KARATZAS & PARTNERS

Data Protection, AI & Cybersecurity

Brief

August - September 2026

KARATZAS & PARTNERS

At a glance

Trump v. Slaughter: Letter to the European Commission

HDPA Decision 15/2026

New State Credit-Scoring System

Guidance on Smart Glasses and Privacy

DSA: Designation of ChatGPT, Reddit and Roblox

HDPA Opinion 10/2026

AI Act: First European Standard on Quality Management Systems

AI Act Enters Enforcement Phase

"Trendsetting" Designs Get No Wider Protection

CJEU: Use of Trademarks in Political Campaigns

First EU Design Registrations Using Video and 3D Files

New Reporting Obligations for Manufacturers for CRA

List of Malicious Websites

EU–US Data Privacy Framework: EDPB Letter to the European Commission on US Supreme Court judgment Trump v. Slaughter

On **31 July 2026**, EDPB Chair Anu Talus wrote to Commissioner Michael McGrath asking the European Commission to "closely assess" whether the US Supreme Court's judgment in Trump v. Slaughter affects the functioning of the EU–US Data Privacy Framework (DPF). In Trump v. Slaughter (**29 June 2026**), the Court overruled Humphrey's Executor and held that the President may remove Federal Trade Commission (FTC) commissioners without the specific restrictions previously understood to apply.

The 2023 adequacy decision underpinning the DPF expressly relied on the FTC's institutional independence and on the understanding that commissioners could be removed only for "inefficiency, neglect of duty, or malfeasance in office."

The EDPB frames the existence and effective functioning of independent supervisory authorities as a key element of adequacy under Article 45 GDPR, but it did not call for suspension or revocation of the Framework.

Why it matters: The DPF remains valid unless the Commission amends or withdraws it, or a court invalidates it. In light of these US developments, organisations relying on the DPF should ensure that fallback mechanisms, such as standard contractual clauses supported by up-to-date transfer impact assessments, are ready to use.

HDPA Decision 15/2026: Ransomware Attack on EETAA Systems Processing Childcare-Programme Data

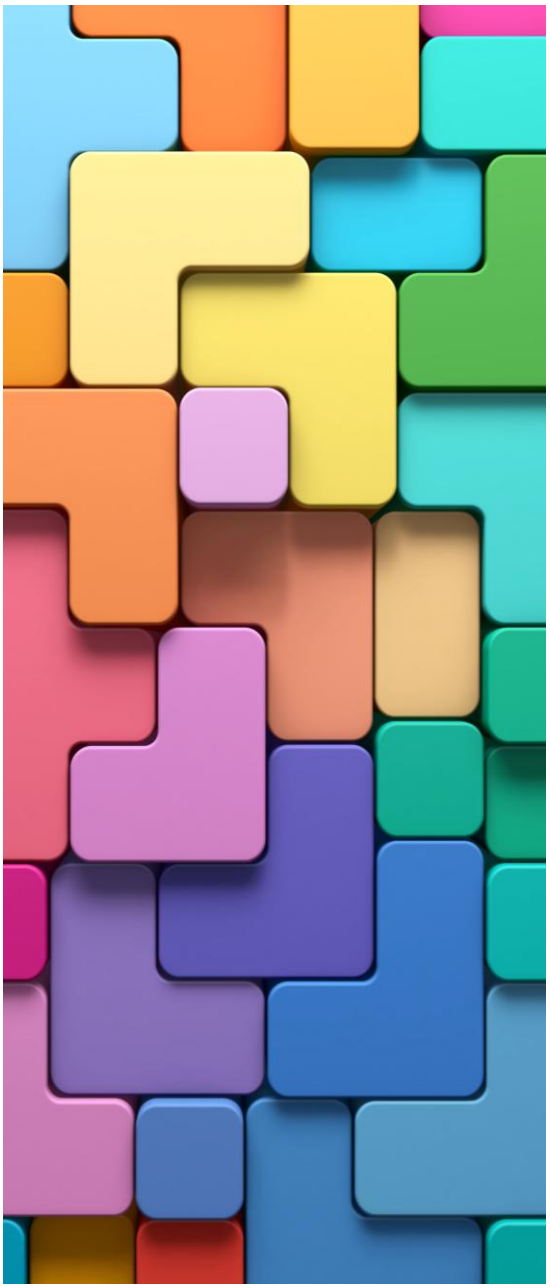
In Decision 15/2026 **(28 July 2026),** the HDPA examined a personal data breach jointly notified by the Ministry of Social Cohesion and Family (YKOISO), acting as controller, and the Hellenic Agency for Local Development and Local Government (EETAA), acting as processor. In early **March 2025**, EETAA's on-premises information systems supporting the "Nursery Schools" and the "Neighbourhood Nannies" programmes were hit by a two-stage ransomware attack that encrypted, and possibly exfiltrated, data affecting up to approximately 2.5 million data subjects over a ten-year retention period.

