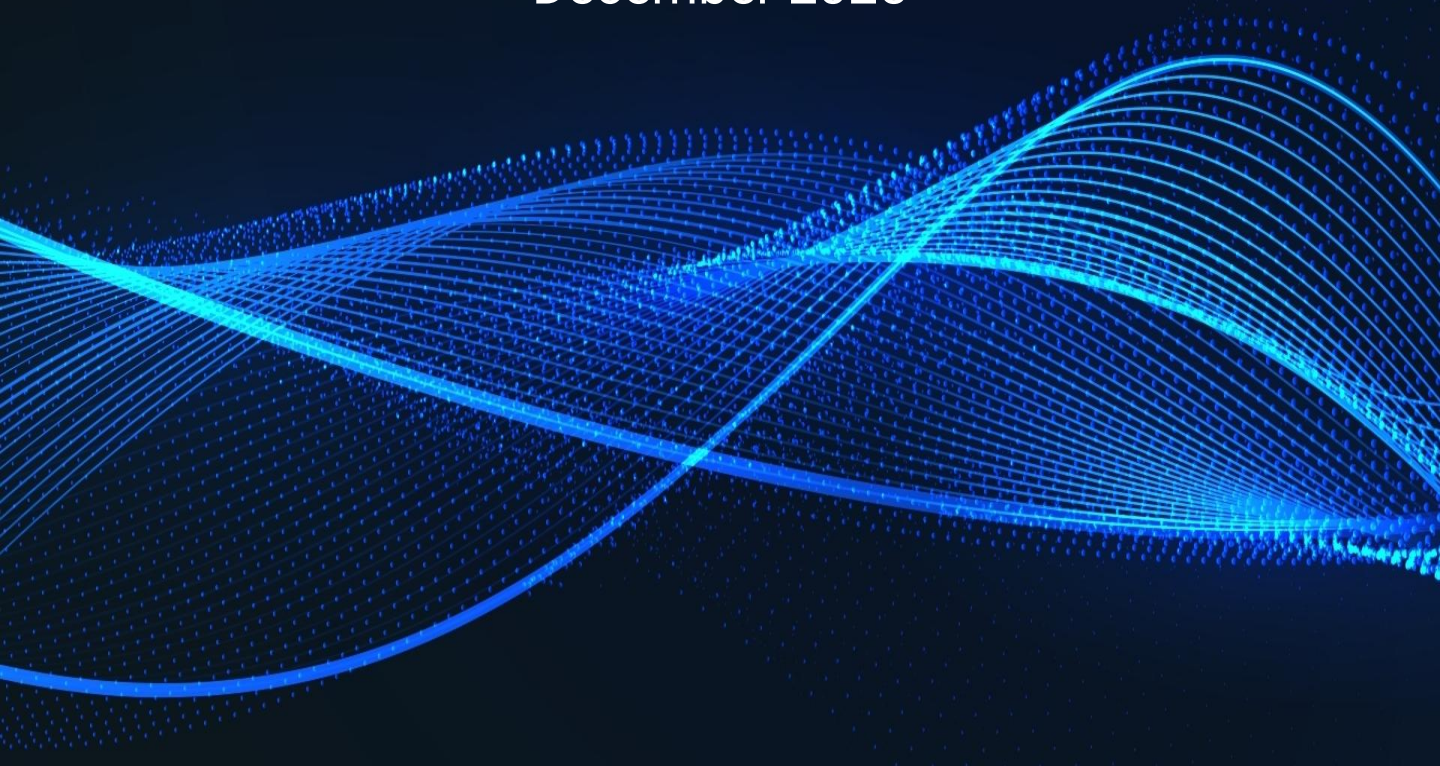
KARATZAS & PARTNERS

# Data Protection, AI & Cybersecurity

*Brief*

December 2025



KARATZAS & PARTNERS

# *At a glance*

Digital Omnibus Package—Toward a “new” era of digital simplification

EU Commission launches whistleblower tool for AI Act

Can AI developers bypass IP protection? The Gema vs. Open AI case

The major Hollywood deal of Netflix-Warner Bros acquisition: Critical IP and data protection implications

