KARATZAS & PARTNERS

Data Protection, AI & Cybersecurity

Brief

October 2026



KARATZAS & PARTNERS

At a glance

EDPB Guidelines 04/2026 on Fines and Corrective Powers

EDPB Statement on Smart Glasses

Norway: NOK 92M Fine for Xandr over Grindr Data

Netherlands: €824.99M Fine for Uber over Automated Decisions

Greek DPA Opinion on Child Abuse Forensic Protocol

Greek DPA Decision on Personal Data on "Diavgeia"

AI Office Sends First Formal Information Requests

General Court T-564/25: Bad-Faith MAP Trademark Filing

US Appeals Court Rejects ROSS Fair Use Defense in Westlaw Case

EUIPO: First Customs Application for a Craft GI

ENISA Threat Landscape 2026: DDoS and Ransomware Lead

EDPB Guidelines 04/2026 on Fines and Other Corrective Powers

On **17 September 2026**, the EDPB adopted Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR. The Guidelines, which are open for public consultation until **13 November 2026**, set out a five-step methodology that data protection authorities (DPAs) should follow when deciding whether a fine is appropriate.

In short, a DPA should check: (1) whether the infringement can lead to a fine under the GDPR or national law; (2) whether the party investigated can be fined for it, depending on who is subject to the provision in breach; (3) whether the infringement was intentional or negligent; (4) any aggravating and mitigating factors; and (5) whether a fine would be effective, proportionate and dissuasive. Minor infringements will generally lead to a reprimand rather than a fine, but where an infringement is not minor there is a strong presumption that a fine should be imposed. The guidelines also refer to the other corrective powers available (warnings, reprimands, orders, limitations, including bans, and withdrawal of certification) and include some practical examples. These Guidelines complement the previously adopted Calculation Guidelines, focusing on the methodology for calculating the amount of an administrative fine.

Why it matters: The guidelines make enforcement outcomes more predictable across the EU. Once a breach is more than minor, organisations should expect a fine to be the starting point rather than the exception. Businesses wishing to influence the final text should consider responding to the consultation.

EDPB Statement on Smart Glasses

On **13 October 2026**, the EDPB adopted a statement on the privacy risks of smart glasses, which can look like ordinary eyewear, allow near invisible recording and, combined with facial or voice recognition, pose a high risk in public spaces.

Responsibility may lie with the user, the device producer or the provider of a linked app or AI service, as sole or joint controllers.

Users fall outside the GDPR only for purely personal or household use, a narrowly construed exemption that does not cover, for example, sharing on public social media or professional use. Producers and providers cannot rely on users to meet their own transparency obligations.

As traditional privacy notices are insufficient for bystanders, the EDPB recommends combining in-the-moment measures such as hard-to-disable LED and audio indicators, proximity notifications and distinctive design.

Bystander consent will be difficult to obtain, and legitimate interests particularly hard to justify for further commercial use or AI training. The EDPB also encourages privacy-friendly defaults, such as blurring bystanders, disabling persistent storage, and geofencing sensitive locations.

Beyond data protection, some uses may be prohibited under national criminal, civil or labour law or sector-specific rules.

EDPB Statement on Smart Glasses

Why it matters: Smart glasses enable covert recording of people who may have no relationship with the controller and cannot easily be informed, consent or object, leaving transparency, legal basis and data subject rights on uncertain ground, especially for commercial reuse or AI training. Producers and providers should build transparency and privacy-protective defaults into the devices rather than rely on users. Further EDPB guidance is expected.



Norwegian DPA: NOK 92 Million Fine Against Xandr for Unlawful Sharing of Grindr Users' Data

On **12 October 2026**, the Norwegian data protection authority (Datatilsynet) announced a fine of NOK 92 million (approx. €8.6 million) on Xandr, the Microsoft-owned advertising technology company, which is the highest fine it has issued to date. The decision, dated **2 October 2026**, followed a 2020 complaint by the Norwegian Consumer Council.

