



Joint Industry Statement:

EU Member States and Policymakers Must Not Undermine the Ambition of the EU Digital Omnibus

The undersigned industry associations, representing a broad coalition of technology providers, digital infrastructure companies, medical technology companies, SMEs and businesses enabled by technology, write to **express concern about the trajectory of negotiations on the Digital Omnibus proposal** in the Council of the European Union (EU).

The Digital Omnibus proposal is a concrete and important opportunity to address overlapping, fragmented, and often contradictory rules on data, ePrivacy, and cybersecurity, creating unnecessary costs, bureaucracy, and hampering innovation. As highlighted in the Draghi Report, regulatory complexity and fragmented implementation are significant obstacles to the competitiveness of businesses, innovators and SMEs in the EU Single Market.

To respond to these challenges, EU Member States have repeatedly expressed strong political support for an ambitious simplification of the EU's digital rulebook. From the 2024 Budapest Declaration, to the European Council conclusions of March 2025, to the discussions at the Alden Biesen retreat in February 2026, European leaders have consistently recognized the need to ambitiously reduce unnecessary regulatory barriers.

However, the ongoing work in the Council of the EU is moving in the opposite direction. The Digital Omnibus compromise texts from the Cypriot Presidency of the Council significantly weaken key simplification goals of the proposal while introducing additional burdens. For example, the texts roll back GDPR simplification by deleting the key Commission's proposals and reject the proposed EU-level Single-Entry Point for cyber incident reporting in favor of fragmented and overlapping national reporting channels. Moreover, the texts maintain or propose concerning amendments to the rules on cookies – such as mandating centralized consent, reverting the rules to the ePrivacy Directive, or providing extremely narrow exemptions to consent-based compliance - which will create complexity and significantly harm the wider online economy and open web, from technology providers to retailers, advertisers, and digitally enabled SMEs.

If this trajectory continues, the outcome will fall short of meaningful simplification and represent a missed opportunity, with tangible consequences for Europe's ability to compete, innovate, and attract investment. A course correction is urgently needed.

In particular, we the undersigned organizations, urge Member States to:

- **Maintain the Commission's targeted GDPR amendments,** including clarifications around the definition of personal data, more workable conditions for the use of personal data for AI while avoiding overly restrictive wording that would curtail future use cases, an innovation-enabling definition of scientific research, and a more practical data breach notification framework. These are crucial calibrations that will reduce legal uncertainty and fragmentation while preserving strong safeguards.
- **Ensure any reform of 'cookies' rules reflects technical and market realities, ensures harmonization, and does not undermine Europe's digital economy and competitiveness.** In particular, Member States should reject complex and unfeasible rules on centralized consent for cookies in Article 88b and amend Article 88a so cookies and similar technologies can rely on any of the GDPR Article 6 legal bases (not consent-only), while avoiding imposing consent restrictions to low-risk processing (e.g., security/fraud prevention and detection, frequency capping, user-requested functionality), and without undermining independent market-agreed audience measurement.
- **Support an EU level Single-Entry Point for incident reporting,** enabling businesses to meet overlapping incident reporting obligations through one single EU mechanism. A national approach would not meaningfully address compliance burdens, especially for cross-border operators. In addition, the Single-Entry Point must be accompanied by an ambitious simplification and harmonization of obligations, timelines, templates and definitions across cybersecurity frameworks.

- Consider the complexity of the EU Data Act and ensure trade secrets are adequately protected, while addressing risks of unlawful use, loss of proprietary know-how, and safety concerns.

We call on Member States to carefully consider the points above before proceeding with reaching a General Approach on the Digital Omnibus. In doing so, we urge Member States to take additional time for the negotiations and robustly engage with impacted stakeholders. **While our industries support a swift approval of the proposal, negotiation speed must not come at the expense of quality and ambition of the Digital Omnibus.**

The Digital Omnibus requires clear political steering. Member States must ensure that the ambition they have publicly endorsed is reflected in the final outcome. We remain ready to engage constructively in support of a meaningful and workable result.

Signatories (in alphabetical order):

AFNUM (Alliance Française des Industries du Numérique)

Anitec Assinform

Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh)

Bundesverband Kooperierender Mittelstand e.V. (BKM)

Business Software Alliance

Chamber of Progress

Computer & Communications Industry Association (CCIA Europe)

Danish Entrepreneurs

Developers Alliance

DOT Europe

eco – Association of the Internet Industry

Europäischer Wirtschaftssenat e.V.

FEDMA - Federation of European Data and Marketing

German Association for the Digital Economy (BVDW)

IAB Europe

ITI – Information Technology Industry Council

Japan Association of New Economy

Middle Tech Europe

MedTech Europe

Taxpayers Association of Europe

Technology Ireland

Zentralverband der deutschen Werbewirtschaft e.V.