Briefing on the AI Omnibus

European Disability Forum Briefing

By Kave Noori | June 2026

A briefing explaining the AI omnibus deal and its proposed changes to the EU AI Act

EDF's advocacy and capacity-building efforts on Artificial Intelligence are possible thanks to the generous grants we have received from the European AI & Society Fund.

European Artificial Intelligence & Society Fund

Table of Contents

Introduction

The European Union adopted the Artificial Intelligence Act (the AI Act) in 2024. This law sets rules for how people design, develop, and use artificial intelligence in the European Union.

The aim of the AI Act is to reduce harm and protect fundamental rights. It focuses on AI systems that can strongly affect people's lives, such as those used in public services, employment, or access to essential support.

However, EU law-makers decided to change the law to streamline some of the rules on the already adopted act, in a so-called 'effort of simplification'. In May 2026, the European Parliament and the Council agreed on a proposal, called the AI Omnibus (available in PDF). On 16 June, the European Parliament approved the May Omnibus agreement with the Council, which must now adopt it for the AI Omnibus to take effect.

EU leaders presented these changes as technical simplifications and a change of the timeline. Many civil society organisations reached a different conclusion. We find

that the **changes weaken key human rights protections** and give greater priority to the interests of companies. In addition, the reforms are taking place against the background of pressure from technology companies as well as diplomatic pressure.

Purpose of the briefing

This briefing is written for organisations of persons with disabilities and complements more detailed legal analyses by digital rights organisations (available in PDF).

It explains what the AI Omnibus is, what it changes in the AI Act, and why those changes matter.

It is written for readers without a background in EU law or digital policy and explains how these changes can affect everyday life, including for persons with disabilities.

Readers who want more background or practical guidance can use the resources below:

- page explaining the AI Act (general overview).
- For detailed guidance and practical resources, use our guide on national implementation of the EU AI Act.

What is the AI Omnibus?

In simple terms, an omnibus proposal amends multiple laws in one package. It may change a few paragraphs in one law, several articles in another law, and bundle all these changes into one political decision.

The EU bundles multiple changes into a single legislative package, instead of updating laws through a separate process.

The AI Omnibus was presented as a way to simplify how the AI Act will be applied. In practice, it makes **several important changes to when and how parts of the AI Act apply**.

The Omnibus also has a closely linked proposal called the Data Omnibus. While the AI Omnibus focuses on changes to the AI Act, the Data Omnibus changes several EU laws on privacy and data protection.

In this case, the AI Omnibus changes parts of the AI Act, alongside related changes to other EU digital and data protection rules through the Data Omnibus.

Change 1 - Using sensitive personal data to identify and correct bias

Artificial Intelligence systems must be inclusive, accessible, and non-discriminatory. Biased AI can cause real harm to persons with disabilities. It can affect access to

work, education, social protection, healthcare, public services, and independent living.

No AI system should be developed, placed on the market, or used if it discriminates against persons with disabilities. Bias in AI systems must be identified and corrected.

However, the AI Omnibus addresses this problem in a highly problematic way.

Instead of placing stronger duties on developers and users of AI systems, the proposal makes it easier to process sensitive personal data. This is especially dangerous when the data concerns groups who already face discrimination and need stronger protection.

Under the General Data Protection Regulation, or GDPR, sensitive personal data includes information about a person's health, disability, biometric data, or political opinions. Information about a **person's disability usually counts as health data**. It should therefore receive strong protection.

The AI Omnibus would allow organisations to use sensitive personal data to identify and correct bias in AI systems **without asking people for their consent**. This would apply to AI developers and to organisations that use AI systems, such as employers, public authorities, and service providers.

It risks undermining the very goal it claims to support: less discriminatory AI.

What changes compared with the current AI Act

Under the current AI Act, providers of high-risk AI systems must test their systems for bias. Providers are companies or organisations that develop AI systems.

The AI Omnibus expands who is covered by the rule. It no longer applies only to developers of high-risk AI systems, but also to providers and deployers of AI systems at all risk levels.

The proposal includes some limits. Organisations may only use sensitive data if anonymised or synthetic data is not enough.

