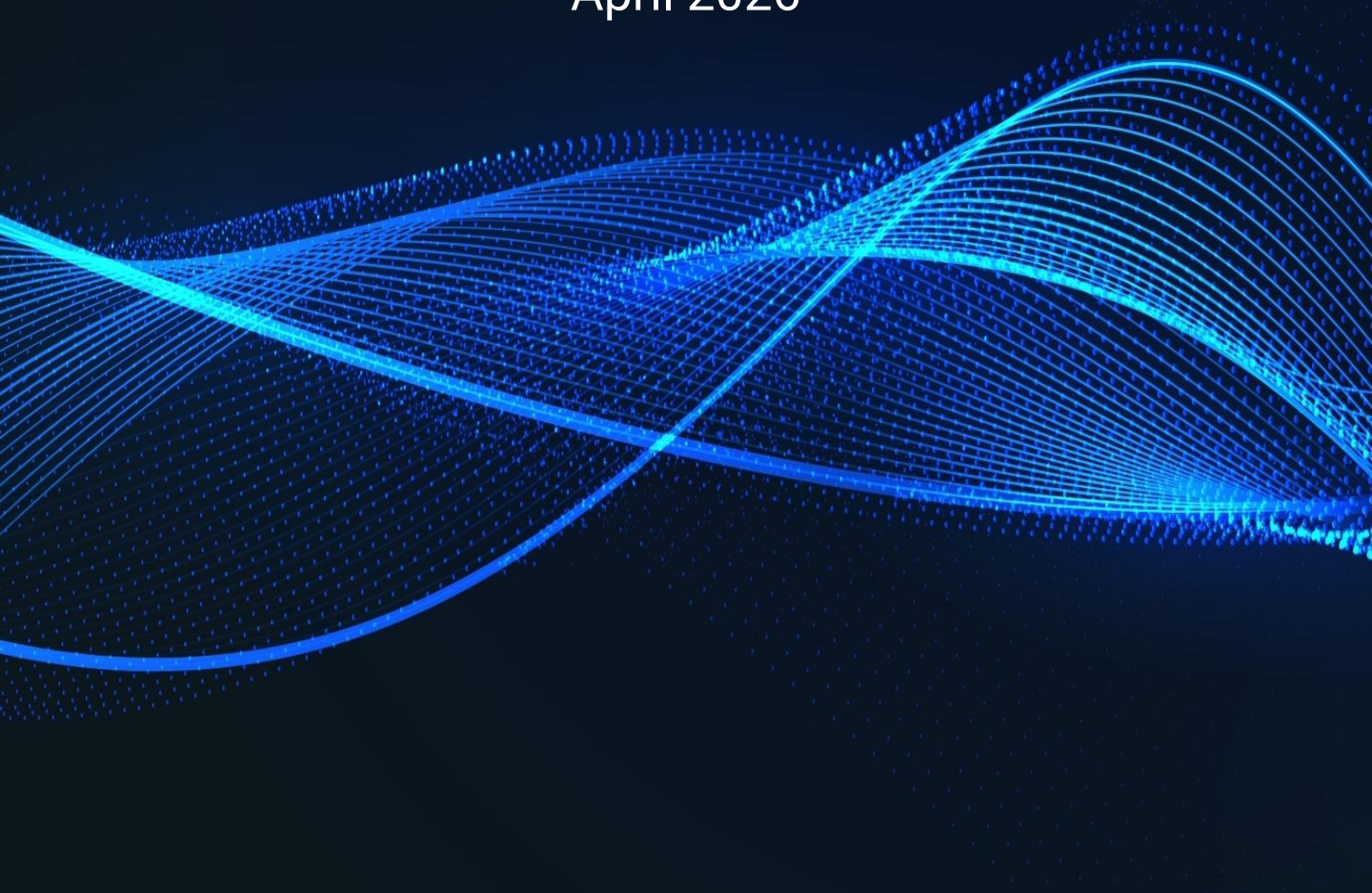


# Data Protection, AI & Cybersecurity

*Brief*

April 2026



## *At a glance*

---

EDPB Adopts Harmonised DPIA Template

€1.25 Million Fine Against ITA Airways and Alitalia for Unlawful Employee Data Transfer

