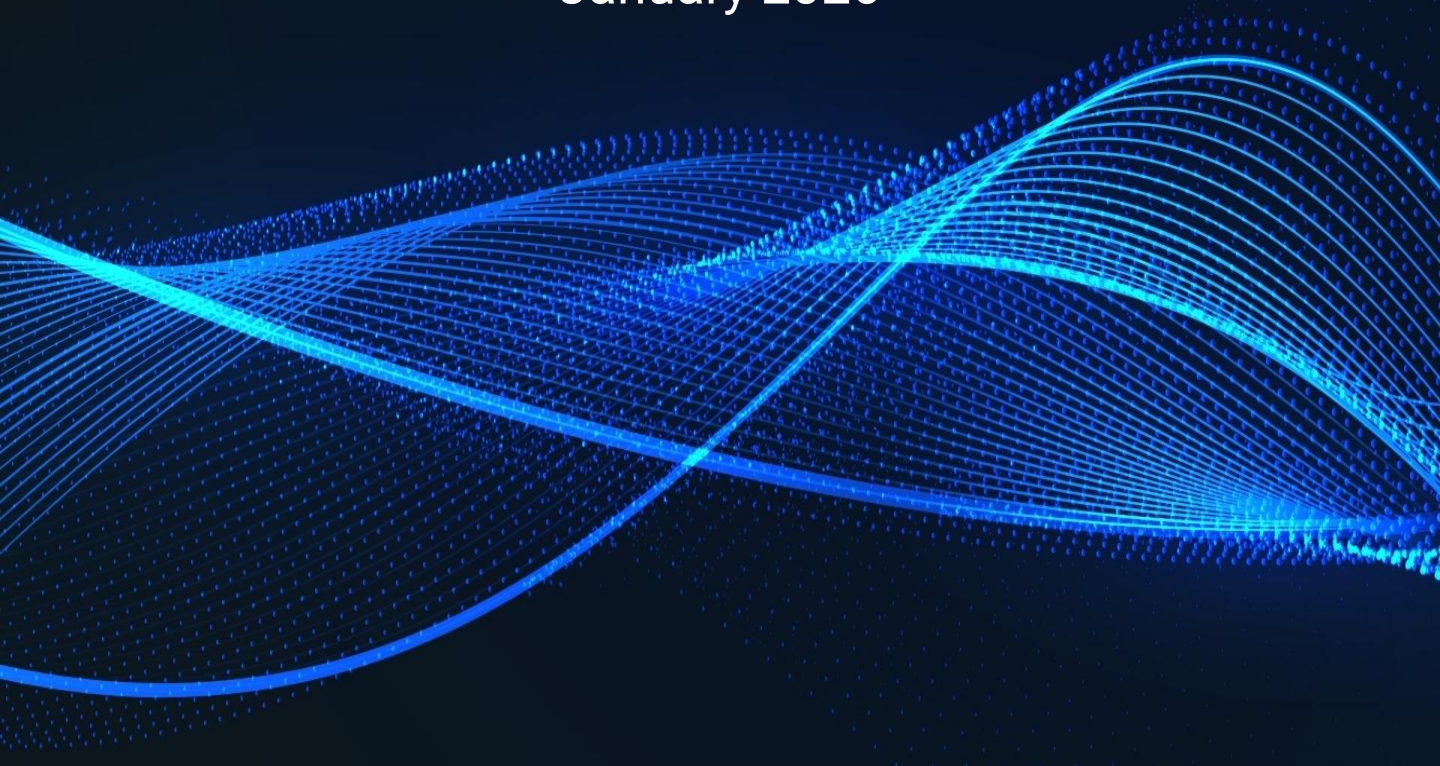
KARATZAS & PARTNERS

Data Protection, AI & Cybersecurity

Brief

January 2026



KARATZAS & PARTNERS

At a glance

New EDPB Recommendations No. 2/2025 on E-commerce User Account Requirements

Recent fines and decisions by the HDPA

EDPB-EDPS Joint Opinion 1/2026 on the Digital Omnibus on AI

First EC Draft Code of Practice on Transparency of AI-Generated Content

Publication of Greece's National Cybersecurity Strategy for 2026–2030, setting national priorities for cybersecurity resilience

Recent Developments abroad

New EDPB Recommendations No. 2/2025 on E-commerce User Account Requirements

Overview

The European Data Protection Board (EDPB) has recently adopted comprehensive recommendations addressing when e-commerce websites may legally require users to create online accounts before making purchases or accessing offers. Public consultation is open until February 12th, 2026.

Key takeaways

- ✓ **Mandatory accounts are rarely justified:**
  The EDPB highlights that, in most cases, requiring account creation violates GDPR as the necessity test under Articles 6(1)(b), (c), and (f) is typically not met. For instance, mandatory accounts cannot be justified for one-time sales of goods or services, order tracking and management, fraud prevention, after-sales services etc.
- ✓ **Security considerations:**
  Contrary to industry claims, the EDPB notes that mandatory accounts may actually increase security risks through data breaches, password reuse, account takeovers etc.
- ✓ **Recommended solution:**
  Guest checkout should be the default option. The EDPB strongly advocates offering users a choice between creating an account or purchasing as a guest, noting that guest mode is the most privacy-protective option and most aligned with data protection by design principles under Article 25 GDPR.

