BEUC The European Consumer Organisation

The Consumer Voice in Europe

Response to consultation

Upholding consumer protections in the Digital Omnibus on AI

February 2026

Why it matters to consumers

The EU AI Act has been designed to ensure safety, transparency and ethical deployment of AI systems across the EU while protecting consumers' fundamental rights. There is a careful balance of interests which the EU's Digital Omnibus now risks overturning. The proposed reopening of the Artificial Intelligence Act exposes consumers to unnecessary risks and more legal uncertainty. It would undermine compliance efforts that responsible businesses have made. It would also compromise essential consumer protections and erode trust in digital products and services.

Published | 5 February 2026
Contact | digital@beuc.eu
Reference | BEUC-X-2026-007
Document coordinator | Cláudio Teixeira
Credit | Photo by lersan8910 from iStockPhoto

The European Consumer Organisation (BEUC) is the largest organisation promoting the general interests of Europe's consumers. Founded in 1962, it proudly represents more than 40 independent national consumer organisations from over 30 European countries. Together with our members, we inform EU policies to improve people's lives in a sustainable and fair economy and society.

BEUC, The European Consumer Organisation
Bureau Européen des Unions de Consommateurs AISBL | Der Europäische Verbraucherverband
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents

Summary

The objective of simplification stands as a unique opportunity to improve the application and enforcement of the EU digital rulebook, making it easier for consumers to exercise their rights and seek redress. However, simplification should not lead to deregulation. Despite the initial assurances from the European Commission[1], we regret to observe that the Digital Omnibus proposal seems to go in the opposite direction.

BEUC is concerned that this proposal seems to go significantly beyond a mere "targeted modification", without having observed key procedural safeguards[2] and without the support of clear evidence or impact assessment[3] as required by the European Commission's Better Regulation principles. As a result, the Digital Omnibus proposal presents a reopening of the Artificial Intelligence Act (AI Act) and diminishes existing rights and protections that could undermine fundamental safeguards for consumers and European businesses. In its current form, the proposal could seriously impact privacy rights and key consumer safeguards against the risks of AI tools.

BEUC remains sceptical that the proposed changes would prove adequate to achieve the announced objectives of increasing European businesses' competitiveness. In practice, the companies who stand to benefit the most are those who currently hold a dominant position in the data industry – and these are all but European.[4]

Nonetheless, BEUC welcomes certain changes which offer some positive examples of how simplification can deliver better and more efficient outcomes for both consumers and businesses. For instance, the clarification of the governance and enforcement framework, and the growing empowerment of the AI Office through additional supervision and enforcement powers should help monitoring, improve information sharing between authorities and make enforcement more efficient, provided that this is accompanied by clear safeguards, transparency, and enough resources. One bottleneck should not replace another.

These elements demonstrate that the Digital Omnibus can deliver meaningful simplification that improves the rights of consumers, if applied in a proportionate and evidence-based manner.

[1] European Commission, *Summary Conclusions of the Implementation Dialogue on the Application of the GDPR* (16 July 2025), available at: https://commission.europa.eu/get-involved/events/implementation-dialogue-application-general-data-protection-regulation-commissioner-michael-mcgrath-2025-07-16_en.
[2] European Commission, *Summary Conclusions of the Implementation Dialogue on the Application of the GDPR* (16 July 2025), available at: https://commission.europa.eu/get-involved/events/implementation-dialogue-application-general-data-protection-regulation-commissioner-michael-mcgrath-2025-07-16_en.
[3] Ares(2025)7724296, Call for evidence - Simplification – digital package and omnibus, September 2025 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus_en
[4] This is especially concerning given the recent reports of how the proposal in detail seems to mostly respond to the demands of Big tech. See Corporate Europe, Article by article, how Big Tech shaped the EU's roll-back of digital rights, January 2026: https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights

In the following contribution, we will highlight the most important changes for consumers regarding the AI Act and share BEUC's recommendations to ensure that both a high level of protection for consumers and a regulatory level playing field for EU businesses remains in place.

BEUC RECOMMENDATIONS

1 **Restrict processing of special data for bias detection**
Promoting bias detection in AI systems should not become a general justification for expanding the processing of special categories of personal data. This should remain limited to clearly defined exceptional cases with compliance safeguards.

