Simplify, protect, compete:
nine Digital Omnibus fixes for European companies

Brussels, 9 November 2026

Dear Members of the European Parliament,

We represent Europe's companies and business associations active in the European market. Together, we represent businesses of every size, from start-ups, SMEs, Unicorns to global leading companies. We share the common goal you have set for this mandate: **to put Europe's future in Europe's hands**.

The Digital Omnibus should be more than an administrative clean-up. It is an opportunity to create the right conditions for applied research, investment in AI and data-driven innovation across Europe, and strengthen our technological leadership. Above all, it must deliver genuine simplification, not replace today's complexity with more bureaucracy.

Two years after the Draghi report, Europe must show it is turning this goal into reality[1]. AI is central to this, and AI is built on data. If European rules make it disproportionately difficult for European companies to use data, they cannot develop and deploy their AI models and systems. As a result, European AI won't be competitive leaving no option but to continue relying on AI built elsewhere.

[1] According to the 2024 Draghi report on competitiveness, GDPR compliance costs may reach EUR 500,000 for SMEs and EUR 10 million for larger organizations.
Mario Draghi, The Future of European Competitiveness (European Commission 2024)
https://commission.europa.eu/topics/competitiveness/draghi-report_en accessed 4 November 2026.

European companies want to develop responsible AI that protects privacy, cybersecurity, safety and to earn consumer trust. Lawmakers should refine the rules without falling for the false choice between protecting citizens and allowing industry to grow.

As Parliament prepares its position on the Digital Omnibus, we ask you to support the following nine fixes to make it work for European companies:

1. **Protect trade secrets and keep data sharing workable.** Data that are a trade secret, or from which a trade secret can be derived, should explicitly be exempted from mandatory data sharing, in line with the Trade Secrets Directive. Companies need a clear safeguard to prevent transfers that would put their unique and highly sensitive know-how at risk, including to competitors inside the EU.

2. **Allow manufacturers' access to non-personal data.** A statutory right for the data holder to access non-personal product data, without jeopardising Data Act safeguards, would empower them to develop industrial AI and maintain, update and secure connected devices without the unnecessary burden of endless bilateral negotiations.

3. **Incentivise the use of privacy-enhancing technologies (PETs).** Companies using PETs protect data effectively by reducing or removing the risk of identifying individuals. GDPR obligations should be proportionate to that lower risk, giving companies a clear reason to invest and develop in PETs. To prevent privacy-washing and ensure fair competition, open standards for PETs should be developed through a multi-stakeholder approach. They avoid proprietary walled gardens and make PETs affordable for all businesses, so that privacy becomes a baseline, not a premium feature.

4. **Confirm legitimate interest for AI training**. Competitive European AI needs predictable rules for training models, running evaluations and correcting bias. Legitimate interest and the GDPR balancing test and safeguards (including PETs) protect citizens and give European businesses a fair chance to compete. Beyond AI training, companies also need to be able to rely on legitimate interest to prevent fraud and enhanced security.

5. **Centralised consent is no solution to consent fatigue.** Consent should remain meaningful without trivialising user choice. Handing Europe's consent architecture to a few providers would cut European businesses' direct relationship with their users. Aligning the terminal equipment rules with the GDPR would let companies rely on its full range of legal grounds and reserve consent for what users care about, such as personalised advertising across websites and sharing data with third parties. Security, fraud prevention and audience measurement should not rely on consent.

6. **Support European Research**. Applied scientific research in both the private and public sector should be able to rely on legitimate interest, where appropriate. Without research, there is no innovation and without innovation, there is no technological competitiveness.

7. **Codify the relative approach to personal data.** Data protection rules should reflect actual risk, not theoretical cases. The Commission rightly proposes to write the Court's jurisprudence into the GDPR, confirming data is not personal for a company that cannot reasonably re-identify the person. It would give European companies immediate legal clarity and assurance that their national authorities and courts will apply the test evenly, while maintaining strong safeguards for individuals.

8. **Keep human oversight obligations proportionate to risk.** Human oversight in automated decision making should focus on decisions where safety, ethics and critical judgement matter, not on every routine, low-risk automated task. New procedural hurdles on applied research and development would stall promising projects and favour those who can absorb the compliance cost, rather than European SMEs.

9. **Build one secure rulebook for incident reporting.** A single entry point for breach and incident notifications is the right approach, with harmonised procedures, deadlines, definitions, thresholds and templates across the cyber and data rules. The single entry point must be resilient to cyber attacks and built to safeguard the information reported.

Simplification must be real. A single market should not mean 177 enforcing authorities, each interpreting the same rules differently. Done well, the Digital Omnibus will boost data-driven and AI innovation across Europe, cut compliance costs[2], while keeping privacy protection strong. Simpler rules and strong protection should reinforce each other, so that Europe becomes a place where companies choose to stay, scale and foster talent.

We would welcome the chance to discuss this with you and your teams at your earliest convenience.

Yours sincerely,

APPLiA - Home Appliance Europe
BUSINESSEUROPE
CECIMO – European Association of Manufacturing Technologies
DIGITALEUROPE - Representing digitally transforming industries in Europe
Ecommerce Europe
EFCEM – European Federation for Catering Equipment Manufacturing
EFPIA - European Federation of Pharmaceutical Industries and Associations
EGMF – European Gardening Machinery Federation
EUnited - European Engineering Industries Association
Euralarm
Eurochambres - Association of European Chambers of Commerce and Industry
EuroCommerce
EFA - European Fintech Association
EUTA - European Tech Alliance, representing tech companies born, bred and headquartered in Europe
FEM – European materials handling federation
Orgalim – Europe's Technology Industries

[2] In 2023, regulatory compliance accounted for 3.9% of employment in the EU, more than twice the share of R&D personnel (1.7%). OECD, 'Time for a Regulatory Reset?' in *OECD Economic Outlook, Volume 2025 Issue 2* (OECD Publishing 2025) 71 accessed 4 November 2026.