Overall impact

The guidance signals a stricter GDPR interpretation of mandatory account creation in e-commerce and encourages the use of guest checkout as the privacy-friendly default.

Recent fines and decisions by the Hellenic Data Protection Authority (HDPA)

Complaints against Energy Supplier Companies

The HDPA recently examined multiple complaints against an energy supplier company regarding delays and failure to satisfy data subjects' rights and conducted ex officio examination of the company's policy for data subjects' rights management. The HDPA (Decision No. 42/2025) imposed a fine of **30.000 EUR** based on infringements of access rights while ordering the company to reorganize its internal procedures (including staff training) as an organizational security measure and to evidence conformity within six (6) months. Also, in another decision, the HDPA (Decision No. 43/2025) imposed administrative fines of 115.000 EUR on the energy supplier company and 35.000 EUR and 15.000 EUR to each partner. In this last case, following several data subjects' complaints regarding the conduct of phone calls for the promotion of products and services of an energy supplier company, the HDPA investigated the relevant activities of the company as well as two partner companies conducting promotional calls (call centers). The Authority found that data was collected and processed for the promotion of products and services through telephone calls in violation of the provisions of the applicable legislation and identified deficiencies in the control and security measures of the partner companies.

“Smart Policing” system: **Law enforcement technologies and biometrics**

The HDPA recently examined the “Smart Policing” system of the Hellenic Police (Decision No. 45/2025), developed by a third-party provider, which involves the processing of biometric data (facial images and fingerprints) through mobile smart devices for the recognition and identification of individuals under investigation. The Authority found that the “Smart Policing” system deployment lacked a sufficient legal basis under the applicable legal framework, while the DPIA was not conducted in time. In this respect, the HDPA issued a corrective warning and advised against activation of the system, given that under the current legal framework the operation of the system would constitute unlawful processing of personal data.

EDPB-EDPS Joint Opinion 1/2026 on the Digital Omnibus on AI

The EDPB and EDPS adopted Joint Opinion 1/2026 on January 20, 2026, regarding the European Commission's proposal to simplify the implementation of the AI Act. While supporting the general objective of reducing administrative burden for businesses and administrations, the bodies emphasize that this must not lower the protection of fundamental rights, particularly data protection. The Opinion raises key concerns including:

a) the need to limit the extended legal basis for processing special categories of personal data for bias detection to cases with sufficiently serious risks,

b) maintaining provider registration obligations for AI systems claimed to be non-high-risk,

c) ensuring competent data protection authorities are properly involved in EU-level AI regulatory sandboxes,

d) clarifying cooperation between the AI Office and data protection authorities,

e) maintaining AI literacy obligations for providers and deployers rather than transferring them solely to the Commission and Member States and

f) concerns about postponing the implementation timeline for high-risk AI system rules. The Joint Opinion provides detailed technical recommend-dations across these seven areas to strengthen the proposal while maintaining robust safeguards for individuals' rights in the rapidly evolving AI landscape.