# Digital Omnibus Package—Toward a "new" era of digital simplification

*The European Commission's proposal of the Digital Omnibus package, submitted on 19 November 2025, marks a new era for Europe by introducing more streamlined and simplified rules.*

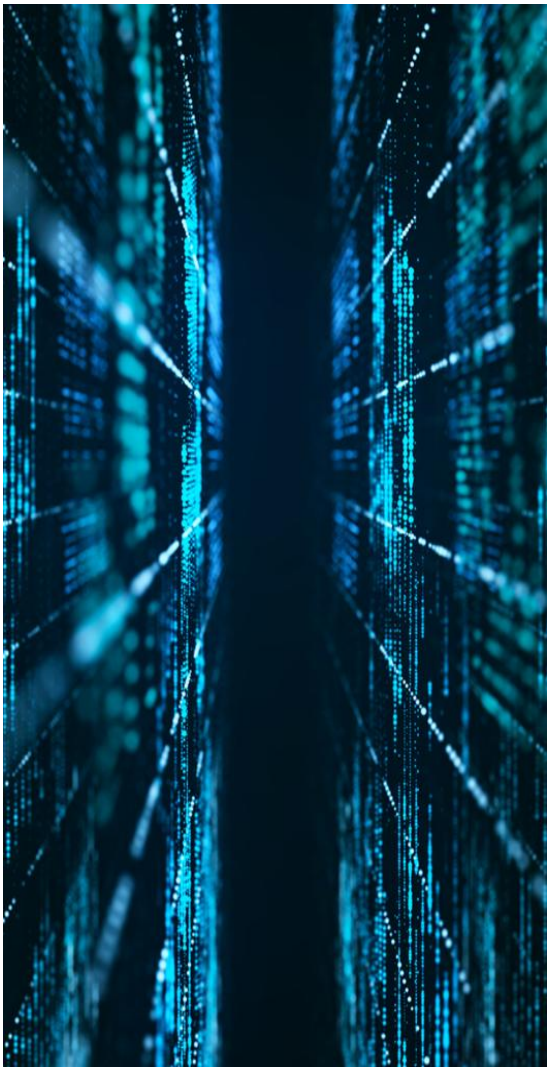
**What are the main goals of Digital Omnibus?**

- ✓ **Simplify, streamline and modernize the EU's digital rulebook**: reduce regulatory duplication and make compliance easier.
- ✓ **Reduce administrative burden and compliance costs:** Companies (especially SMEs) often struggle to comply with overlapping, sometimes contradictory, regulatory demands. The EU Commission claims the package could save up to €5 billion by 2029 by making compliance simpler.
- ✓ **Modernize rules and streamline existing laws**: The amendments seek to streamline legal rules on data, privacy, e-privacy, cybersecurity, AI Act provisions etc.

**What are the main amendments of the Digital Omnibus?**

- ✓ **Consent fatigue and changes to the ePrivacy framework:** The proposal would permit storing or accessing personal data on terminal equipment without consent in certain circumstances (e.g., first-party audience measurement). However, consent is still required for other cookie categories (e.g., advertising cookies).
- ✓ **Cyber-security & incident reporting simplification:** The amendments presented will introduce a single-entry point through which entities can simultaneously fulfill their incident reporting obligations under multiple legal acts (including notification under GDPR, NIS2). The proposal establishes the obligation on ENISA to develop the single entry-point.
- ✓ **Data breach notification timeframe:** The deadline for reporting data breaches to competent authorities will be extended to 96 hours.
- ✓ **Changes to the definition of personal data:** The Digital Omnibus proposes narrowing the GDPR's definition of personal data to exclude data held by an entity that does not have "*means reasonably likely to be used to identify*" the data, incorporating the position of the Court of Justice of the European Union (CJEU) in SRB (C-413/23 P, September 2025. The proposed amendment paves the way for wider and more flexible use of pseudonymized data.
- ✓ **Limitation of Right of Access:** Data controllers may refuse access requests if they determine the request is an "*abuse of the rights conferred*" by the GDPR. In practice, that means a controller could decline a request if they consider it was not submitted for genuine data-protection reasons (e.g. fishing purposes).
- ✓ **AI training simplification rules:** For certain AI models, the proposal allows training on personal data under legitimate interest under specific safeguards and balancing tests. Additionally, easier use of pseudonymized data also assists the AI training, as fewer transparency/consent requirements are needed when the data controller genuinely cannot identify data subjects.

