

Feedback on the Digital Omnibus on AI

Introduction

Artificial intelligence is rapidly transforming Europe’s retail and wholesale ecosystem, reshaping how businesses serve customers, optimise supply chains, and compete in an increasingly digital marketplace. As the EU advances its regulatory framework through the Digital Omnibus on AI, retailers and wholesalers stand ready to embrace rules that foster trust, safeguard consumers, and enable innovation to thrive.

EuroCommerce has consistently supported a clear, future-proof, and risk-based approach to regulating AI, ensuring that only genuinely high-risk applications face stringent obligations while everyday AI-enabled tools—such as product recommendations or inventory optimisation—remain fully accessible to businesses of all sizes. At the same time, the sector has emphasised the need for legal certainty, proportionality, and alignment with existing EU legislation, so that companies can innovate confidently without unnecessary administrative burden.

Considering the nearing application date of the AI Act’s high-risk requirements later this year we urge EU institutions to agree on a final Digital Omnibus on AI.

1. Exemptions SMCs and SMEs

We support the introduction of exemptions for small mid-cap companies (SMCs) and the extension of certain micro-enterprise exemptions to SMEs.

A study of our German member association HDE, shows that smaller retailers are more cautious about implementing AI projects. 90% of companies with net sales of between €50 million and €1 billion stated that AI projects were in the planning or implementation stage or had already been completed. The same statement was made by 86.4% of companies with net sales of over €1 billion. Among companies with net sales of up to €50 million, only 46.9% have planned, implemented or completed AI projects. The fact that small and mid-cap companies can now benefit from simplified requirements, e.g. for technical documentation, is therefore a step in the right direction to promote AI projects in smaller companies and give them the opportunity to become more active in this area.¹ AI literacy (Art.4 AIA)

We believe the European Commission and Member States have a better overview of ensuring AI literacy for society as a whole, which is a strategic EU priority. The obligation that is now imposed on companies is too broad and vague. This is particularly challenging for non-tech SMEs who are hardly able to comply with this far-reaching obligation and are exposed to many fraudulent offers and practices. Despite placing the legal burden elsewhere, companies can and will continue their voluntary

¹ [Safaric HDE KI-Index 2025.pdf](#)

initiatives without this leading to legal uncertainty. In any case, Art. 26 still mandates AI literacy obligations on deployers of high risk AI systems.

However, we would recommend to make the obligation on the European Commission and Member States more concrete. For example, creating a voluntary EU curriculum providing recommendations on training and support measures accompanied by training programmes for companies free of charge. This would help especially SMEs and could also address the problem with fraudulent, low quality and expensive trainings offered by third parties. Another interesting idea is to create Public-Private Partnerships.

2. Bias detection (Art. 4a new)

We support broadening the legal basis for processing special categories of personal data for the purposes of bias detection and mitigation, taking into account the safeguards and strict conditions already embedded in the AI Act for high-risk AI systems. This will make it possible to use special categories of personal data in important and essential areas to improve AI systems in a way that benefits everyone. At the same time, protective measures are being put in place to clearly regulate access to this data and ensure a technical protection standard. The protection of the fundamental rights and freedoms of natural persons is also included in Article 4a, and the assessment should remain at the same level. Below some potential use-cases examples:

1. SIA used in HR applications, such as CV sorting: a publisher (or even a deployer) may need data to verify that the algorithm does not systematically penalise women or certain ethnic minorities: the idea is to be able to ‘test’ the model with real data on gender or origin.
2. Voice recognition models (potentially voice-controlled apps): real data is needed to avoid biases related to local accents and languages, foreign accents, differences in pitch or prosody, etc.
3. AI for recommending size and body type: the algorithm may be less effective for certain specific body types or body types linked to ethnic origin or age (e.g. seniors vs junior athletes; Mediterranean vs Scandinavian phenotypes). To ‘refine’ the model, we may need to test whether the error rate is higher for a specific demographic segment, specific geographical areas, etc.

3. Reducing administration burden (Art. 6(4))

We support to remove the disproportionate registration obligation for Annex III AI systems in the EU data base when the system does not constitute a high-risk AI use case. Instead require providers to document its assessment and provide it on request. An examples could be HR tools where human intervention still determines the final outcome.

At the same time, the proposal requires providers to document why an Annex III system is considered not high-risk, but it does not ensure that this documentation is made available to deployers. As a result, deployers often lack visibility at procurement, making it harder to assess suitability and responsibility.

In addition, the proposal does not clearly address software updates or new features that introduce or expand AI functionality after placement on the market. Classification documentation should be shared with deployers in advance, potentially made available by the company upon request or through an EU-level register, and updated whenever changes are likely to affect the system’s risk profile. This becomes a decrease in the administrative burden for deployers and providers during the vendor assessment process, and an assurance for when validating the risk categories of products.

4. Strengthening coherent and consistent enforcement of the AI Act

We believe that the AI Office should have a stronger enforcement role. We support the possibility of the AI Office to establish AI regulatory sandboxes at Union level.

We support measures that strengthen cross-border coordination and collaboration among national authorities.

To increase legal certainty and ensure a harmonised approach to placing AI systems on the market, a principle of mutual recognition should apply: once a national authority has assessed an AI system as compliant, this should be recognised across all EU Member States. And companies should have fast and clear channels to obtain clarifications. Effective coordination reduces duplication and increases certainty for those operating within the single market.