Between **July 2018** and **April 2020**, Xandr ran real-time advertising auctions inside the Grindr dating app and relayed users' personal data, including data revealing sexual orientation, to potentially thousands of other companies. The authority found that Xandr processed Grindr users' personal data without a legal basis under Article 6(1) GDPR and processed special category data without a valid exemption, in violation of Article 9(1) GDPR.

Xandr argued that it had relied on Grindr obtaining users' consent. The authority rejected this, noting that Xandr never verified the consent, and held that Xandr shared legal responsibility with Grindr. The fine was calculated on Xandr's own turnover rather than Microsoft's, as Microsoft did not own the company at the time of the infringements. Xandr has three weeks to appeal.

Why it matters: The decision outlines that data protection duties cannot be outsourced. Each company in the real-time bidding chain must itself make sure, and be able to prove, that it is allowed to use the data it receives, especially sensitive data. AdTech providers and publishers should review how consent is verified across their supply chain, rather than relying on contracts or on their partners' assurances.

Dutch DPA: €824.99 Million Fine Against Uber for Automated Decision-Making

On 8 October 2026, the Dutch data protection authority (Autoriteit Persoonsgegevens) announced a fine of €824,990,000 on Uber for unlawful automated decision-making and for failing to give drivers enough information about profiling.

The investigation followed complaints from 171 French Uber drivers, filed through the Ligue des droits de l'Homme with the French CNIL and handled by the Dutch authority under the one-stop-shop mechanism, as Uber's European headquarters are in the Netherlands. The case concerned incidents between 2018 and 2022.



The authority found that, where fraud was suspected or customer ratings were too low, drivers' accounts were automatically deactivated, temporarily or (for persistently low ratings) permanently, cutting off their Uber income. This breached the prohibition on fully automated decisions under Article 22 GDPR, while drivers were not properly informed under Article 13. Uber has stopped the practices and has appealed the fine.

Why it matters: This is one of the largest GDPR fines to date and a clear signal that algorithmic management of workers is a priority for regulators. Organisations that use automated tools to suspend accounts, assess performance or make similar decisions should make sure there is meaningful human review and clear, accessible information for the people affected.

Greek Data Protection Authority Issues Opinion on Child Abuse Forensic Protocol

Summary: On **2 September 2026**, the Hellenic Data Protection Authority issued Opinion 11/2026 on a draft Ministerial Decision establishing a protocol for healthcare professionals, police and forensic authorities responding to suspected child abuse. The proposed protocol includes the photographic documentation, storage and transfer of minors' bodily injuries for potential use in criminal investigations. While recognising the fundamental importance of child protection, the Authority highlighted shortcomings in the legal basis for the proposed data processing and called for stronger safeguards, including limiting photographs to strictly necessary evidence, using approved official devices, ensuring encrypted storage and transfer, controlling access and conducting a Data Protection Impact Assessment (DPIA) before processing begins.

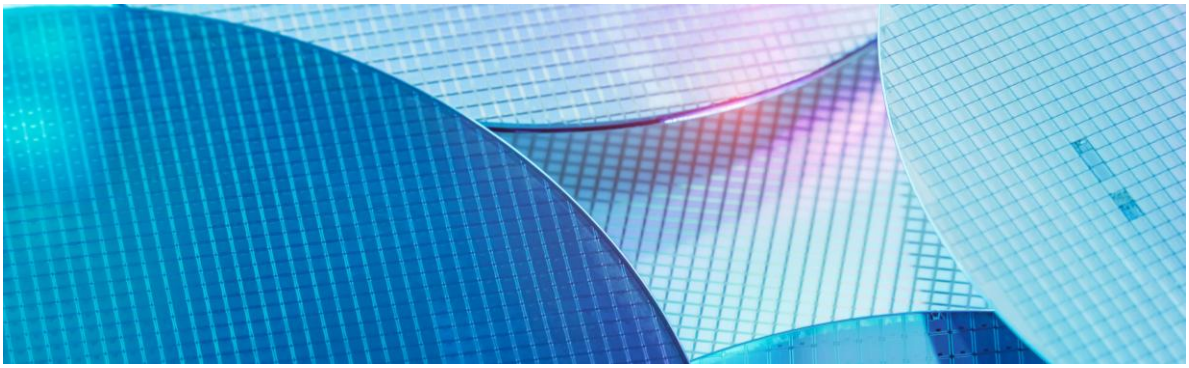
Why it matters: The opinion highlights the need to balance the protection of vulnerable children and the preservation of criminal evidence with the strict requirements of data protection law. It reinforces that sensitive personal data, particularly information concerning minors and potential abuse, must be processed on a sufficiently clear legal basis and subject to robust technical and organisational safeguards. Public authorities should therefore incorporate data protection by design into investigative procedures from the outset, in line with the GDPR.

