KARATZAS & PARTNERS

Data Protection, AI & Cybersecurity

Brief

March 2026

KARATZAS & PARTNERS

At a glance

EDPB CEF 2026: Transparency and information obligations under the GDPR

EDPB–EDPS Joint Opinion on the European Biotech Act

CJEU: A First-Time Access Request Can Be Abusive

Guidelines on Good Law-Making for Personal Data

Vodafone Fined for Breaches of Data Subject Rights

The First EU Case on Generative AI and Copyright

The Jo Malone Name Dispute

EDPB–EDPS Joint Opinion on the Cybersecurity Act 2

European Parliament Resolution on Copyright and Generative AI

Council's Mandate on Streamlining Rules on AI

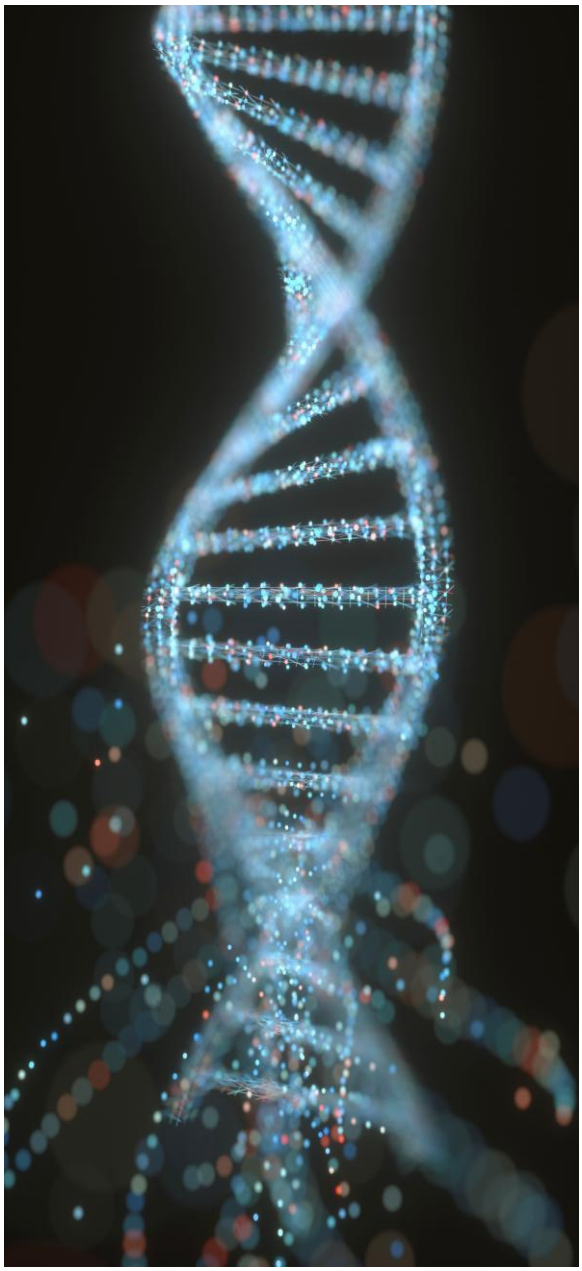
EDPB launches its Coordinated Enforcement Action for 2026 on transparency and information obligations under the GDPR

On 19 March 2026, the EDPB formally launched its Coordinated Enforcement Framework (CEF) for 2026 focused on compliance with the transparency and information obligations under the GDPR (Articles 12–14). Each of the 25 participating European Data Protection Authorities (DPAs), including Greek DPA, will examine whether controllers are meeting their obligations to inform data subjects about how their personal data is processed. In this respect, DPAs will contact controllers from a range of sectors, either by opening formal investigations or through fact-finding exercises, which may themselves generate follow-up enforcement activity. In the second half of 2026, participating authorities will pool their findings and submit a consolidated report to the EDPR informing targeted follow-up action at both national and EU level.

Why it matters: Privacy notices, even if technically complete in principle, may still fall short if they are inaccessible or if they provide unclear or confusing information to data subjects. Under the GDPR, the standard is not merely that information about data processing activities is provided; it must also be concise, intelligible, and easily accessible by data subjects. For organizations with cross-border operations, the risk is amplified, since parallel investigations by multiple DPAs are possible under the CEF model. Controllers should regularly audit their privacy notices, checking both accuracy and usability across all relevant channels.