While the Authority found compliance with the notification obligations under Articles 33 and 34 GDPR, it held that the Article 32 security breach resulted from operating an obsolete legacy server with a known and exploitable vulnerability. It also found that the controller failed to appoint a processor providing sufficient security guarantees and that both parties breached Article 28(3) GDPR by not concluding a compliant data processing agreement. The Authority imposed fines of €200,000 on the controller and €150,000 on the processor for the respective violations.

Why it matters: The decision confirms that Article 32 imposes an ongoing "state of the art" security obligation requiring continuous vulnerability management and the timely retirement of legacy systems. It also highlights the need for controller–processor arrangements to clearly allocate responsibility for ongoing security maintenance.

New State Credit-Scoring System for Citizens and Businesses

Issued in **July 2026**, Joint Ministerial Decisions 117113 EX 2026 (Government Gazette B' 4422/20.07.2026) and 117786 EX 2026 (Government Gazette B' 4436/21.07.2026) set out the methodology and operational framework for Greece's new state-operated unified credit-scoring system, administered by the General Secretariat for the Financial Sector and Private Debt Management (ΓΓΧΤΔΙΧ) and accessible through the gov.gr digital platform.



For the first time, a public-sector credit assessment, based on financial-behaviour data drawn from sources including AADE tax records, KEAO social-security debt records and the Electronic Insolvency Registry, is combined with credit assessments provided by private-sector credit bureaus to generate a single "unified score."

New State Credit-Scoring System for Citizens and Businesses

Machine-learning models analysing historical financial-behaviour data estimate the likelihood of future default. Individuals are assigned one of six credit grades and businesses one of ten. The assessment is issued electronically within 24 hours, remains valid for three months and is generated only upon the data subject's explicit consent. Where the score is requested by a private-sector entity, that consent also covers the lifting of tax secrecy and the disclosure of the credit assessment for that specific request.

Why it matters: The new framework significantly expands the role of algorithmic credit assessment in both public administration and private transactions. By combining government-held financial data with information from private credit-assessment providers into a single credit profile, the system is likely to become an important factor in lending, financing and other commercial decisions. This places increased emphasis on GDPR compliance, particularly regarding explicit and request-specific consent, transparency of automated processing, data accuracy and individuals' rights to understand, challenge and correct the information underlying their assessment.

Designation of ChatGPT, Reddit and Roblox under the Digital Services Act

On **31 August 2026**, the European Commission designated ChatGPT as a Very Large Online Search Engine (VLOSE), and Reddit and Roblox as Very Large Online Platforms (VLOPs), under the Digital Services Act (DSA), each service having declared at least 45 million average monthly users in the EU. ChatGPT is the first standalone AI service brought under the DSA's strictest regime, treated as a "hybrid" search service because it can respond to queries by searching the web.

The three services have four months to comply with the additional obligations for very large services, including assessing and mitigating systemic risks, submitting to annual independent audits and publishing transparency reports. Supervision will be shared between the Commission and the Digital Services Coordinators: Coimisiún na Meán (Ireland) for ChatGPT, and the Authority for Consumers and Markets (Netherlands) for Reddit and Roblox. The Commission has now designated 28 VLOPs and VLOSEs in total.