2 **Maintain registration obligations for high-risk systems.**
The registration obligation must remain a necessary safeguard for transparency, effective enforcement and consumer protection

3 **Regulatory privileges should remain exclusive to SMEs and EU start-ups.**
The proposed extensions must remain strictly limited to genuine SMEs and EU start-ups. High-risk AI systems must remain subject to full compliance obligations, regardless of the size of the provider.

4 **Reject the reversal of AI literacy obligations.**
A clear obligation to ensure sufficient AI literacy should remain an obligation for providers and deployers, not a burden for consumers or public entities.

5 **Clarify governance and enforcement framework.**
Empowering the AI Office should complement the work of national regulators. Any centralising enforcement must require clear safeguards, adequate resources and more accountability.

6 **Reconsider "Stop the Clock" timeline.**
Extending deadlines for high-risk AI obligations and suspending labelling requirements weakens consumer protection. Transparency and accountability safeguards should remain in place.

1. Processing of special categories of data to tackle bias must have stronger safeguards

The proposal establishes a legal basis for processing special categories of personal data for detecting and correcting bias in AI systems (new Article 4a, AI Act). While framed as narrowly scoped and with strict controls, the new provision can significantly expand the circumstances under which sensitive data may be processed, including by AI providers and deployers beyond high-risk systems.

From a consumer perspective, this raises serious concerns. The proposed conditions under which AI providers and deployers can process sensitive data **rely heavily on their self-assessment**, including assessments that bias mitigation "cannot be effectively fulfilled" using other data.

The argument that more sensitive data is needed to prevent discrimination is also problematic, as it **normalises the large-scale collection of data that can expose consumers to heightened risks** without their knowledge or meaningful control. Yet, existing research demonstrate that bias can be detected and mitigated using other methods that do not require the collection of such data (e.g. XAI methods), in line with the principle of data minimisation.[5]

Moreover, the distinction between processing sensitive data for "bias detection" and using it for model training or optimisation is blurred in practice. **Once collected, such data creates strong incentives for broader reuse, undermining the principles of data minimisation and purpose limitation**.

Key concepts such as "effectiveness" and "state-of-the-art security measures" **remain undefined**, and there is no **clear mechanism for independent verification or oversight**. In addition, in complex AI supply chains involving cloud services and subcontractors, it will be difficult to enforce the guarantees that are meant to prevent sensitive data from being reused or shared.

[5] For instance, Explainable AI in Algorithmic Trading: Mitigating Bias and Improving Regulatory Compliance in Finance https://www.researchgate.net/publication/390170221_Explainable_AI_in_Algorithmic_Trading_Mitigating_Bias_and_Improving_Regulatory_Compliance_in_Finance

Recommendation

BEUC welcomes the objective of promoting bias detection yet **cautions against it becoming a general justification for expanding the processing of special categories of personal data.** This would risk undermining core GDPR principles and exposing consumers to disproportionate risks.

BEUC recommends to either **reject this change or strictly limit its scope to exceptional and clearly defined cases**, with additional safeguards of compliance and oversight. Priority should be given to privacy-preserving technical solutions that address bias without expanding the collection and use of sensitive personal data.

2. Registration obligations for AI high risk systems must remain

The Commission proposes to delete the obligation for providers to register high-risk AI systems in the EU database which fall under the exemption of Article 6(3) AI Act. Removing the obligation in Article 49(2) together with Article 6(4) AI Act **would remove the only transparency and accountability mechanism attached to the self-exemption regime.**

The self-exemption regime under Article 6(3) AI Act allows providers to unilaterally conclude that an AI system which otherwise meets the criteria for high-risk classification does not pose a significant risk to health, safety or fundamental rights. **This self-assessment mechanism has been highly contested during the legislative process precisely because of its potential for misuse[6]:** in October 2023, BEUC and more than 100 civil society organisations signed an open letter on the risks of AI systems deployers to exempt themselves of such rules as a critical loophole in the AI Act.[7]

The registration obligation under Article 6(4) was introduced as a minimum safeguard. This requires providers to submit the basic information and reasoning upon which the exemption relied upon in the system.