Social Media Ban for Minors in Greece

EDPB Scientific Research Guidelines

Cybersecurity incident affecting Europa.eu

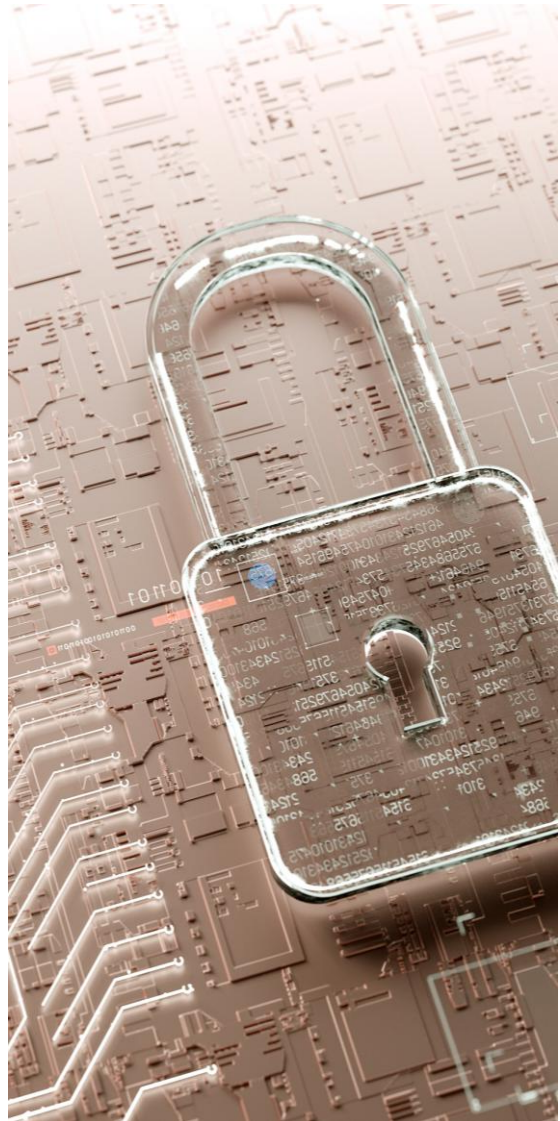
AI Traffic Enforcement in Greece

30 Years of the EU Trade Mark System

DSA Gets IP Boost Through New EUIPO Collaboration

# EDPB Adopts Harmonised DPIA Template and Launches Public Consultation

In line with its Helsinki Statement to make GDPR compliance easier and strengthen consistency across Europe, the European Data Protection Board (EDPB) adopted, on **14 April 2026**, the first harmonised template for Data Protection Impact Assessments (DPIAs) under the GDPR. The template is accompanied by an explainer document providing concise explanations for completing it effectively, breaking down key concepts in simple language and addressing possible questions and knowledge gaps controllers might have.



# EDPB Adopts Harmonised DPIA Template and Launches Public Consultation

A DPIA is a process required in situations where processing is likely to result in a high risk to individuals, describing how personal data will be processed, assessing whether the processing is necessary and appropriate, and identifying and reducing risks to individuals' rights and freedoms. The EDPB template has been conceived to support organisations step by step through this process, with predefined fields that prompt complete and structured responses.

While use of the template is not mandatory for controllers to choose, the template is subject to public consultation until **9 June 2026**. Following the consultation, all national Data Protection Authorities will

initiate the necessary steps to adopt the template either as their sole standard or as a template to which national specific templates will align.

**Why it matters:** For organisations operating across multiple EU jurisdictions, the harmonised DPIA template has the potential to significantly reduce compliance burdens by ending the era of divergent national expectations. DPOs and compliance professionals should familiarise themselves with the template, as it shall become the de facto European standard once finalised.

# €1.25 Million Fine Against ITA Airways and Alitalia for Unlawful Employee Data Transfer



On **4 March 2026**, the Italian Data Protection Authority imposed administrative fines amounting to a total of €1.25 million (€1 million on ITA Airways and €250,000 on Alitalia) for the unlawful processing of employees' personal data during the transition between the two airlines.

The investigation was initiated following a complaint filed in July 2023 by a trade union representative who reported that Alitalia had transferred employee personnel files to ITA Airways without an adequate legal basis.

# €1.25 Million Fine Against ITA Airways and Alitalia for Unlawful Employee Data Transfer

The Italian DPA found that Alitalia had made available to ITA Airways the personal files of Aviation department employees through a shared electronic folder, allowing ITA to access employees' data before those employees had even submitted applications for positions at ITA.

The key violations found by the Italian DPA concerned the absence of a valid legal basis for the data transfer, the failure to provide adequate privacy notices to the data subjects, and an inadequate response to data access requests submitted by the affected employees.

**Why it matters:** This decision underscores that even in complex corporate restructuring and transition scenarios, the sharing of employees' personal data between companies must comply fully with GDPR principles of lawfulness, fairness, and transparency.

# Social Media Ban for Minors: The Greek Regulation and the Global Debate on Protection

Greece announced, on **8 April 2026**, a new legislative intervention to ban social media access for minors, reflecting a broader global shift from general concern to concrete regulation on the impact of social media platforms on children and adolescents. The ban will apply to children younger than 15 years old and the proposal of the Greek Government includes the mandatory use of the age verification mechanism for all platforms serving users under 15 and the obligation for six-monthly age re-verification by platforms. The legislation is expected to come into force on **1 January 2027**.

