bitkom

Position Paper

2026 March

Digital Omnibus: Delivering Genuine Relief for Businesses

Executive Summary

The Digital Omnibus is the only instrument in the current legislative term capable of providing immediate, tangible relief from bureaucratic burdens for Europe's digital economy. Importantly, this initiative is not about dismantling fundamental rights or lowering protection standards, but about targeted, proportionate adjustments that address well-known practical frictions in the existing framework.

These adjustments can significantly improve legal certainty and competitiveness without entailing any substantive reduction in the level of fundamental rights protection. While other initiatives will take years to implement, this proposal offers a unique opportunity to resolve legal uncertainties now. Any failure or ”watering down” by Member States would paralyse the broader digital agenda and significantly increase the ”costs of inaction”.

These adjustments can significantly improve legal certainty and competitiveness without entailing any substantive reduction in the level of fundamental rights protection. Rather, they are a necessary response to unbalanced and disproportionate interpretations of existing rules, which go far beyond what is required for effective fundamental rights protection and create avoidable legal and economic friction.

The Framework for a successful reform

- **Responsibility of Member States:** The Omnibus is currently the only option on the table for a better regulation by simplification and modernisation. If Member States dilute the proposal or block progress, they take one step back from digital de-bureaucratisation and towards further deterioration of the competitiveness of the European industrial base. Rather than calling the proposal into question, efforts should focus on further developing and strengthening it in a pragmatic and forward-looking manner.

- **Institutional Realignment:** The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) are part of the current complexity of the law and not the solution to it. Their interpretations have in some cases actively contributed to legal and market uncertainties. It is unlikely that simplification and clarity can be reached without clarifications in the legislation itself. This should not be left to any of the implementing or law enforcing parties.
- **Articulating the "Costs of Inaction":** A refusal to reform leads to permanent "over-compliance" (unnecessary consent layers, excessive documentation). This is exacerbated by the limited cooperation between supervisory authorities and industry in for example developing GDPR-compliant Privacy-Enhancing Technologies within Europe. As a result, companies of all sizes are forced to develop innovations in sectors such as health, automotive, or finance outside of Europe, as European champions are structurally disadvantaged by fragmented national interpretations.

Core Demands for a GDPR Reform

Bitkom welcomes the goal of simplification but criticises the Council's tendency to shift crucial clarifications into non-binding recitals or to delegate decision-making power back to the EDPB and national authorities. This undermines the objective of genuine harmonisation.

1. **Identifiability and the "Relative Approach" (Art. 4 GDPR)**

Determining whether data is "personal" should not be an abstract-theoretical exercise; it must be based on the tools and means realistically available to the specific actor in question. The clarification of the "relative approach" must remain in the normative part (Art. 4 GDPR). Only Including it in Recital 27 is insufficient; Information should not be considered personal data for an entity if that entity lacks the means to identify the individual with reasonable effort. Moving technical definitions to delegated acts or EDPB guidelines creates no legal certainty; it merely perpetuates the status quo of overly restrictive interpretation by prohibiting to process data in case of any marginal doubt.

2. **Legal Certainty for AI Innovation (Art. 6 & 9 GDPR)**

AI models require vast datasets for training and validation.

- **Legitimate Interest:** The processing of data for the training, testing, and validation of AI systems should be explicitly recognised as a "legitimate interest" under Art. 6(1)(f);
- **Handling Sensitive Data:** We advocate for an exception to the strict prohibition on processing sensitive data when such data is present merely as incidental "by-catch" (residual data) within a dataset, without being functionally necessary for the AI training;

- If removing such data would require a substantial ”re-engineering” of the model, technical safeguards (e.g., preventing biased output or disclosure) must be recognised as equivalent protective measures.

3. **Curbing the Abuse of Rights (Art. 12 & 15 GDPR)**

The right of access is increasingly being weaponised for purposes unrelated to data protection, such as forcing legal settlements or strategically preparing for damages claims. We welcome the clarification that requests can be refused in cases of proven abusive intent (e.g., offering to withdraw a request in exchange for payment);

Since the evidence for excessive or bad-faith requests often lies outside the controller’s sphere, the burden of proof for businesses should be lowered to a ”reasonable level”.

4. **Pragmatic Information Requirements (Art. 13 GDPR)**

- In clearly defined, non-data-intensive customer relationships, it should be possible to waive formal information obligations if the data subject is already aware of the basic data processing;
- For scientific research, simplifying information requirements in cases of ”disproportionate effort” is essential for Europe as a research hub. Public announcements (indirect information) should be established as the standard in these cases.

5. **A Coherent Framework for Cookies and Device Access (Art. 88a & 88b GDPR)**

The current legal uncertainty at the intersection of the GDPR and the ePrivacy Directive leads to ”consent fatigue” and hinders data-efficient innovation.

- **Art. 88a – Risk-Based Approach:** We call for device access to be consistently aligned with the GDPR. For low-risk processing, such as reach measurement, fraud prevention, or contextual advertising, the ”legitimate interest” (Art. 6(1)(f)) must be made legally secure without requiring explicit consent. This is the only way to sustainably reduce the flood of banners;
- **Art. 88b – Rejection of Browser Signals:** We oppose the proposal for machine-readable preference signals (e.g., via browser). Such signals cannot meet the strict requirements for ”informed and specific” consent and would effectively result in a ban on ad-supported internet offerings. Furthermore, they would cement the market power of a few browser manufacturers, who would then dictate data access for the entire ecosystem. We recommend the deletion of Art. 88b in favour of a strong Art. 88a.

Conclusion

A failure of the Digital Omnibus would send a fatal signal regarding European competitiveness. We urge the European Parliament and the Council to seize this opportunity for genuine harmonisation and to prioritise legal certainty through clear, directly applicable statutory definitions within the Regulation itself.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Isabelle Stroot | Head of Data Protection Law & Policy
P +49 30 27576-228 | i.stroot@bitkom.org

Elena Kouremenou | Policy Officer for Data Privacy
P +49 30 27576-425 | e.kouremenou@bitkom.org

Responsible Bitkom committee
WG Data Privacy