POLICY BRIEF n. 4/2026

www.techno-polis.com

# The EU Digital Omnibus: simplification, competitiveness, and the challenge of integrated governance

*Andrea Stazi**

**Abstract:** The paper examines the EU Digital Omnibus package, assessing its potential to simplify the regulatory framework and enhance EU competitiveness by addressing the technological gap with the US and China. It discusses the challenge of balancing fundamental rights with an "innovation-oriented" approach, exemplified by the expansion of regulatory sandboxes. Specific frictions include the difficulty of coordinating the AI Act with the GDPR, as is evident for example in the proposal for consent at the browser level, which conflicts with GDPR's requirement for granular consent. Conversely, the recognition of "legitimate interest" as a legal basis for AI training appears as a positive, albeit complex, coordination effort. Finally, the paper notes unresolved issues such as the regulatory gap on liability after the withdrawal of the AI Liability Directive and the question of copyright protection for generative AI training. It concludes by advocating for a pragmatic, operational approach focusing on developing concrete use cases, incentivizing Privacy Enhancing Technologies, and enforcing existing rights like data portability through interoperable standards.



## 1. The usefulness of the Digital Omnibus corrections for EU competitiveness

The Digital Omnibus package, presented by the European Commission and currently under negotiation between Parliament, Council and Commission, represents a pragmatic response to the challenges highlighted by the Draghi Report[1], who stressed the urgency of bridging Europe's technological gap with the United States and China.
The aim of the proposal is to **streamline the regulatory framework and reduce bureaucratic burdens and compliance costs** for businesses by up to 35%.[2]

[1] M. Draghi,The future of European competitiveness, September 2024.
[2] Morrison, Foerster, EU Digital Omnibus on AI: What Is in It and What Is Not?, December 2025.

The European Union has built a very high level regulatory framework, but the rapid succession of regulations, such as the AI Act, Data Act, GDPR etc., has generated a fragmentation that risks suffocating investments.[3]
In this sense, the proposed remedies offer crucial relief: for example, postponing the application of the rules for high-risk AI systems until late 2027 or 2028 acknowledges the need to wait for the development of harmonized technical standards, without which businesses would face crippling legal uncertainty.[4]

## 2. The complexity of balancing governance and rights from an "innovation-oriented" perspective

The real test for the EU legislator is to maintain the solid paradigm based on **fundamental rights**, while introducing innovation-oriented rules.[5]
The rapid evolution of technologies like artificial intelligence requires agility, and the Digital Omnibus seeks to promote a **"pro-innovation" approach**.
An example of this is the intention to expand the use of **regulatory sandboxes**[6]. This tool will allow developers to test products, services or business models in a controlled environment without immediately encountering strict regulatory constraints, moving from a purely precautionary approach to one that favors industrial development[7].

## 3. The persistent challenge of coordinating the AI Act with the GDPR

Despite the efforts, the package highlights the profound difficulty of **coordinating** the new digital regulations **with the pre-existing legal infrastructure**, first and foremost the **GDPR** and **ePrivacy Directive**[8].
A clear example of this friction is the proposal on the supply of the **consensus at the browser level**.
Designed to solve the problem of "consent fatigue" by automating users' tracking preferences, this solution struggles to comply with the GDPR, which requires granular, informed and specific consent[9].

---

[3] B. Lazarotto, The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act, December 2025.
[4] B. Martens, The European Union needs more than the digital omnibus to make digital services competitive, December 2025.
[5] See: B. Lazarotto, The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act, cit.
[6] A. Stazi, R. Jovine, A Comparative Analysis of Regulatory Sandboxes: Models, Evolution and Strategic Implications in EU, USA and China, September 2025, and Id., A Comparative Analysis of Regulatory Sandboxes: Models, Evolution, and Strategic Implications in the UAE and Singapore, January 2026.
[7] See: B. Martens,The European Union needs more than the digital omnibus to make digital services competitive, cit.
[8] Cf.: Morrison, Foerster, EU Digital Omnibus on AI: What Is in It and What Is Not?, cit.; B. Lazarotto, The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act, cit.
[9] See: B. Martens, The European Union needs more than the digital omnibus to make digital services competitive, cit.