Why it matters: The designation signals that AI-powered services are being folded into the EU's strict online-safety regime, with non-compliance exposing providers to fines of up to 6% of global annual turnover. Providers of large interactive or user-content services should monitor whether they approach the 45-million-user threshold and prepare systemic-risk and audit frameworks well ahead of designation.

Luxembourg CNPD Publishes Guidance on Smart Glasses and Privacy

On **7 August 2026**, Luxembourg's National Commission for Data Protection (CNPD) published new guidance titled "Smart glasses: data protection and respect of privacy." The guidance confirms that purchasing and merely wearing camera- and microphone-equipped smart glasses is not, in itself, prohibited, but that using their recording or AI features may bring the GDPR into play.

The CNPD stresses that recording identifiable individuals in public generally falls within the GDPR and private users may struggle to establish a lawful basis or meet transparency obligations because bystanders may not realise that they are being recorded.

The guidance also notes that recording without consent may infringe a person's right to their own image and give rise to civil claims and further points to Luxembourg's 1982 privacy law, which criminalises covert observation in non-public places. For devices such as Ray-Ban Meta, the competent lead authority is that of the controller's main establishment (Meta).

Why it matters: The guidance reflects intensifying European scrutiny of smart glasses. Although such devices are available across the European Union, applicable data protection requirements may significantly limit the circumstances in which their recording features can be used lawfully.

Unified Property Hub (EKA): Hellenic DPA Opinion 10/2026

On **24 August 2026**, the Hellenic Data Protection Authority (HDPA) issued Opinion 10/2026 on the draft bill of the Ministry of Digital Governance and Artificial Intelligence concerning the establishment of the Unified Property Hub (Ενιαίος Κόμβος Ακινήτων – ΕΚΑ). The ΕΚΑ is envisaged as a unified electronic system, accessible through the Single Digital Portal of Public Administration, consolidating legal and other data relating to properties across Greece, including cadastral, planning, forestry, tax, energy, administrative, municipal, agricultural and judicial information, as well as data concerning their connection to energy, water and telecommunications networks.

The proposed framework aims to facilitate access to property-related information by allowing property owners to access data concerning their properties through a single digital platform, while public authorities and property-related service providers may also access certain data, subject to the applicable conditions. Following the HDPA's initial observations, the Ministry revised the draft bill, which the HDPA considered to address, in general terms, the relevant data protection principles under Article 5 GDPR. However, in Opinion 10/2026, the HDPA identified further issues in Articles 8 and 9, including the clarity of the categories of data to be processed, data minimisation, retention periods, and certain legislative authorisations.

Unified Property Hub (EKA): Hellenic DPA Opinion 10/2026

Why it matters: The EKA would centralise a broad range of property-related information within a single digital system. The HDPA's observations highlight the importance of clearly defining the scope of the data processing, access conditions and retention periods to ensure that the final legislative framework remains aligned with GDPR requirements.

AI Act: First European Standard on Quality Management Systems Published

EN 18286:2026, the first European standard developed to support implementation of the EU AI Act, has been published. It sets out a framework for providers of AI systems to establish and maintain a quality management system (QMS) aligned with the AI Act, covering governance, documentation, risk management and the management of AI systems throughout their lifecycle.

The standard is most relevant to providers of high-risk AI systems, which are required to operate a QMS under Article 17 of the AI Act.

It is the first output of the wider European standardisation process underpinning the practical implementation of the Act.

Why it matters: EN 18286:2026 gives providers of high-risk AI systems a ready-made benchmark for building or stress-testing their QMS and documenting compliance. Aligning existing AI governance processes with the standard now should make it easier to demonstrate conformity as the high-risk obligations approach.