# EU Commission launches whistleblower tool for AI Act



The European Commission has launched a secure whistleblower tool for the AI Act , allowing individuals to confidentially report suspected violations directly to the EU AI Office. Reports can be submitted in any EU language and format, with certified encryption ensuring full anonymity and data protection.

Whistleblowers help the EU detect early risks, supporting the safe and transparent development of AI technologies. The main aim is to enable **early detection of violations**, e.g. potential misuse of AI systems, threats to fundamental rights or public trust — before they cause widespread harm.

By providing insiders a safe way to report concerns confidentially, the EU Commission aims to reinforce transparency, accountability, and compliance across AI systems operating in the EU.

# Can AI developers bypass IP protection? The Gema vs. Open AI case

In November 2024, Germany's music collecting society, GEMA, brought an action before the Munich I Regional Court against US-based AI developer OpenAI, alleging that OpenAI used protected song lyrics to train its GPT-4 and GPT-4o large language models, which power ChatGPT , without obtaining a license. OpenAI argued that its models do not store or copy specific training data but instead reflect statistical correlations learned from the dataset as a whole.

On 11 November 2025, the Court ruled in favor of GEMA. It found that ChatGPT had indeed stored (or "memorized") and reproduced protected song lyrics, constituting unauthorized reproduction under copyright law. The court rejected OpenAI's arguments and ordered OpenAI to pay damages and cease using the copyrighted lyrics in its models without valid licenses.

The ruling has wide-ranging implications for how AI systems may be trained and how existing copyright and IP laws apply to generative models.

**Key takeaway**

**Copyright applies to AI training, and IP licenses may be necessary**: if the training set contains copyrighted works and the resulting model can reproduce them, such reproduction constitutes infringement. Businesses training AI models on copyrighted content may need to enter licensing agreements with IP holders or collecting societies.

Open AI is appealing against the case ruling and has until January 2026 to file its argument for supporting its appeal against GEMA.

# The major Hollywood deal of Netflix-Warner Bros acquisition: Critical IP and data protection implications

Netflix, the world's dominant streaming service, has announced its planned acquisition of Warner Bros. in a deal valued at $82.7 billion. The takeover would create a new entertainment industry giant, but the deal must be approved by competition authorities. Paramount has already launched a hostile takeover bid for Warner Bros., valuing the company at $108 billion, higher than Netflix's offer.

The transaction has major consequences for ownership, control, exploitation, and management of some of the world's most valuable entertainment IP, in addition to antitrust issues. Warner's core IP assets include numerous famous brands and copyrighted content, such as comic book films (e.g., Batman, Superman, Joker), animation (e.g., Looney Tunes), and HBO originals.

- If the deal closes, Netflix will gain **direct ownership and control** over **high-value IP** for global streaming, production, licensing, and merchandising. Netflix could choose to make this content exclusive to its platform, removing it from other services and increasing Netflix's market power. However, **Netflix cannot immediately migrate all content to its platform** due to existing long-term licensing agreements with other companies worldwide; some content must remain on other platforms until those agreements expire. **Full IP integration** may therefore take years, depending on contract expirations. Additionally, regulators may view such consolidation of premium IP as anticompetitive. The deal also has several implications for how personal data is handled, shared, and protected. Both Netflix and Warner Bros. hold **large volumes of user data**.
- Merging these datasets may create data protection risks, including issues regarding lawful bases for combining user profiles, failure to meet consent and transparency requirements, and data transfer risks.
- The merger would combine Netflix's approximately 300 million subscribers with Warner Bros. Discovery's 130 million HBO Max subscribers, creating a massive database of user data under a single entity.
- Additionally, Netflix would inherit all of Warner's obligations under applicable **local legislation** in countries where Warner operates its streaming services (e.g., GDPR, UK Data Protection Act). This may require **harmonizing inconsistent legacy practices** and reassessing privacy notices, retention periods, and related matters.

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