

Why it matters to consumers

The EU AI Act was designed to ensure safety, transparency and ethical deployment of AI systems across the EU while protecting consumers' fundamental rights. The AI Omnibus, however, risks undermining these protections, exposing consumers to heightened risks and more legal uncertainty. By weakening core safeguards, it threatens to erode consumers' trust in digital products and services. Trilogues must ensure that these protections are preserved and strengthened, not compromised.

This paper summarises BEUC's recommendations for trilogue negotiations on the AI Omnibus. For more information, see our [position paper](#), the [Commission's proposal](#), the [EU Parliament's](#) and [Council's positions](#).

Check our
position paper



TOPICS

BEUC POSITION

PRESERVING THE SCOPE OF THE AI ACT

The AI Act should remain a piece of horizontal legislation which applies to a wide range of industrial and consumer AI systems. Legislators should **reject** changes to the scope and changes to the rules determining how AI systems are classified as high-risk. It is crucial that any alternative compromise proposals do not remove and/or weaken the link between sector specific regulation and horizontal AI rules.

DELAYS IN APPLICATION

We **oppose** the proposed extension of the grace period for high-risk AI systems that have already been placed on the market and the delay of the application of the AI Act in general. Transparency requirements should apply by November 2026 (**as per the Parliament position**). In addition, co-legislators should ensure the delays in application are unconditional and non-renewable.

REGISTRATION OBLIGATIONS FOR HIGH-RISK AI SYSTEMS

The public registry requirement for self-exempted high-risk AI systems should be reintroduced (**Parliament and Council**).

However, the registration requirements should remain detailed to allow the public to check whether AI systems have been legitimately self-exempted by companies.

REGULATORY PRIVILEGES FOR SMALL AND MEDIUM-SIZED ENTERPRISES (SMES) AND SMALL MID-CAP COMPANIES (SMCS)

We **regret** the Commission's proposal to extend SMEs regulatory privileges – regarding provider obligations, conformity assessment, registration duties and enforcement mechanisms under the AI Act – to SMCs. At a minimum, SMCs should not benefit from regulatory privileges when engaging in prohibited AI practices (**Parliament**).

Only SMEs without partner or linked enterprises should be allowed to comply with simplified internal processes and documentation requirements for high-risk AI systems (known as quality management systems) (**Council**).

TOPICS

BEUC POSITION

SPECIAL CATEGORY DATA USE

Allowing the use of special category data for bias detection and correction beyond high-risk AI systems introduces significant risks for consumers. At a minimum, its scope should be strictly limited to exceptional and clearly defined cases, with strong compliance and oversight safeguards.

The text needs to clarify that non-high-risk systems will, in most cases, not meet the conditions required to process the data (**Council**). The use of special category data should in any case be explicitly prohibited for secondary purposes.

GOVERNANCE AND ENFORCEMENT

The **enforcement role and competences of the AI Office should be clarified** in the AI Act and not primarily through implementing acts (**Council**).

It is important to adequately resource the AI Office (**Parliament**) and empower the national competent authorities to initiate proceedings against Very Large Online Platforms and Very Large Online Search Engines where the Commission has not acted (**Parliament/Council**). This should be extended to other AI systems where the Commission has enforcement powers.

The text should ensure authorities' access to information without undue delay and preserve the "without prejudice" clause on authorities' powers under other laws (**Parliament**), to ensure enforcement of the AI Act does not become more complex or slow.

Any rules on imposing penalties should explicitly require such penalties to be "**dissuasive**" or "**deterrent**".

FUNDAMENTAL RIGHTS IMPACT ASSESSMENTS (FRIAS)

We **do not** support the Parliament's proposal to require cross-referencing between data protection impact assessments (DPIAs) and FRIAs, given the distinct role of FRIAs in protecting fundamental rights. Tying the two together risks watering down FRIAs in practice, reducing them to a data protection exercise and causing other fundamental rights to be overlooked.

AI LITERACY

It is crucial that AI providers and deployers continue to have literacy obligations. Co-legislators should maintain the original wording of the AI Act, or at minimum follow the **Parliament's** position to preserve AI literacy obligations for providers and deployers.

NUDIFICATION BAN

The list of prohibited practices under the AI Act should be extended to address and prevent harmful practices. However, the proposed ban on 'nudification' needs a careful assessment to avoid unintended effects. For example, this includes affecting the legality of open-source general purpose AI models, which policymakers have previously sought to avoid overregulating.