Removing this obligation would significantly weaken oversight and reduce market transparency. Without registration, supervisory authorities or civil society would no longer be able to monitor how frequently exemptions are used, in which sectors or Member States, or whether patterns of systemic misuse are emerging. This would

[6] AI Act – BEUC's recommendations ahead of third trilogue, 2 October 2023: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-125_AI_Act%E2%80%93BEUCs_recommendations_ahead_of_third_trilogue.pdf

[7] EU legislators must close dangerous loophole in AI Act: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-109_EU_legislators_must_close_dangerous_loophole_in_AI_Act.pdf

seriously undermine the AI Act's function as a product safety and risk governance framework. It would also complicate independent scrutiny and enforcement, weakening the effectiveness of **collective redress mechanisms**, including actions brought under the Representative Actions Directive (RAD).

In addition, **the lack of transparency risks distorting competition in the internal market.** Providers that fully comply with high-risk obligations would be disadvantaged compared to those who exploit the exemption without public scrutiny. Rather than strengthening EU competitiveness, this approach risks undermining trust in the AI regulatory framework, potentially allowing AI providers to take advantage of loopholes.

The Commission's justification based on administrative burden does not hold up, as the registration obligation **entails a minimal effort**: providers are already required to document their self-exemption internally and share this documentation with authorities upon request. **Registration merely ensures that this information is more easily accessible,** contributing to promote **transparency, accountability and fair competition**, all of which clearly outweigh the negligible administrative costs.

Recommendation

BEUC considers that the **registration obligation for self-exemptions** of Article 6(3) AI Act is a **necessary and proportionate safeguard.** Transparency is essential for effective enforcement, public accountability and fair competition in the internal market.

BEUC therefore recommends that the **deletion of the registration obligation under Article 49(2) in conjunction with Article 6(4) AI Act is rejected,** to preserve transparency, effective enforcement and consumer protection.

3. SME regulatory privileges should remain exclusive, not extended

The proposal extends the existing exemptions and simplification measures for SMEs under the AI Act to small mid-cap companies (SMCs). The changes are embedded across multiple provisions, including Articles 11(1), 17(2), 63(1), 95(4), 96(1), and 99 AIA. These measures would apply even to providers of high-risk AI systems and include simplified technical documentation, proportionate quality management systems and reduced penalties.

This extension raises serious concerns from a consumer perspective. The AI Act is a **risk-based product regulation.** This means it is designed to ensure that compliance obligations reflect the potential impact of an AI system on health, safety and fundamental

rights. **Extending SME exemptions to SMCs weakens this logic by linking regulatory obligations to a company's size rather than to the risks posed by their technology.**

However, the facts show that SMCs are fully able to develop and deploy high-risk AI systems that already affect very large numbers of consumers, for example in areas such as creditworthiness, recruitment, biometric identification or access to essential services. By reducing SMC's compliance obligations and the risk of regulatory scrutiny, the digital omnibus proposal weakens incentives to invest in compliance. As a result, the proposal risks **lowering safety standards and increasing the likelihood of consumer harm**.

It is also important to note that **mid-cap companies – based on the new EU definition – can be quite substantial organisations**[8], which have sufficient resources for dedicated compliance teams and proper compliance procedures. By applying reduced penalties and simplified obligations to SMCs, the proposal **places European SMEs and start-ups at a disadvantage**, as they will have to compete with a larger pool of better-resourced competitors.

Recommendation

Exemptions under the AI Act must remain strictly limited to genuine SMEs and must not apply to providers of high-risk AI systems based on company size alone. The AI Act must remain firmly risk based.

BEUC therefore recommends rejecting **the proposed extensions of SME exemptions to small mid-cap companies** and to ensure that high-risk AI systems have to comply fully with the AI Act, regardless of the size of the provider.

4. A concerning reversal of AI literacy obligations

The proposal modifies Article 4 AI Act on AI literacy, **shifting responsibility for AI literacy obligations from providers and deployers to Member States and the Commission**. Instead of requiring companies to ensure that staff operating AI systems have a sufficient level of AI literacy, the amendment merely obliges public authorities to encourage such measures. This difference will impact how strict enforcement can be, how far liability goes and what compensation or remedies consumers can claim under the AI Act.

[8] As defined by the European Commission in accordance with Recommendation 2003/361/EC, SMCs are enterprises with between 250 and 750 employees, with an annual turnover not exceeding €150 million.

This change risks undermining the AI Act's role as a product safety and accountability framework. **AI literacy is a basic precondition for the safe development, deployment and use of AI systems**. Staff who do not understand how AI systems function, what data they rely on and what risks they pose are less able to prevent misuse, bias, discrimination or harmful outcomes, particularly in consumer-facing contexts.