EDPB–EDPS Joint Opinion 3/2026: Safeguarding Personal Data in the European Biotech Act

Adopted on 10 March 2026, Joint Opinion 3/2026 of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) comments on the Commission's proposed European Biotech Act, which seeks to strengthen EU biotechnology and biomanufacturing sectors. The EDPB and EDPS broadly welcome its objectives, and in particular the drive to reduce regulatory fragmentation and promote responsible AI use in health. However, they also make a series of targeted recommendations to ensure the simplification agenda does not quietly erode the data protection standards that apply to personal data related to health.



EDPB–EDPS Joint Opinion 3/2026: Safeguarding Personal Data in the European Biotech Act

The bulk of the Opinion concerns the **amendments to the Clinical Trials Regulation (CTR)**. The Proposal seeks to establish a single legal basis (Article 6.1.c GDPR) for processing by sponsors and investigators across the EEA, which the EDPB and EDPS support. Key recommendations include that:

1. the proposed Article 93(1) and (2) CTR be amended to require processing only "where necessary" for the listed purposes;
2. the 25-year minimum retention period under Article 58 CTR be expressly limited to the clinical trial master file (rather than all personal data in a trial);
3. the further processing provision (Article 93(6) CTR) be reframed to identify Article 6(1)(e) GDPR as its legal basis and narrow the overly broad purpose of "fostering the innovation capacity of European medical research";
4. the roles of sponsors and investigators as sole or joint controllers be spelled out directly in the legislation.

Why it matters: For sponsors, investigators, and CROs, the Opinion's call for clarity on joint controllership, retention scopes, and further processing purposes is directly relevant to compliance planning.

CJEU Rules That a First-Time Access Request Can Be Abusive (Case C-526/24)

In a judgment delivered on 19 March 2026, the Court of Justice confirmed in Case C-526/24 (*Brillen Rottler*) that a data subject's first-ever request for access to personal data under Article 15 GDPR can, in certain circumstances, already be characterised as "excessive" and refused, even though the GDPR generally limits the "excessive request" ground to *repeat* requests. The case arose from an access request submitted from an Austrian individual who subscribed to the newsletter of a German optician, just 13 days after subscribing, and, when the request was refused, claimed compensation for non-material damage. The controller refused on the basis that, according to publicly available information, the said individual had systematically subscribed to newsletters of various companies before submitting access requests and subsequent compensation claims.

CJEU Rules That a First-Time Access Request Can Be Abusive (Case C-526/24)

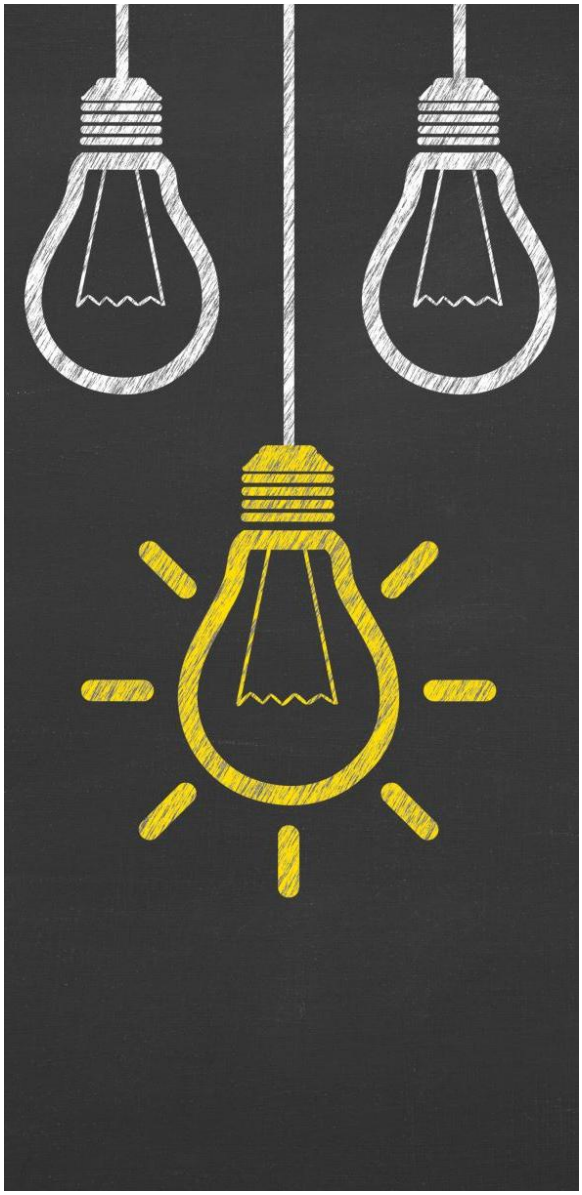
The Court held that even a first request may be abusive where the controller demonstrates that, despite formal compliance with GDPR's requirements, the request was made not to verify the lawfulness of processing but with the intention of artificially creating the conditions for a compensation claim under Article 82 GDPR. Relevant indicators include the following:

- the very short interval between provision and the access request;
- publicly available evidence of a systematic pattern of identical behaviour towards multiple controllers;
- the fact that the data was provided voluntarily.