Synthetic data is data that is artificially created instead of collected directly from real people. One type of synthetic data is generated from real datasets. It creates fictional people while preserving key patterns in the original data. For example, a real person called Anna, aged 35 and working as an electrician, could be replaced by a fictional person called Betty, aged 36 and working as a plumber.

However, synthetic data may still reproduce the same biases, gaps, or incorrect assumptions as real-world data.

Organisations must use the sensitive data only for bias testing. They must not reuse it for other purposes or share it with third parties.

This makes the permission much broader than in the current AI Act. Many more organisations could rely on this rule to process sensitive personal data for bias testing.

This is a major expansion. The obligation to test for bias still mainly concerns providers of high-risk AI systems, but the permission to use sensitive personal data could reach much further.

What this means in simple terms

In simple terms, the changes mean the public interest in detecting and correcting bias can be more important than a person's right to refuse the use of their sensitive personal data.

The law adds protections that are meant to prevent misuse. But these rely heavily on the organisations that want to use the data.

Why is this problematic?

Fixing bias in AI systems matters. AI systems must not discriminate against persons with disabilities.

But this change makes it **easier to collect and use very sensitive personal data** on a large scale. That creates serious risks.

The safeguards are weak. In practice, companies and public bodies would often decide for themselves when sensitive data is needed. They would also decide how much data they can use, and whether they have stayed within the limits.

The permission is also too broad. It does not only apply to AI developers. It also applies to employers, public authorities, and other organisations that use AI systems. These organisations could decide that there may be a bias problem and use that as a reason to process sensitive data.

This is not a change that civil society or human rights bodies called for. It was **mainly pushed by industry**.

Equality and human rights networks, including the European Network of Equality Bodies (Equinet) and the European Network of National Human Rights Institutions (ENNHRI), have warned that this approach risks normalising the large-scale collection of sensitive data.

Children's rights organisations have raised the same concern. In a joint letter on the Digital Omnibus on AI, more than 80 children's rights, family, and mental health organisations and experts warned against allowing children's personal data to be used for AI training, bias detection, or mitigation. They called for children's data to be **explicitly excluded from the proposed new Article 4a**. Their warning reinforces the same principle: the law should not protect people from discrimination by making it easier to process more data about them.

The deeper problem is that the Omnibus treats more data processing as a solution to discrimination, even for groups who need stronger protection. It is giving organisations a broad legal permission to process sensitive data in the name of bias testing. **Without strict limits, this risks turning inclusion into extraction.**

Developers and deployers could use sensitive data from persons with disabilities to improve AI systems without giving people meaningful choice, consent, control, or fair compensation.

This matters because disability-related data can be deeply personal and economically valuable. In AI developed for sign language, data may include a person's face, body movements, facial expressions, and signing style. In speech recognition, data may include the voices of people with atypical speech patterns.

These are not neutral data points. They are part of a person's body, identity, communication, and lived experience. If such data is used to train or improve AI systems, the people who provide it should not be treated as free raw material.

This is contrary to the idea of inclusive design under equal conditions. Inclusive design should mean that persons with disabilities help shape technology on fair terms. It should not mean that they provide the data, carry the risks, and lose control, while others own and profit from the resulting systems.

Bias mitigation must not become a loophole for unpaid data extraction.

AI should not discriminate. But fixing bias must not become an excuse to collect more sensitive data than necessary. Data collected for one reason is often later used for another. A rule saying "do not reuse it" is not enough if no one checks whether organisations follow it.

This is especially worrying because the Omnibus is part of a wider reform that aims to reduce obligations for businesses. Fundamental rights protections should not be weakened in that process.

Change 2 - Changes to the role of anti-discrimination bodies and other Article 77 authorities

This change affects public bodies that protect fundamental rights, such as equality bodies. Under Article 77 of the AI Act, these bodies play an important role when high-risk AI systems may harm people's rights.

Under the current AI Act, these authorities can ask providers or deployers of high-risk AI systems directly for relevant documents and information. The AI Omnibus changes this approach. **These requests now have to go through the market surveillance authority .**

The text also says that this change does not affect any powers these bodies may have under other EU or national laws. In other words, it only limits how they can request information under this specific provision of the AI Act. It does not automatically remove other legal routes to access information.