Transforming a (already limited) obligation into a non-binding encouragement sends a **problematic signal to the market which weakens accountability**. In practice, the difference between a duty to "ensure" and a general encouragement will be decisive for enforcement, liability and consumer redress once the AI Act is applied. This is especially concerning for deployers who integrate off-the-shelf AI systems into real-world settings without having sufficient internal expertise to assess risks and impacts.

The current lack of enforcement cases is not a justification for weakening the provision, as it merely reflects the early stage of implementation and the fact that market surveillance structures are still being put in place. Removing this safeguard now risks pre-emptively lowering standards before its importance can be properly assessed in practice.

Recommendation

AI literacy is an essential element of safe and responsible AI deployment and a necessary safeguard for consumers' fundamental rights. Responsibility for ensuring adequate AI literacy **must remain with providers and deployers**, who are best placed to train their staff.

BEUC therefore recommends **rejecting the proposed change** to maintain a clear obligation on providers and deployers to ensure sufficient AI literacy. Any encouragement by public authorities should complement, not replace, binding industry obligations.

5. Clarify the governance and enforcement framework

The proposed changes to Articles 75 and 77 AI Act significantly reshape how the law is enforced by expanding the role of the AI Office and changing the cooperation mechanisms with national supervisory authorities.

The proposed changes to Article 75 AIA would give the AI Office direct supervisory and enforcement powers over two key types of AI systems:

1. Those based on general-purpose AI models where the model and system are developed by the same provider.
2. Those AI systems that are integrated into or constitute Very Large Online Platforms (VLOPs) or Search Engines (VLOSEs) under the Digital Services Act (DSA).

The Commission would also be empowered to define the enforcement powers of the AI Office, including the imposition of fines, through implementing acts, and to organise or delegate pre-market conformity assessments.

Such changes to the institutional framework should strengthen, not complicate, the ability of authorities to investigate harmful AI practices and ensure that **consumers can benefit from effective protection and redress.** From a consumer perspective, this centralisation raises concerns about accountability, transparency and the effectiveness of oversight. While strong EU-level enforcement can address risks posed by powerful market actors, it must not weaken the role of national authorities. For consumers**, national authorities are often the first point of contact** and play a key role in **identifying harmful practices in practice**.

While the amendments to Article 75 AI Act expand the AI Office's responsibilities by giving it direct supervisory and enforcement powers, it does not address existing issues such as a lack of capacity and resourcing. **However, we note that the AI Office is still in the process of becoming operational** which has come with challenges in fulfilling its existing coordination and oversight tasks with the current allocated resources. Adding direct supervisory and enforcement powers over complex and highly technical AI systems **requires significant additional expertise, staffing and financial resources.** Without adequate resourcing, there is a real risk that enforcement will **become slower and less effective**, creating bottlenecks at EU level and weakening consumer protection in practice.

At the same time, changes to Article 77 AIA should not make **enforcement more complex and less accessible.** There is a potential risk that fundamental rights authorities would no longer be able to directly request information or documentation from AI providers or deployers but would instead have to submit a "reasoned request" to market surveillance authorities, which would act as intermediaries. Introducing this additional procedural step should not create delays and turn market surveillance authorities **into gatekeepers, rather than facilitators of enforcement**. In cross-border cases – involving AI systems deployed across several Member States – this structure could lead to **significant bottlenecks**. Authorities may need to coordinate through multiple market surveillance bodies with different procedures and priorities, delaying investigations and making timely intervention more difficult. This change therefore risks making the AI Act more difficult to enforce and reduces the chances that harmful practices affecting consumers will be identified and addressed quickly.

Moreover, although Article 77(1a) AIA provides that market surveillance authorities "shall grant" access to information. This obligation is expected to facilitate the tasks oof these authorities and bodies, but it is subject to unspecified conditions which, if not clarified, risks legal uncertainty and inconsistent application. This would further undermine effective oversight and enforcement.

Recommendation

The effective enforcement of the AIA requires a balanced approach combining strong EU-level oversight with efficient, direct involvement of national authorities responsible for market surveillance and consumer protection. Any **increased centralisation must not undermine accessibility, timeliness or the practical enforceability** of the rules.

BEUC therefore recommends clarifying the changes to **ensure that any expanded role of the AI Office is accompanied by clear safeguards, transparency, adequate resourcing and accountability.**

At the same time, **national authorities and relevant bodies must retain direct and effective access to information held by AI providers and deployers**, without unnecessary procedural barriers or gatekeeping. The conditions under which **access to information may be restricted must be clearly defined** to avoid delays and legal uncertainty.