The approach to minors' access to social media platforms varies across jurisdictions, while EU has not yet adopted a horizontal ban on social media for minors.

Indicatively, Australia has adopted one of the first and strictest models regarding the access of minors to social media, setting the age limit at 16.

**Why it matters:** The Greek regulation represents a significant step in the evolving international debate on protecting minors from the harmful effects of social media. At the same time, it creates challenges regarding its implementation, related to the technical reliability of age-verification mechanisms and the compliance of the platforms themselves.



# EDPB Scientific Research Guidelines

On **15 April 2026**, the European Data Protection Board (EDPB) published draft Guidelines 1/2026 offering long-awaited guidance on how data protection rules apply to scientific research across academia, the public sector, and industry, including AI-driven research and large-scale data processing. The key message is that data protection rules are not intended to obstruct scientific research, however only research that is genuinely scientific can benefit from research-specific provisions, and only where appropriate safeguards are in place.

The Guidelines outline indicative factors for determining what constitutes scientific research. They also explain how personal data may be lawfully reused for

scientific research or for different research purposes, and how organizations can rely on legal bases such as consent or legitimate interests. Furthermore, they emphasize the importance of ongoing transparency with research participants, clarify when individual notification may be considered disproportionate, and provide guidance on how the roles of controllers and processors should be assessed in research contexts.

**Why it matters:** Organizations involved in scientific research are encouraged to review their governance framework and data use practices in light of the draft Guidelines, which are expected to shape supervisory authority enforcement once finalized.

# Cybersecurity incident affecting Europa.eu

On **27 March 2026**, the European Commission issued a press release disclosing a cybersecurity incident affecting the cloud infrastructure hosting its Europa.eu web platform. According to the statement, swift containment and mitigation measures were taken following detection of the incident, ensuring that the availability of the Europa websites was maintained and that the Commission's internal systems remained secure. The statement also notes that relevant Union entities are being notified as the assessment of the incident continues.

CERT-EU later published a detailed overview of the incident, describing it as a supply-chain compromise linked to Amazon Web Services (AWS) cloud infrastructure.

CERT-EU was formally notified in line with the applicable EU cybersecurity framework and provided operational support to the Commission throughout the response process.

The incident is set against the wider backdrop of the EU's strengthened cybersecurity architecture, including the Cybersecurity Regulation, the NIS2 Directive, and the Cyber Solidarity Act. Together, these instruments aim to enhance prevention, detection, cooperation, and collective response to cyber threats, which widely affect diverse stakeholders across the EU, including EU institutions.

# AI Traffic Enforcement in Greece: Data Protection Implications

AI-enabled traffic enforcement has recently been introduced in Greece, where smart cameras equipped with automated image recognition technology are used to monitor roads and public transport lanes. The system detects traffic violations such as illegal use of bus lanes, identifies vehicles through license plate recognition, and automatically triggers the issuance of fines, which are then communicated digitally to vehicle owners via Gov.gr platforms.

Following its rollout in 2026, the system has already started issuing fines based on these automated detections, a process that has been in effect since **30 March 2026**.

This development is significant under the General Data Protection Regulation because it involves large-scale, AI-driven processing of vehicle and potentially personal data, as well as automated decision-making that produces legal effects in the form of fines.



# AI Traffic Enforcement in Greece: Data Protection Implications

The initiative raises several data protection considerations under the General Data Protection Regulation, including the need for a clear legal basis for large-scale automated processing of vehicle and potentially personal data, strict purpose limitation, and compliance with data minimization and storage limitation principles. It also triggers requirements around transparency, particularly regarding the use of AI-enabled cameras and automated fine issuance through Gov.gr systems, as well as safeguards against fully automated decision-making, accuracy risks, and the need for human oversight and effective challenge mechanisms. Given the integration of multiple public systems, questions also

arise around controller responsibility, data sharing arrangements, and the need for a Data Protection Impact Assessment, all of which fall under scrutiny by the Hellenic Data Protection Authority.

