.

e) Failure to inform the former employee and third parties breaches GDPR transparency rules under Articles 5(1)(a), 6(1), 12, and 13 GDPR.

Why It Matters: In this case, improper handling led to administrative fines of around €176,000. The decision highlights that email account deletion, clear retention policies, and transparent communication are essential to GDPR compliance. Employers should implement strict procedures for deactivating and deleting corporate email accounts promptly after employee departures to avoid regulatory and financial risk.

Greek DPA Warns Hotels Against Copying IDs and Payment Cards

On **24 June 2026**, the Hellenic Data Protection Authority (HDPA) issued compliance recommendations to hotels and tourism accommodation providers following complaints regarding the collection and retention of guests' personal data. The Authority found that practices such as photographing or photocopying identity documents and storing copies of customers' credit or debit cards violate key GDPR principles, including lawfulness, transparency, and data minimization, while creating unnecessary risks of unauthorized access, fraud, and financial harm. The HDPA called on hotel associations to inform their members of their obligations and urged accommodation providers to review check-in, payment and booking procedures, ensure an appropriate legal basis for all data processing activities, and provide clear privacy information to guests.

Why it matters: The HDPA's intervention serves as an important reminder that convenience-driven business practices must not override GDPR requirements. The guidance is particularly relevant for the hospitality sector, where large volumes of personal and payment data are processed daily, and highlights the need for organizations to adopt privacy-by-design principles, minimize data collection and strengthen customer trust while reducing regulatory and cybersecurity risks.

EU-Wide Cyber Exercise Tests Response to Attacks on Critical Transport Infrastructure

On **10 and 11 June 2026**, the European Union conducted a major EU-wide cyber exercise to test how Europe would respond to cyberattacks on critical transport infrastructure, specifically targeting rail and maritime networks. A total of 5,000 experts participated in the exercise.

The exercise, organized by the EU Agency for Cybersecurity (ENISA), forms part of the EU's broader cybersecurity preparedness framework, including the NIS2 Directive and the Cyber Solidarity Act.

The exercise focused on detection, containment, and cross-border cooperation in responding to simulated large-scale attacks on critical transport systems.

Why it matters: The exercise underscores the EU's commitment to operational readiness and cross-border cooperation in the face of evolving cyber threats. For organisations in the transport sector and other NIS2-regulated industries, the exercise serves as a reminder that regulatory focus is shifting from implementation to enforcement.

European Commission Proposes Tech Sovereignty Package

On **3 June 2026**, the European Commission released its European Technological Sovereignty Package, a set of legislative and policy measures to strengthen the EU's capacity in semiconductors, artificial intelligence, cloud computing, and open-source software. The Package aims to reduce Europe's dependence on non-EU technology providers and strengthen the EU's digital autonomy and resilience.

These measures are part of the EU's broader ambition to become a global leader in the research, development, and adoption of AI, complementing the Competitiveness Compass and the Economic Security Strategy.

Why it matters: The Tech Sovereignty Package represents a significant shift in EU technology policy, moving from a regulatory-focused approach to a more proactive strategy of building domestic capacity. Semiconductor companies, cloud providers, data centre operators, AI developers, software vendors, and public-sector suppliers should assess how the proposed initiatives could affect market access, funding opportunities, procurement conditions, and cybersecurity expectations.

Greece Opens Public Consultation on National AI Act Implementation Framework

On **21 June 2026**, the Ministry of Digital Governance and Artificial Intelligence placed on public consultation a draft law titled "Measures for the Implementation of Regulation (EU) 2024/1689 on Artificial Intelligence - Amendment of Law 4961/2022 and other provisions". The consultation runs on the OpenGov platform until **6 July 2026**.

The bill establishes Greece's national framework for applying the EU AI Act domestically, ahead of the Article 50 transparency obligations taking effect on **2 August 2026**.