6. Reconsider the "Stop-the-Clock" approach

The Commission proposes to change the currently defined application timeline for high-risk AI obligations. The proposal **introduces a conditional mechanism under which key obligations would apply only after the Commission confirms that supporting compliance tools**, such as standards, are available.

In addition, by postponing the application of high-risk AI obligations under Article 111 AIA, the proposal also **delays the associated labelling and transparency requirements for providers**, including those under Article 50 AIA. Under the new approach, high-risk AI systems would have to comply six months (Annex III AI Act) or twelve months (Annex I, AI Act) after such a Commission decision. If no decision is adopted, the application of the rules would be automatically delayed until 2 December 2027 for Annex III systems and 2 August 2028 for Annex I systems.

The Commission's proposed delays for key obligations related to high-risk AI systems and to the temporarily suspension of transparency and labelling requirements is **based exclusively on industry calls to halt the implementation of the AI Act** due to harmonised standards necessary for compliance not being available in time. However, civil society and standardisation organisations' have consistently denounced that the industry actors calling for a "stop the clock" are the same who are mainly responsible for delaying this process of standardisation.[9]

Despite the growing industry narrative that this proposal is a widely agreed, necessary update of the timeline to ensure compliance, we recall that this proposal has been contested from its inception**. BEUC,** together with a broad range of stakeholders from civil society to lawmakers[10] and industry[11,12] **has opposed this proposal to pause the AI Act's implementation from the start**, as simply pausing the implementation could lead to serious consequences for consumer rights, protection of fundamental rights and the overall integrity of the EU digital legal framework.

This pause is problematic from a consumer perspective as it would **delay the implementation of protections within high-risk AI systems and create uncertainty** about when these protections will effectively apply. As a result, consumers will remain exposed to the risks posed by high-risk AI systems for a significantly longer period. without the safeguards foreseen by the AI Act. In particular, postponing obligations related to high-risk AI undermines transparency and makes it difficult, if not impossible, for consumers to recognise when they are subject to AI-driven decisions.

In addition, **without clear labelling of high-risk AI systems, consumers cannot properly exercise their rights under the AIA**. Without clear labelling, it will be difficult to identify whether an AI system is being used for decision-making or generating content. As a result, consumers cannot properly assess if online information is reliable, request explanations of AI-based decisions, or lodge complaints with authorities. **This also severely limits the effective enforcement of existing prohibitions on unacceptable AI practices**, which formally apply but cannot be meaningfully identified or challenged in practice without transparency obligations.

The same concerns apply to the **proposed suspension of labelling obligations for generative AI systems**. Without clear disclosure that content is AI-generated or manipulated, consumers are left unable to assess the reliability of information, particularly in sensitive contexts such as advertising, influencer marketing or

[9] Civil Society, Industry, Academics, Experts Open Joint Letter against the Delaying and Reopening of the AI Act, 9 July 2025: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-066_Open_Joint_Letter_against_the_Delaying_and_Reopening_of_the_AI_Act.pdf

[10] Financial Times, EU lawmakers warn against 'dangerous' moves to water down AI rules: https://www.ft.com/content/9051af42-ce3f-4de1-9e68-4e0c1d1de5b5

[11] For instance, see TIC Council's position as the umbrella organisation representing the certification industry organisations in Europe. https://www.tic-council.org/news-and-events/news/tic-council-releases-recommendations-digital-omnibus-ai

[12] Open Joint Letter against the Delaying and Reopening of the AI Act, 9 July 2025. https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-066_Open_Joint_Letter_against_the_Delaying_and_Reopening_of_the_AI_Act.pdf

disinformation. In the long-term, this weakens transparency, accountability and trust in digital markets.

Recommendation

At the very minimum, **transparency obligations** (i.e. labelling of high-risk and generative AI systems and consumers' right to receive explanations of AI-based decisions), **should apply from the original date foreseen** in the AI Act.

BEUC therefore recommends **reconsidering the deadline extensions** and to ensure that core transparency and accountability safeguards remain in place. **At the very least,** any extension should be **unconditional, strictly limited in time, and non-renewable**. It should only be a temporary and exceptional measure, without encouraging for further delays or regulatory uncertainty.