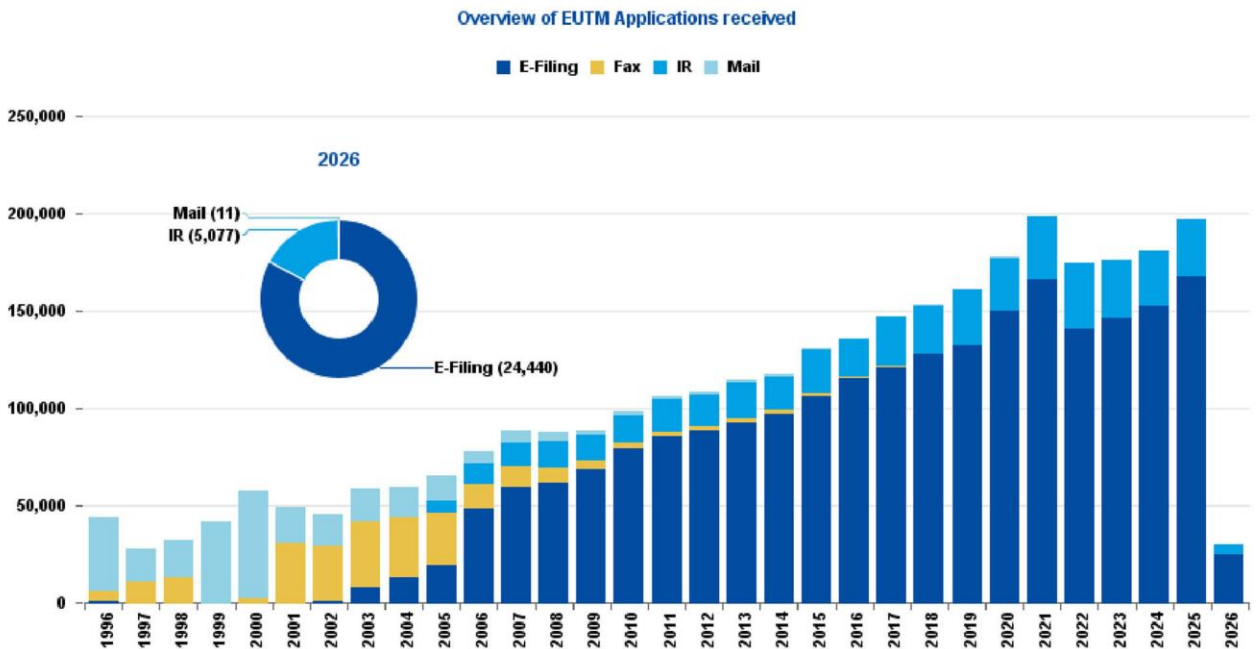
**Why it matters:** This matters because non-compliance could undermine the validity of fines, trigger regulatory action from the Hellenic Data Protection Authority, and lead to complaints or legal challenges. It may also cause delays, additional costs, and reputational harm, while reducing public trust in the use of AI-based enforcement systems.

# 30 Years of the EU Trade Mark System

The European Union Intellectual Property Office (EUIPO) marks 30 years of the EU trade mark system, which began in 1996. Since its launch, the system has received more than 3.2 million trade mark applications, making it one of the most widely used IP registration systems globally. Annual filings have grown significantly over time—from around 43,000 in 1996 to nearly 200,000 per year in recent years—reflecting sustained demand for EU-wide brand protection. The milestone highlights the evolution of a centralised system that allows businesses to secure protection across all EU Member States through a single application.

**Why it matters:** This milestone underscores the increasing importance of intellectual property as a core business asset in the EU economy. The scale and growth of filings show that companies rely heavily on the EU trade mark system to support cross-border trade, brand expansion, and market exclusivity. It also reflects the efficiency and attractiveness of a harmonised EU-wide registration mechanism, which reduces legal fragmentation and facilitates commercial activity across the internal market.

# 30 Years of the EU Trade Mark System



<https://www.euipo.europa.eu/en/news/eu-trade-mark-system-marks-30-years-with-more-than-3-2-million-applications-filed>

# DSA Gets IP Boost Through New EUIPO Collaboration

European Commission and EUIPO signed a new cooperation agreement on **2 April 2026**, aimed at strengthening the enforcement of intellectual property rights online under the framework of the Digital Services Act.

The agreement enhances coordination between the two institutions to better detect, address, and prevent online IP infringements, particularly on digital platforms that facilitate the distribution of counterfeit goods or infringing content. It is intended to improve information exchange, support more effective monitoring tools, and reinforce operational cooperation so that enforcement actions can be more consistent and timely across the EU.

**Why it matters:** This matters because it strengthens the EU's ability to address IP infringement in the digital space, where enforcement has traditionally been fragmented and slow. By integrating EUIPO expertise into the enforcement ecosystem of the Digital Services Act, the EU is moving toward more coordinated and proactive platform oversight, which can increase compliance pressure on online intermediaries and improve rights holders' ability to act quickly against infringing content.

## About Us

**Dimitra Karampela, Senior Associate**  
[d.karampela@karatza-partners.gr](mailto:d.karampela@karatza-partners.gr)

**Panagiotis Kontizas, Associate**  
[p.kontizas@karatza-partners.gr](mailto:p.kontizas@karatza-partners.gr)

**Georgia Patiri, Associate**  
[g.patiri@karatza-partners.gr](mailto: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](mailto:mail@karatza-partners.gr)

[dataprotection@karatza-partners.gr](mailto:dataprotection@karatza-partners.gr)