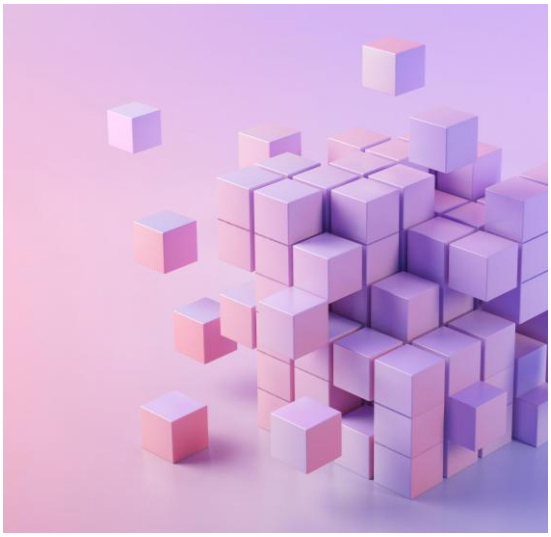
AI Act Enters Enforcement Phase as New Transparency Obligations Apply

Since **2 August 2026**, the European Commission and national authorities have been able to enforce the applicable provisions of the EU AI Act. New transparency obligations also took effect on the same date.

Users must now be told when they are interacting with an AI system, such as a chatbot, and certain AI-generated or manipulated content, including deepfakes, must be clearly marked so that it can be recognized as AI-generated.

To support implementation, the Commission has published a Code of Practice on the marking and labelling of AI-generated content, setting out practical guidance on how to meet these requirements.

Why it matters: The AI Act has moved from preparation to enforcement. Businesses deploying chatbots or producing AI-generated content for customers should check which of their tools fall within the new transparency rules and update their internal AI policies, user disclosures and labelling practices accordingly.



EU General Court: "Trendsetting" Designs Get No Wider Protection — PUMA Loses Safety-Footwear Challenge

On **2 September 2026**, the EU General Court (Case T 376/25) dismissed PUMA's attempt to invalidate an Italian company's registered EU design for a footwear sole, holding that "trendsetting" designs do not enjoy broader protection. PUMA had argued that it created the "pebble-like" design trend and had effectively exhausted the available design freedom, such that the contested design lacked individual character.

The Court rejected that argument, finding that the differences between the designs at issue were sufficiently pronounced to produce a different overall impression on the informed user, while the designer's freedom does not lie solely in the use of a particle structure in the midsole, but also extends to the shape, materials and colour of the various elements of the sole, which are all equally arbitrary features.

Why it matters: The judgment confirms that being first to establish a design trend does not, by itself, narrow the design freedom available to competitors or widen the scope of an earlier design owner's protection. Brand owners relying on distinctive product designs should ensure portfolios capture the specific features that give a design its individual character, rather than assuming market-leading or trendsetting status expands the monopoly.

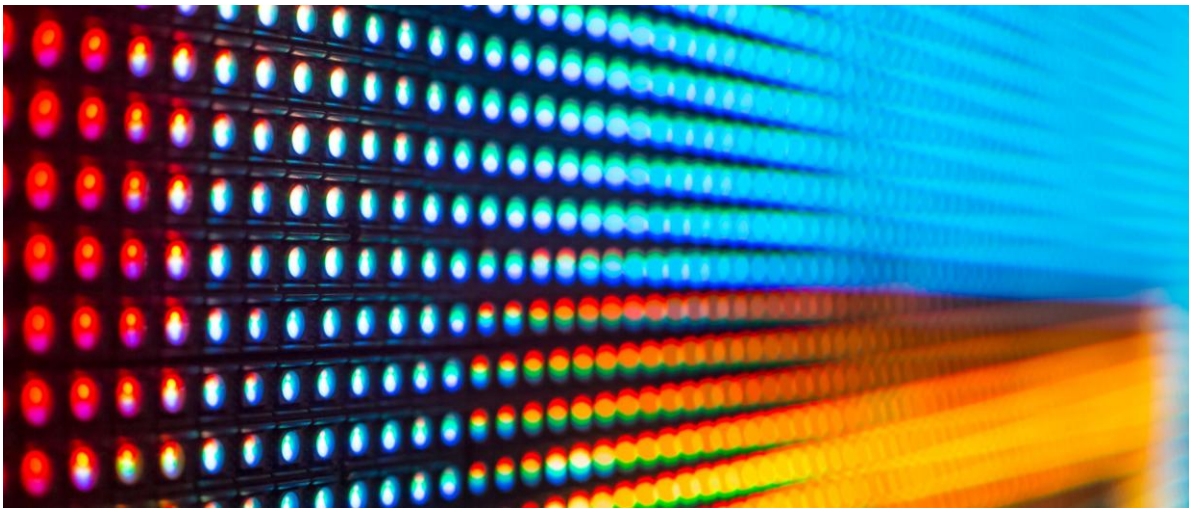
CJEU: Use of Trademarks in Political Campaigns and Freedom of Expression