The AI Office should be responsible for enforcing Article 50 of the AI Act.

We support the amendment to Art 75 of the AI Act, to make the AI Office exclusively competent for the supervision and enforcement of AI systems based on general-purpose AI models. We are seeing increasingly rapid and dynamic developments in GPAI and new AI models within search engines and VLOPs. In the retail sector, we are seeing a particularly strong trend towards AI agents for shopping and AI commerce. In order to ensure legal certainty in this area without hindering innovation, there must be uniform interpretation and enforcement of the law across the EU. The implementation of EU rules must be clear, consistent and legally certain. Align application deadlines Annex I and III, taking into account guidelines

Diverging application deadlines for Annex I/Article 6(1) and Annex III/Article 6(2) create unnecessary burdens. We recommend maintaining a single deadline—for example, 2 August 2028—as a *fixed* date.

Additionally, businesses need sufficient time to implement guidance. There should be 6 to 12 months between the publication of final guidance and the application of the corresponding provisions (e.g., AI transparency requirements). If guidance is not ready, the application date should be adjusted accordingly.

We also recommend to include a detailed timeline of upcoming “adequate measures” in support of compliance with Chapter III of the EU AI Act. This detailed timeline should include specific deadlines for the Commission to present the mentioned guidelines. Priority should be given to the guidelines on: practical application of the high-risk classification; practical application of the transparency requirements under Article 50 AI Act; reporting of serious incidents by providers of high-risk AI systems; a template for the fundamental rights impact assessment; practical application of rules for responsibilities along the AI value chain AI Act’s interplay with other Union legislation, e.g. with GDPR, CRA, Machinery Regulation; competences and designation procedure.

Where systems are later classified as high-risk, deployers should have the right to renegotiate contracts if compliance obligations change and the provider cannot or will not meet high-risk requirements. This is particularly important where systems were initially procured as non-high-risk and helps prevent deployers from being locked into non-compliant solutions.

5. Simplification of AI obligations used exclusively within a corporate group

It would be sensible to ease information requirements for AI models or systems that are used exclusively within a corporate group.

For example, when general-purpose AI is deployed solely by other entities within the same group, it is reasonable to exempt such internal deployments from full documentation obligations. In these cases,

the deploying entity can assume the necessary responsibilities without the need to prepare separate, ex-ante documentation tailored to each internal use case.

These obligations were originally designed to facilitate smooth cooperation and accountability across independent actors in the value chain. However, when applied within a single corporate group—functioning effectively as one entity toward third parties—they no longer serve their intended purpose.

6. Exclude optimisation models from the scope of the AI Act.

Optimisation systems and models used to find an optimal solution to a problem defined by rules and objectives have existed for a long time in wide-spanning sectors from logistics to financial services.

These systems are designed to solve a long list of specific mathematical problems (for instance: linear programming, logistic regression, etc.) that include limited non-deterministic elements with negligible inference of results in their iterations.

In the spirit of simplifying the compliance with the AI Act for industry and to avoid ambiguity in the interpretation of the law, since these systems do not pose a risk in their deployment and are extensively used, they should be explicitly excluded from the definition of AI under this Regulation.

Suggestion for amendment:

Article 2 (13) new:

This Regulation does not apply to systems or models used solely to solve mathematical optimization problems defined by an explicit objective function and constraints (including linear and mixed-integer programming, convex and combinatorial optimisation, constraint programming and network-flow optimization), unless they are placed on the market or put into service or used for the purposes of predictive inference, content generation, pattern recognition or autonomous decision-making affecting natural persons.

7. Additional simplification proposals

- Streamline risk-management assessments across Articles 9, 26(5), 27, and related sanctions under Article 72.
- Align GDPR Data Protection Impact Assessments with AI Act Fundamental Rights Assessments.
- Ensure that compliance with the Cyber Resilience Act constitutes compliance with Article 15 of the AI Act.
- Align the definition of biometric data in the GDPR and the AI Act.
- Introduce predictable timelines for drafting guidance to increase legal certainty.
- Maintain consistency between the definitions of AI models (Art. 3(63)) and AI systems (Art. 3(1) and (66)), including in recital 21 of the Omnibus.
- Avoid regulating proven safe systems such as chatbots; establish a non-exhaustive list of derogation conditions under Article 6(3).
- Ensure Article 60 on voluntary agreements for real-world testing does not lead to fragmentation; instead provide a clear, exhaustive list of exceptions.

Allow more time for compliance with watermarking obligations under Article 50(7); AI-generated code should be explicitly exempted.

Contact: Ilya Bruggeman
Name Lastname | bruggeman@eurocommerce.eu

EuroCommerce is the principal European organisation representing the retail and wholesale sector. It embraces national associations in 27 countries and 5 million companies, including leading global players and many small businesses. Over a billion times a day, retailers and wholesalers distribute goods and provide an essential service to millions of business and individual customers. The sector generates 1 in 7 jobs, offering a varied career to 26 million Europeans, many of them young people. It also supports millions of further jobs throughout the supply chain, from small local suppliers to international businesses. EuroCommerce is the recognised European social partner for the retail and wholesale sector.