As regards compensation claims, the Court added two important clarifications: a claimant must demonstrate that damage was *actually suffered*, and a data subject cannot recover compensation if their own conduct is the determining cause of the damage.

Why it matters: This ruling is a meaningful tool for controllers facing cases of access-request abuse, where access rights are used not to exercise genuine data subject rights but as a means to compensation litigation. The judgment confirms that a single request can be abusive if the surrounding circumstances reveal that litigation strategy, not transparency, was the real objective. Therefore, controllers should document evidence of systematic behaviour where it exists and keep records that allow them to demonstrate the motive behind a refusal.

Guidelines on Good Law-Making for Personal Data



On 10 March 2026, the Hellenic Data Protection Authority (HDPA) issued guidelines providing practical direction for drafting legislation involving personal data. The document emphasizes that laws must be necessary, proportionate, and aligned with core data protection principles such as transparency, purpose limitation, and security. It also stresses the importance of clearly defining key elements (e.g., purpose, data categories, retention periods, and safeguards) and consulting the Authority in higher-risk cases. Overall, the guidelines function as a checklist to ensure legislation incorporates data protection by design and complies with EU GDPR standards.

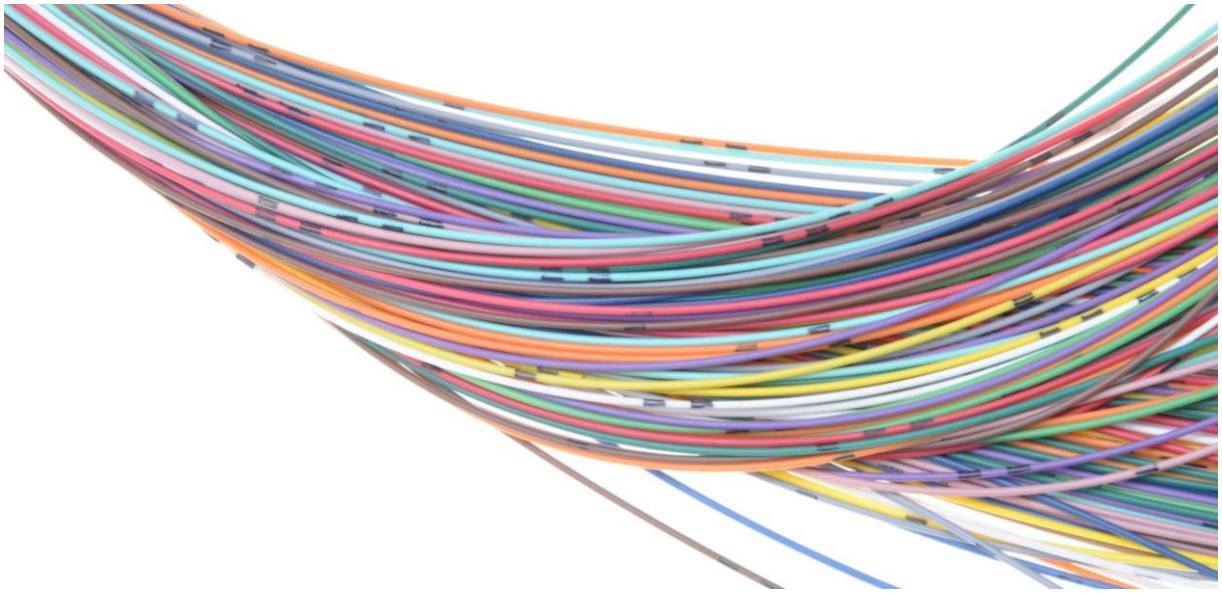
Vodafone Greece Fined €30,000 for Breaches of Data Subject Rights

The HDPA has issued Decision no. 2/2026, imposing significant penalties on telecommunications giant Vodafone for multiple violations of data subject rights under the GDPR.