On 8 September 2026, the Court of Justice of the European Union (CJEU), in **Case C-298/23**, examined the use of the IKEA trade marks by a Belgian political party in connection with its political campaign on immigration. The campaign used signs corresponding to the IKEA trademarks and illustrations resembling IKEA's product assembly instructions. Inter IKEA, the proprietor of the trademarks, brought infringement proceedings, while the political party argued that the use was justified by the right to freedom of expression and constituted "due cause" under EU trademark law.

The CJEU held that **mere reliance on freedom of expression is not sufficient to establish "due cause".** The national court must balance the proprietor's right to property and interests against the third party's right to freedom of expression. The Court found that, in the circumstances of the case, the use of the IKEA trademarks could cause significant detriment to their reputation and to the interests of their proprietor, although the final assessment remains for the referring national court.

Why it matters: The judgment provides guidance on the limits of using well-known trademarks in political speech and confirms that freedom of expression does not justify unauthorized use of a trademark with a reputation. It also highlights the need to balance trademark protection against competing fundamental rights on a case-by-case basis.

EUIPO Publishes First EU Design Registrations Using Video and 3D Files



Following the latest phase of the EU design reform, which became applicable on **1 July 2026**, the EUIPO has published the first EU design registrations represented through video and 3D files rather than static images alone.

The new format is intended for designs involving movement, animation or three-dimensional features that standard images cannot fully capture.

Among the first registrations are an animated graphical user interface for a mobile game and a 3D model of a dice tray with a mobile phone holder.

Why it matters: For products that rely on movement or complex 3D shapes, such as digital interfaces, animated icons or consumer products, video and 3D filings can capture the design more accurately and help define the scope of protection more clearly. Applicants should factor this option into their filing strategy for future EU design applications.

Cyber Resilience Act: New Reporting Obligations for Manufacturers of Products with Digital Elements

Since **11 September 2026**, manufacturers of products with digital elements placed on the EU market must report actively exploited vulnerabilities and severe cybersecurity incidents through the Single Reporting Platform (SRP) operated by the EU Agency for Cybersecurity (ENISA), as required by the Cyber Resilience Act (CRA). The obligation applies irrespective of company size and covers a three-stage process: an early-warning notification within 24 hours, a detailed notification within 72 hours, and a final report (at the latest within 14 days of a corrective or mitigating measure becoming available for a vulnerability, or within one month of the 72-hour notification for a severe incident). Manufacturers must also inform affected users and, where relevant, the wider user base. In Greece, notifications may be routed to the EL-CSIRT of the National Cybersecurity Authority. Note that **11 September 2026** does not mark the full application of the CRA: the essential cybersecurity requirements, technical documentation, conformity-assessment procedures and CE-marking requirements apply from **11 December 2027**.

Why it matters: Reporting is now a live obligation across the entire hardware and software supply chain, from IoT and connected devices to commercial software and standalone components. Manufacturers should ensure their internal incident-detection, vulnerability-management and reporting processes are in place and capable of meeting the tight CRA deadlines.

Greece: National Cybersecurity Authority Maintains List of Malicious Websites

Greece's National Cybersecurity Authority maintains and regularly updates a national list of websites and links identified as malicious, targeting phishing, social engineering and other forms of online fraud.

The list is intended to support the blocking of, and prevention of access to, these websites. As of **25 September 2026**, it contained 110 active entries. The full list is available on the National Cybersecurity Authority's website: *https://cyber.gov.gr/ethnikos-katalogos-apokleismoy-kakovoylon-istotopon/.*

It is particularly relevant for internet service providers, intermediary service providers, and financial and payment institutions, which may be required to take specific measures in respect of listed websites.

Why it matters: The list is a useful resource for fraud prevention and security. Organisations, especially those in the financial sector, should consider using it in their blocking, monitoring and threat-intelligence processes to identify newly listed websites quickly.

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