Greek Data Protection Authority Issues Decision on Publication of Personal Data on “Diavgeia”

Summary: On **6 October 2026**, the Hellenic Data Protection Authority issued the Decision 18/2026, following a complaint filed against the Decentralized Administration of the Aegean. The case concerned the refusal of the administrative authority to delete an engineer’s full name from eleven (11) rejection decisions regarding groundwater drilling license applications that had been published on the “Diavgeia” transparency portal. While acknowledging the principle of public sector transparency, the Authority highlighted that the publication lacked a proper legal basis, as the specific legislative provisions only mandate the publishing of approved licenses rather than rejections containing third-party personal data. The Authority held that the publication infringed the principles of lawfulness and transparency under Article 6(1)(c) GDPR, and that the refusal to delete the data breached the data subject’s right to erasure under Article 17(1)(d) GDPR.

Why it matters: The decision underscores the critical need to balance public transparency initiatives, such as the "Diavgeia" program, with strict adherence to data protection principles. It clarifies that public authorities cannot broadly publish administrative acts containing personal data without an explicit, unambiguous legal mandate. Furthermore, it reinforces that data controllers must respect the rights of data subjects—such as the right to erasure—and ensure that personal information published online is strictly limited to what is legally required and necessary for the stated purpose.

AI Office Issues First Formal Requests for Information



The AI Office's enforcement powers over providers of general-purpose AI (GPAI) models became applicable on **2 August 2026**.

Although the Commission has not officially confirmed which companies received requests, the first formal Requests for Information (RFIs) under the AI Act appear to have already been issued by the European Commission. They concern, among others, model safety, security, external model evaluations and post-market monitoring, as well as compliance with EU copyright rules.

RFIs are legally binding. GPAI providers that ignore them, or give incorrect, incomplete or misleading answers, face fines of up to €15 million or 3% of global annual turnover.

Why it matters: AI Act enforcement has started in practice. GPAI providers should keep technical documentation, copyright policies and training-data summaries up to date and ready for scrutiny. Businesses using AI should map their AI systems and agree internally who will respond to regulators, as scrutiny is likely to extend beyond model providers.

General Court T-564/25: Bad-Faith Filing of the MAP Trademark

On **30 September 2026**, the General Court dismissed an action against an EUIPO decision declaring the international registration of the word mark MAP, covering goods in classes 5 (including pharmaceutical products) and 29 (including dietary supplements), invalid on the ground of bad faith.

The applicants had collaborated for years with a US company whose founder had developed the "Master Amino Acid Pattern" (MAP) formula. They had bought large quantities of MAP-labelled bottles from the company and knew of its earlier marks, before filing for MAP in their own name in 2011 without its consent.

The Court confirmed that bad faith is assessed at the date the EU was designated in the international registration, not the date of the underlying national filing. It held that a cooperation or contractual relationship, whatever its exact form, can create a duty of fair play that prevents one party from registering the other's sign. It added that conduct after filing may confirm a dishonest intention at the time of filing.

Why it matters: The judgment is a useful reminder for businesses that work with distributors, licensees or other partners: a commercial relationship, even an informal one, can be enough to challenge a partner's registration of your brand as a bad-faith filing. Partnership agreements should still state clearly who owns, and may register, the relevant marks.