A blanket six-monthly consent process, on the one hand, lacks the specific details needed for "informed" consent across millions of websites and for a variety of purposes; on the other, it risks drastically reducing data availability and advertising revenue, forcing publishers to hide behind paywall models.
This would dry up the source of free and open data that is vital to fueling the AI ecosystem.
On the contrary, a positive example of coordination is the introduction of **"legitimate interest" as a legal basis for AI training**.
Until now, diverging interpretations from the 27 national privacy authorities had created a regulatory blockade, delaying the introduction of advanced models in Europe.
The new Article 88c of the GDPR codifies the opinion issued by the European Data Protection Board in 2024, recognizing that training AI models represents a valid "legitimate interest".
The use of publicly available personal data becomes lawful for the algorithmic training, provided that rigorous technical safeguards and the unconditional right to opt-out are guaranteed, thus unlocking huge amounts of data for the European ecosystem[10].

## 4. The issues still to be resolved and the pragmatic path to regulation

The EU digital landscape, however, presents further crucial issues that the Omnibus' push for deregulation risks aggravating or leaving unresolved[11].
Among these, the regulatory gap on liability stands out: the official **withdrawal of the proposed AI Liability Directive** leaves unresolved the issue of how to allocate responsibility when complex AI systems cause harm. This choice leaves citizens without a harmonized European path, forcing them to face enormous difficulties in proving causality and placing the burden of proof on them.
Another unresolved issue is whether or not generative AI training is eligible for **copyright** protection, which is currently under consideration by the European Court of Justice in the *Like Company* case[12].
Regarding **algorithmic transparency**, instead, the recent *Dun & Bradstreet Austria*[13] ruling of the Court of Justice has just reaffirmed that citizens have a genuine right to a clear and intelligible explanation of the logic applied by the "black box" decision-making[14].

---

[10] Cf.: B. Martens, The European Union needs more than the digital omnibus to make digital services competitive, cited; A. Stazi, Legitimate Interest: A Legal Basis for AI?, July 2025.
[11] See: B. Lazarotto,The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act, cit.
[12] Request for a preliminary ruling from the Budapest Regional Court (Hungary) lodged on 3 April 2025 – Like Company v Google Ireland Limited (Case C-250/25, Like Company). See: J. Hoffmann,Technological Determination of AI-Relevant Press and Copyright Law and Generative Content's Relevance for EU Competition Law -The referral in Case C-250/25, Like Company v. Google Ireland Ltd., August 2025.
[13] Judgment of the Court (First Chamber) of 27 February 2025 (request for a preliminary ruling from the Verwaltungsgericht Wien - Austria) – CK v Magistrat der Stadt Wien (Case C-203/22 1, Dun & Bradstreet Austria).
[14] VUB Cyber & Data Security Lab, EU AI Law and Policy in 2025: Year-in-Review, January 2026.

## Conclusion: an operational approach to user protection

The best approach to unravel these knots does not lie in a continuous rewriting or layering of abstract rules, but in a method inspired by the concrete functioning of technology and the real relationship between market players[15].
In practical terms, this translates for example into the need to:

- **Develop prototypes and concrete use cases**: The real barrier to data sharing isn't just bureaucratic, but operational. Funding is needed to create prototypes that demonstrate to businesses the economic value of data intermediaries.
- **Encourage Privacy Enhancing Technologies**: To enable secure data use without disrupting business models, regulations should incentivize techniques such as differential privacy and synthetic data, which enable value extraction while maintaining compliance.
- **Putting existing rights into practice**: Rather than simply deregulating, we need to enforce key rights, such as data portability, by forcing the creation of interoperable standards that allow citizens to move their information securely and seamlessly.

Only by anchoring the rules to the operational reality of the technological infrastructure and supporting those who develop practical solutions, will it be possible to build a digital ecosystem in which compliance it is not seen as a brake but as a pillar for ethical and sustainable innovation[16].

** CEO and Co-Founder Techno Polis*

[15] Cf.: B. Lazarotto, The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act, cit.
[16] Cf.: VUB Cyber & Data Security Lab, EU AI Law and Policy in 2025: Year-in-Review, cit.