First EC Draft Code of Practice on Transparency of AI-Generated Content

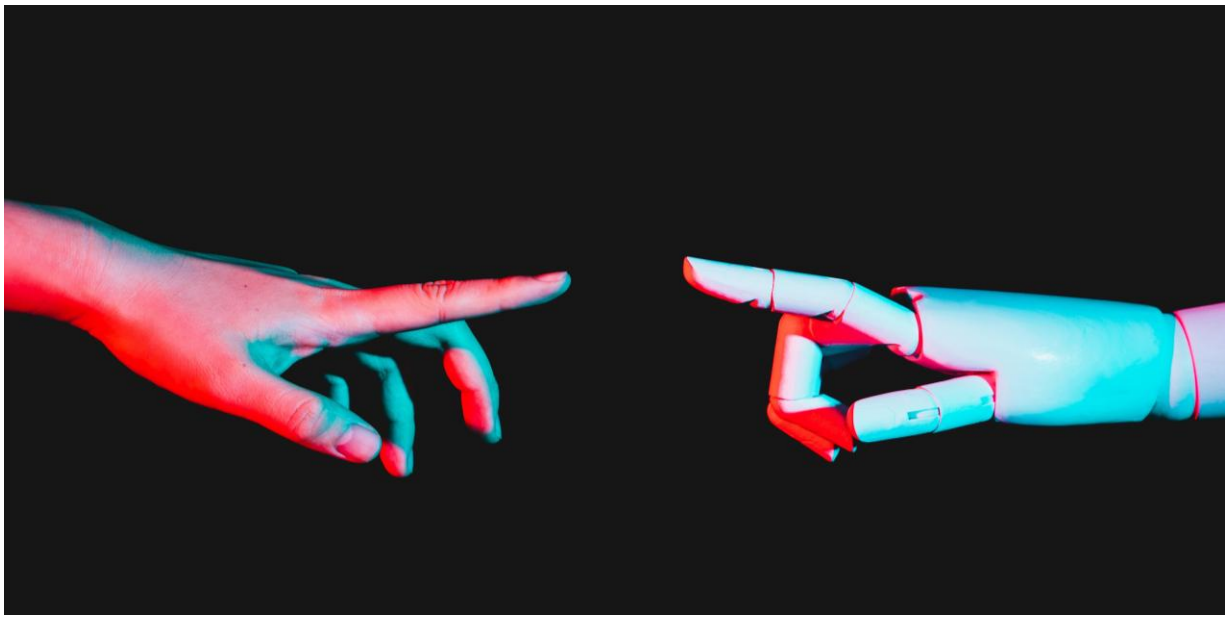
Overview

The European Commission (EC) released, on 17 December 2025, the First Draft Code of Practice on Transparency of AI-Generated Content (Code) under the AI Act. This document establishes rules for both AI system providers and deployers to ensure transparent marking and disclosure of AI-generated/manipulated content across the EU.

Public consultation is still open, after which a second draft and a final version are expected in 2026 ahead of the rules becoming applicable on 2 August 2026.

Key Takeaways

The Code is structured in two main sections:



Section 1

Rules for marking and detection of AI-generated and manipulated content (for generative AI system providers), which include, inter alia, the following:

- Multi-layered marking approach required - no single technique is sufficient;
- Detection mechanisms provided free of charge to users and third parties;
- Need for effective, reliable, robust, and interoperable technical solutions.

Section 2

Rules for labelling deepfakes and AI-generated and manipulated text (for AI system deployers), which include, inter alia, the following:

- Common taxonomy distinguishing between "fully AI-generated" and "AI-assisted" content;
- Standardized EU- wide icon system;
- Accessibility compliance requirements;
- Appropriate disclosure for creative works not hampering artistic enjoyment.

Overall impact

The Code strengthens trust, accountability, and transparency in the AI content ecosystem. While non binding, adherence to the Code may serve as evidence of good faith compliance and reduce regulatory risk for participants.

Greece's National Cybersecurity Strategy 2026–2030

Greece's new Cybersecurity Strategy, issued in December 2025, identifies crucial cybersecurity risks and challenges, providing a comprehensive framework for the effective management of cybersecurity threats in Greece, stressing convergence of cybersecurity, data protection, and broader digital regulation (NIS 2, DORA, GDPR, AI Act, etc.). The Strategy flags critical success factors, including a stable, comprehensive and adaptable regulatory framework, as well as technological readiness and investment in resilient and interoperable infrastructure.

The **main strategic goals** of the new Cybersecurity Strategy include capacity building and awareness, strengthening of the national, European and international cooperation, a governance system of cybersecurity and the strengthening of regulatory compliance and upgrading policies.

Developments abroad

❖ **Sweden**

On 18 December 2025, the Court of Justice of the European Union (CJEU) ruled (C-422/24) that when data obtained by means of **body cameras** are collected directly from the data subject, that data subject must be **provided with certain information immediately**. The most important information may be indicated on a warning sign, while other information may be provided in an easily accessible place. The Swedish court hearing that dispute asked the Court of Justice to interpret the GDPR. The Court replies that, since data obtained by means of body cameras are collected directly from the data subject, that data subject must be provided with certain information immediately.

❖ **United Kingdom**

On 19 December 2025, the Commission renewed the two 2021 **adequacy** decisions for the free flow of personal data with the United Kingdom. The decisions ensure that personal data can continue flowing freely and safely between the European Economic Area (EEA) and the United Kingdom, as the UK legal framework contains data protection safeguards that are essentially equivalent to those provided by the EU. The new decisions are subject to a sunset clause of six years, running until **27 December 2031**, with the possibility to be renewed.

❖ **New York (USA)**

In December 2025, New York enacted two laws that will impact the use of AI-generated human images (The law amends **Section 396-b of New York's General Business Law, S.8420-A / A.8887-B**). The first requires a conspicuous disclosure where synthetic performers are used in advertising, and the second expands the right of publicity for deceased personalities to encompass the use of digital replicas for commercial purposes. The law **requires advertisements that use "synthetic performers"** (AI-generated digital images or likenesses intended to resemble humans) to include a **conspicuous disclosure** that such performers are not real people. Civil penalties apply for non-compliance: $1,000 for a first violation and $5,000 for subsequent violations. The law's effective date is June 9, 2026.

In **December 2025**, *The New York Times* and *The Chicago Tribune* filed separate **copyright infringement lawsuits** against **Perplexity AI** in the **U.S. District Court for the Southern District of New York**, alleging that the AI-powered answer engine used their news content without authorization. The complaints claim that Perplexity's system copied, distributed, and displayed millions of copyrighted articles to train and operate its generative AI, including through retrieval-augmented generation, and that this use violated the newspapers' copyrights. These lawsuits are part of a growing wave of legal challenges by major publishers seeking to hold AI companies accountable for the unlicensed use of journalistic content.

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