US Court of Appeals Rejects ROSS's Fair Use Defense in Westlaw AI Copyright Case

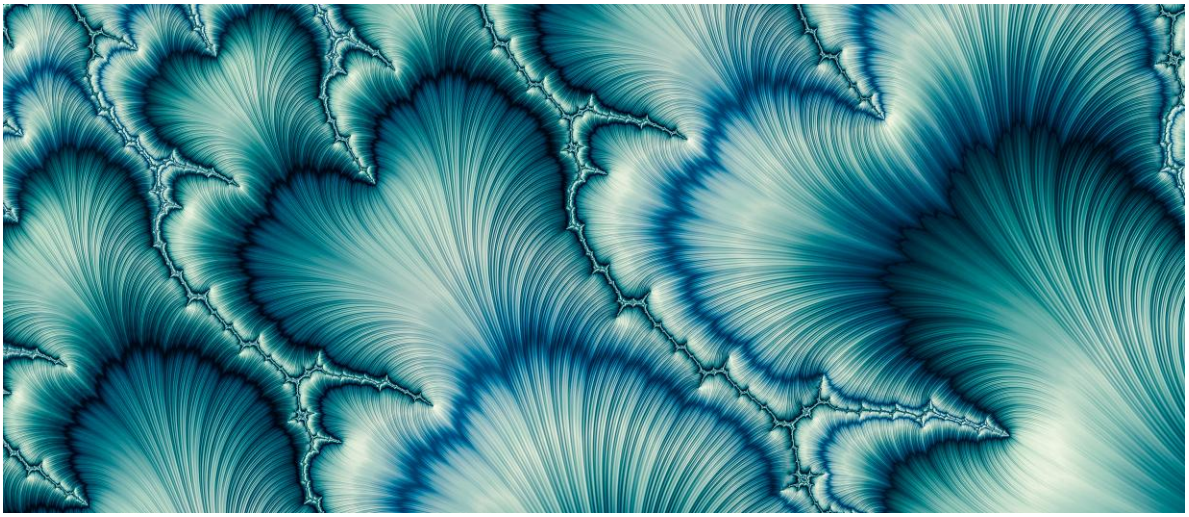
Summary: On **29 September 2026**, the US Court of Appeals for the Third Circuit upheld a ruling that ROSS Intelligence infringed Thomson Reuters' copyrights by using Westlaw's editorial headnotes to train its AI-powered legal research tool. The court found that the headnotes were sufficiently original to qualify for copyright protection and that ROSS's use did not constitute fair use, emphasising the commercial nature of the use and the fact that ROSS intended to compete directly with Westlaw. The court characterised the dispute as an "ordinary" copyright case, distinguishing it from cases involving generative AI.

Why it matters: The decision reinforces that established copyright principles apply to AI development and that using protected content to train AI systems may not qualify as fair use, particularly where the resulting product directly competes with the rights holder. However, the ruling is fact-specific and does not resolve the broader question of whether training generative AI models on copyrighted works constitutes fair use. It also highlights the importance of lawful data sourcing, appropriate licensing arrangements and due diligence when engaging third-party vendors for AI training.

EUIPO: First Customs Enforcement Application for a Craft and Industrial Geographical Indication

Summary: On **24 September 2026**, the EUIPO announced the filing of the first Application for Action (AFA) for a craft and industrial geographical indication (CIGI), concerning *Porcelaine de Limoges*, the first CIGI registered under the EU's new protection system. Filed through the EUIPO's IP Enforcement Portal (IPEP), the application enables customs authorities to take action against suspected counterfeit products at the EU's external borders, marking an important step in the practical enforcement of this new intellectual property right.

Why it matters: This milestone demonstrates that CIGI protection can extend beyond registration to practical border enforcement. It provides producers with an additional tool to safeguard product authenticity, reputation and traditional know-how, while strengthening the EU's fight against counterfeiting.