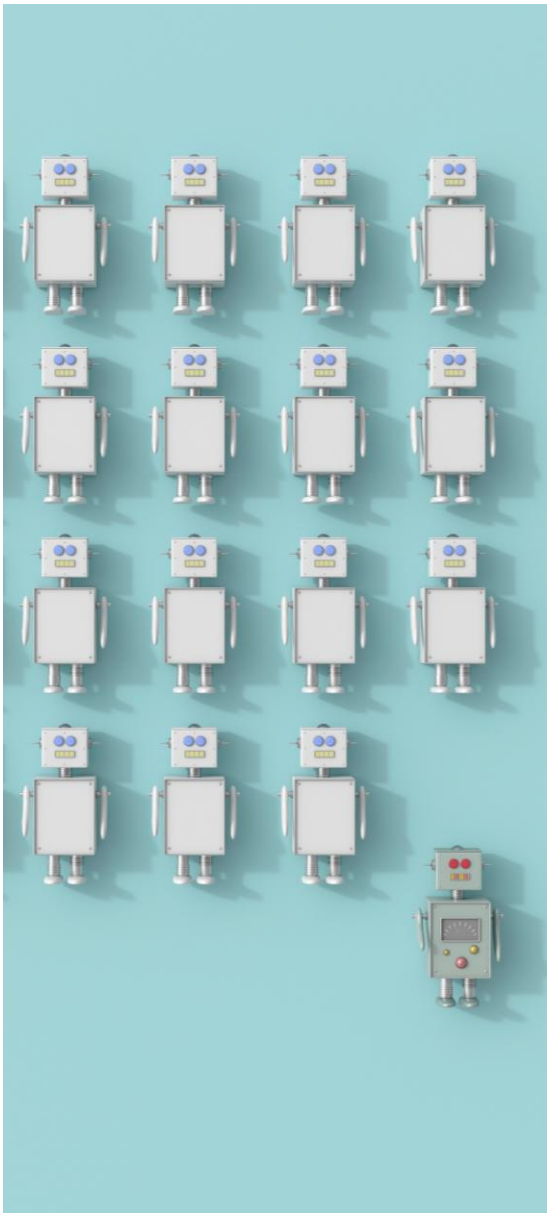
Key elements

- Market surveillance authority: The Hellenic Data Protection Authority (HDPA) is designated as the central market surveillance authority and national contact point for the AI Act in Greece.
- Notifying authority: The Hellenic Telecommunications and Post Commission (EETT) will act as the notifying authority for conformity assessment bodies.
- AI Coordination Centre: A new Artificial Intelligence Coordination and Expertise Centre will support the regulatory framework's application.
- Regulatory sandbox: The bill creates a sandbox for AI innovation, aimed at start-ups and SMEs, in line with Article 57 of the AI Act.
- Complaints and penalties: The law establishes complaint procedures and a national penalty regime for AI Act breaches.

Greece Opens Public Consultation on National AI Act Implementation Framework

Why it matters: The designation of the HDPA as central market surveillance authority signals that AI enforcement and GDPR enforcement will increasingly converge within a single institution. Organisations deploying AI systems in Greece should assess their compliance posture ahead of **2 August 2026**, particularly regarding transparency obligations.

The regulatory sandbox offers a structured pathway for testing AI systems under supervision, while the formal complaints mechanism and penalties framework confirm that enforcement risk is no longer theoretical. Practitioners should review the draft law and consider submitting feedback by **6 July 2026.**



Commission Publishes Final Code of Practice on Marking and Labelling AI-Generated Content

On **10 June 2026**, the European Commission published the final voluntary Code of Practice on marking and labelling AI-generated content. The Code provides practical guidance to help providers and deployers of generative AI comply with the transparency obligations of Article 50 of the Artificial Intelligence Act, which apply from **2 August 2026**.

From that date, the Artificial Intelligence Act requires clear labelling of deepfakes and AI-generated or AI-manipulated content on matters of public interest, as well as user notification when interacting with AI systems such as chatbots.

The Code has two sections. Section 1 addresses providers and requires technical measures for marking and detection, including machine-readable metadata, watermarking, and free detection tools, with interoperable solutions to be implemented by **2 February 2027**. Section 2 concerns deployers and sets rules for visible labelling using standard EU icons and a common taxonomy distinguishing fully AI-generated from AI-assisted content.

Why it matters: Once approved by the Commission and the AI Board, signatories will be able to rely on the Code to demonstrate compliance. Although voluntary, the Code is expected to become the main benchmark for assessing compliance with Article 50, which is among the earliest applicable obligations of the Artificial Intelligence Act.

Thomson Reuters v. ROSS Intelligence – First US Appeals Court to Review Fair Use in AI Training

In **June 2026**, the US Court of Appeals for the Third Circuit heard oral arguments in Thomson Reuters v. ROSS Intelligence, the first US appellate case to examine whether using copyrighted content to train AI systems qualifies as fair use. The dispute concerns ROSS's alleged unauthorised use of Westlaw headnotes and key number classifications to train an AI legal research tool. The district court found copyright infringement and rejected fair use; ROSS has appealed, arguing its use was transformative.

Why it matters: The forthcoming decision will be the first appellate ruling in the United States on fair use and AI training and is closely watched by technology, publishing, and creative sectors. Although based on US law, the outcome may influence global debates on AI training data, including EU discussions on the interaction between the AI Act, copyright law, and text and data mining exceptions, as well as the future development of licensing markets for AI training data.

KARATZAS & PARTNERS

About Us

Dimitra Karampela, Senior Associate
d.karampela@karatza-partners.gr

Panagiotis Kontizas, Associate
p.kontizas@karatza-partners.gr

Georgia Patiri, Associate
g.patiri@karatza-partners.gr

Contact Us

The Orbit-5th floor, 115 Kifissias Ave.11524 Athens, Greece

+30 210 371 3600

mail@karatza-partners.gr

dataprotection@karatza-partners.gr