Case Overview

The HDPA examined a complaint of a subscriber against Vodafone - Panafon Hellenic Telecommunications Company S.A., involving the following violations: (i) breach of the subscriber's right of access to recorded telephone calls related to technical issues reported to the company, (ii) violation of the right to restriction of processing, (iii) obstruction of the exercise of the right of access by the company, and (iv) provision of contradictory information regarding access request handling procedures. Following thorough investigation, the HDPA determined that Vodafone violated multiple GDPR provisions, specifically Articles 12 par. 1, 2, 3, 4, 15, and 18 and imposed a €30,000 administrative fine, reflecting the severity of the violations and the company's failure to properly facilitate the exercise of the data subject's rights. The HDPA also issued a binding order requiring Vodafone to implement appropriate technical and organizational measures to ensure proper and timely examination of data subject rights, including providing enhanced training to its representatives, and to submit documentation to the Authority within six (6) months of the notification of the decision.

Vodafone Greece Fined €30,000 for Breaches of Data Subject Rights



Why it matters

The ruling serves as a reminder to all data controllers that procedural delays, inadequate responses, and contradictory information regarding data subject rights will face serious regulatory consequences. Controllers are expected to identify deficiencies in a request promptly and inform the data subject clearly and within the required timeframe, rather than allowing delays that may lead to data loss through routine retention policies. Where there is a foreseeable risk of deletion, organizations must take timely steps to preserve the relevant data until the request is fully resolved. That being said, transparency, prompt communication and operational readiness are critical to compliance and to maintaining trust with customers in data-intensive industries.

The First EU Case on Generative AI and Copyright

In 2025, the case Like Company v. Google Ireland (C-250/25) became the first major dispute over generative AI to reach the Court of Justice of the European Union (CJEU). The case originated in Hungary, where a news publisher accused Google's AI chatbot, Gemini, of reproducing and summarizing its copyrighted articles without permission. The Hungarian court referred key questions to the CJEU, asking whether AI-generated responses that closely reflect protected content amount to copyright infringement under EU law—particularly as a form of unauthorized "communication to the public." The Court's decision, expected in the coming years, will be its first direct ruling on generative AI.

Why it matters: It's the first time the CJEU directly addresses generative AI. The CJEU's ruling could determine whether AI systems can be trained on publicly available content without explicit licenses or whether stricter permissions will be required. The outcome will shape not only how companies like Google build AI tools, but also how creators are protected in the digital age. In short, this case will help decide whether Europe becomes a restrictive or innovation-friendly environment for AI—and its impact could ripple far beyond the EU.

The Jo Malone Name Dispute

In March 2026, Estée Lauder Companies filed a lawsuit against British perfumer Jo Malone over her collaboration with Zara. The dispute stems from Malone's use of her own name in connection with fragrances created for Zara under her newer brand, Jo Loves. Estée Lauder argues that this violates the terms of a 1999 agreement, under which Malone sold her original brand, Jo Malone London, along with the commercial rights to her name. The company claims that phrases such as "Created by Jo Malone" could mislead consumers into believing the Zara fragrances are linked to its established brand.

Why it matters: This case raises a fundamental issue at the intersection of trademark law and personal identity: to what extent can someone be prevented from using their own name in business? The outcome could shape how brand acquisition agreements are interpreted, particularly in industries where personal reputation is central to commercial success. More broadly, it highlights the long-term implications of selling a brand—suggesting that ownership may extend beyond products and logos to include the very identity of its creator.

EDPB–EDPS Joint Opinion on the Cybersecurity Act 2

In their March 2026 joint opinion, the European Data Protection Board and the European Data Protection Supervisor support the EU's proposed Cybersecurity Act 2 and related updates to the NIS2 Directive, emphasizing the need for stronger and more harmonized cybersecurity across Member States. However, they caution that enhanced information-sharing and security measures must remain fully compliant with General Data Protection Regulation principles, particularly necessity, proportionality, and purpose limitation. The opinion ultimately stresses that cybersecurity and data protection should be developed in tandem, ensuring that increased security does not come at the expense of fundamental privacy rights.

Why it matters: This joint opinion highlights that, while the EU strengthens cybersecurity through frameworks like the NIS2 Directive, organizations must still fully comply with the General Data Protection Regulation, ensuring privacy is never compromised for security. It also signals rising compliance risk, as companies implementing cybersecurity measures involving personal data will face stricter oversight from the EDPB and EDPS.

European Parliament Resolution on Copyright and Generative Artificial Intelligence

On 10 March 2026, the European Parliament adopted a resolution and accompanying report titled "Copyright and Generative Artificial Intelligence – Opportunities and Challenges". The resolution is politically significant though not legally binding and signals how European Parliament aspires future EU legislation to address generative AI (GenAI) and copyright law interplay.