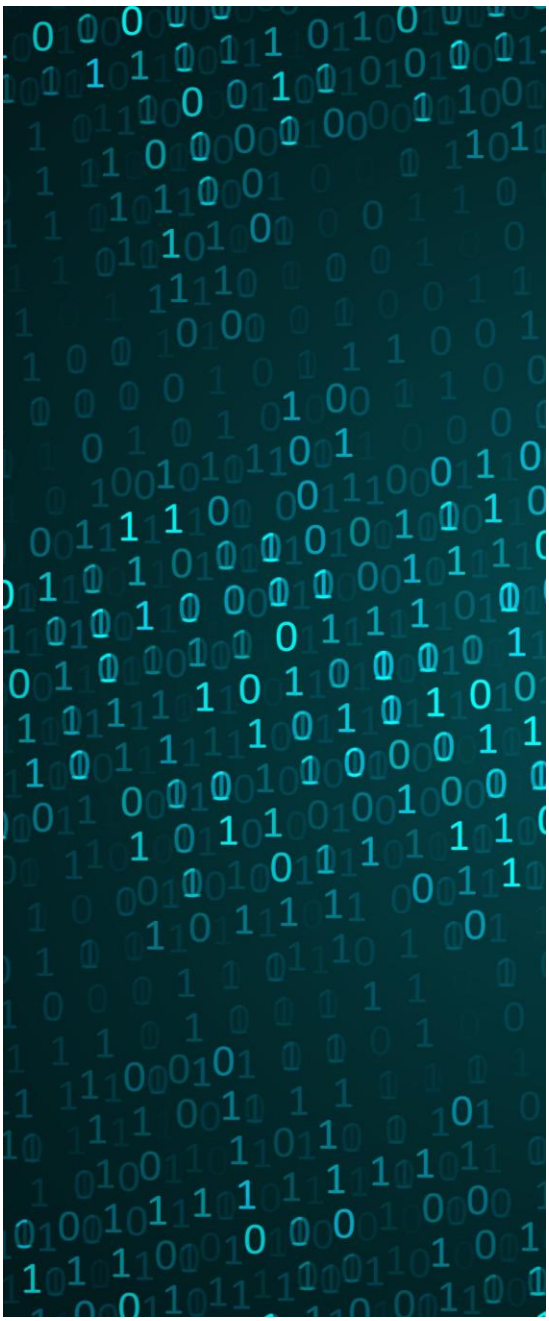
ENISA Publishes Threat Landscape 2026: DDoS and Ransomware Dominate EU Cyber Activity in 2025

ENISA's latest Threat Landscape report, published in **September 2026**, reviews more than 8,000 cyber incidents that affected the EU in 2025.

DDoS attacks and unauthorized access accounted for most of the activity, with phishing and the exploitation of software vulnerabilities as the main ways in. Most DDoS attacks came from hacktivists and were organized under operation-labelled campaigns. Ransomware and other financially motivated attacks were less frequent but did the most harm. Ransomware groups are increasingly stealing data for extortion instead of encrypting systems. ENISA notes that in the EU, GDPR and incident reporting obligations are likely to push victims toward paying the ransom.

Attacks on suppliers and service providers had some of the widest effects. As per example, a single ransomware attack on a single Swedish IT supplier affected around 200 municipalities. Another disrupted check-in at several EU airports. State-linked groups, mainly from Russia and China, focused on espionage. Throughout 2025, they kept up their targeting of central and local government bodies and diplomatic missions. In this context, it is crucial to highlight that many of the threats targeted EU entities outside of the EU territory. Several of these groups also targeted EU manufacturers, especially in the defense industry. ENISA considers it plausible that part of this activity aimed at the theft of intellectual property, either to evade sanctions or to gain a

ENISA Publishes Threat Landscape 2026: DDoS and Ransomware Dominate EU Cyber Activity in 2025



competitive edge in international markets. Public administration was the most targeted sector, followed by business services (including legal and consultancy firms), transport, manufacturing and finance. Attackers are making growing use of AI to work faster and on a larger scale.

Why it matters: ENISA expects cybercrime to remain the most serious threat to business continuity in the EU. A single breach at a software or service provider can now spread to many of its customers. As a single breach at a supplier can now spread across many customers, third-party and supply-chain risk deserves close attention. Companies should confirm their NIS2 status, keep their incident response procedures current, and prepare for more AI-enabled attacks.

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