Key Recommendations

New Legal Framework and Licensing

- Establish an additional legal framework to clarify licensing rules for GenAI and to address potential infringements of current copyright law;
- Create a new licensing market for copyrighted material, including collective licensing agreements per sector, to ensure fair remuneration and restore bargaining power to rightsholders.

Transparency, Accountability and Rights Protection

- Require full transparency and fair terms regarding copyrighted content used in AI training;
- Enable rights holders to effectively exclude their works from AI training through standardized machine-readable formats;
- Establish the European Union Intellectual Property Office (EUIPO) as a trusted intermediary to manage opt-out mechanisms;

European Parliament Resolution on Copyright and Generative Artificial Intelligence

- Create rebuttable presumptions that copyrighted works have been used for AI purposes when transparency obligations are not met;
- Ensure rights holders, especially from the press and news media sector, have full control over digital use of their content;
- Protect against unauthorized use of copyrighted content for purposes beyond AI training (e.g., inference, retrieval-augmented generation).

Enforcement Measures

- Apply EU copyright law to all AI providers operating in the EU market, regardless of where training occurs;
- Bar non-compliant GenAI systems from EU operation;
- Establish clear labeling requirements for purely AI-generated content.

Future Actions

The Parliament calls on the Commission, among other things, to:

- Conduct urgent assessments of current copyright framework adequacy;
- Explore immediate solutions for fair remuneration of past unauthorized uses;
- Develop EU codes of practice for content labelling.

Why it matters

The resolution aims to balance promoting AI innovation with protecting creators' rights and ensuring fair compensation for the use of copyrighted content in the digital transformation era.

Council's Mandate on Streamlining Rules on Artificial Intelligence

The Council of the European Union has agreed its negotiating mandate on a proposal to streamline and simplify certain rules within the Artificial Intelligence Act (AI Act). This initiative forms part of the EU's broader "Omnibus VII" simplification agenda, which aims to reduce administrative burdens, enhance legal certainty, and strengthen EU competitiveness while safeguarding fundamental rights.

Core Purpose of the Mandate

The mandate supports a more proportionate and workable implementation of the AI Act, ensuring that obligations are applied only when the necessary technical standards, tools, and governance structures are in place. The Council broadly endorses the European Commission's proposal, while introducing targeted adjustments and additional safeguards.

Council's Mandate on Streamlining Rules on Artificial Intelligence

Key Elements

- **Delayed application of high-risk AI rules:** The Council introduces fixed application dates for high-risk AI systems rules:
  - 2 December 2027 for stand-alone high-risk AI systems.
  - 2 August 2028 for high-risk AI systems embedded in products.
- **Adjustment of implementation timelines:** The deadline for establishing national AI regulatory sandboxes is postponed to 2 December 2027, allowing national authorities additional preparation time.
- **Expanded prohibitions:** A new explicit prohibition is added for AI practices involving the generation of non-consensual sexual or intimate content, including child sexual abuse material.
- **Obligations for AI system registration:** Providers claiming exemptions from high-risk classification must still register their AI systems in the EU database for high-risk AI systems, reinforcing transparency and oversight.
- **Data protection safeguards:** The mandate reinstates the "strict necessity" standard for processing special categories of personal data when used for bias detection and mitigation, aligning AI governance with data protection principles.
- **Support for SMEs and small mid-caps (SMCs):** Certain regulatory exemptions initially designed for small and medium-sized enterprises are extended to small mid-cap companies, reducing compliance burdens.

Council's Mandate on Streamlining Rules on Artificial Intelligence

- **Clarification of the AI Office's competences:** The role of the AI Office is strengthened for supervising AI systems based on general-purpose AI models developed by the same provider, while clearly preserving national authority competences in sensitive areas such as law enforcement and financial institutions.
- **Commission guidance obligation:** The Commission is required to issue guidance to assist providers of high-risk AI systems, with the aim of minimizing compliance complexity.

Next Procedural Steps

Following the adoption of the mandate, the Council presidency will start negotiations with the European Parliament, with the objective of reaching a final agreement on the amended regulatory framework.

Why it matters

The Council's mandate seeks to balance innovation and competitiveness with legal certainty, fundamental rights protection, and effective enforcement. It reflects a political priority to ensure the AI Act is implementable in practice while maintaining the EU's leadership in trustworthy artificial intelligence.

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