At the same time, the Omnibus requires the market surveillance authority to act without undue delay. Where necessary, it must obtain the requested information from the provider or deployer and share it with the Article 77 authority. The text also calls for close cooperation and mutual assistance between the authorities.

What this means in simple terms

This means that these specific authorities tasked with protecting human rights, the equality bodies, will have a harder time accessing information and analysing if AI systems are breaching fundamental rights.

Why is this problematic?

This change is particularly concerning because the AI Act is designed as a product safety law, not as a human rights law.

Under the logic of the AI Act, discrimination or bias caused by an AI system is treated as a defect in a product. It is regulated in a similar way to a technical fault in a physical product, such as a defective light bulb. The authority responsible for detecting and correcting such defects is the market surveillance authority.

Market surveillance authorities mainly have technical and product-compliance expertise. They are not specialised in equality law, discrimination, or human rights.

Because AI systems can seriously affect fundamental rights, the AI Act recognises this limitation. It gave authorities that protect fundamental rights an advisory role and, crucially, a direct right to access technical documentation from AI providers and deployers. **This direct access is essential for them to fulfil their mandate effectively.**

EDF agrees with the concerns about this change expressed by Equinet and ENNHRI. The AI Omnibus weakens this design. By removing the direct access route, fundamental rights authorities become dependent on the market surveillance authority to act on their behalf. This creates several risks:

Requests for information may be delayed or filtered.

Access depends on the capacity and willingness of the market surveillance authority.

If market surveillance authorities are overstretched, fundamental rights authorities may be unable to act effectively to protect marginalised groups.

As a result, expertise on discrimination and human rights is pushed further away from the centre of enforcement, even though discrimination is one of the most serious risks posed by high-risk AI systems. This is done in the name of making the law more efficient and streamlined.

Change 3 - Delayed rules for high-risk AI systems

What are high-risk AI systems?

The AI Act classifies some AI systems as high-risk. These are systems that can seriously affect people's rights, opportunities, and access to essential services.

High-risk AI systems include AI used to make or support decisions about who gets a job or is rejected, who is admitted to a university or training programme, who receives a bank loan, and who has access to social benefits or public services.

The AI omnibus delays the application of rules for high risk AI systems, including those listed in annex III of the AI Act.

For people affected by AI-driven decisions today, this means that **several important safeguards will remain out of reach for now.** In the meantime, high-risk AI systems can still shape decisions about people's jobs, benefits, education, or access to services without the full legal protections the AI Act was meant to guarantee.

Stand-alone high-risk AI systems (Annex III)

These are AI systems used on their own, for example in recruitment, education, lending, or social security decisions. Under the original AI Act, the main obligations would have applied from **2 August 2026**. Under the AI Omnibus, this is delayed to **December 2027**.

Embedded high-risk AI systems (Annex I)

These are AI systems that are part of products already regulated under other EU laws. Examples include AI inside a toy covered by EU toy safety rules, AI inside a vehicle covered by vehicle safety legislation, or AI inside a medical device covered by medical device laws.

Under the original AI Act, the rules would have applied from **2 August 2027**. Under the AI Omnibus, this is delayed to **August 2028**.

Change 5 - Weaker obligations on AI literacy

The AI Act originally required organisations to ensure that people involved in using and overseeing AI systems have a sufficient level of AI literacy.

Under the AI Omnibus, this obligation has been weakened. Organisations now only need to **support** AI literacy efforts, **rather than ensure** that people operating AI systems actually have the necessary understanding.

Why this matters

- People often tend to over-rely on AI recommendations, especially when they are presented as "objective" or technical.
- AI systems often reflect very normative assumptions about what is "normal" or "efficient".

For example, a **public official deciding on disability-related benefits may rely too heavily on an AI recommendation** if they lack experience in disability support and do not feel confident questioning the system. This can lead to unfair or inappropriate decisions that are hard to challenge.

Change 6 - Registration of exempted high-risk AI systems (a small but important safeguard)

One important safeguard was preserved during the Omnibus negotiations.

Under the original AI Act, if a company claims that its AI system is not high-risk, despite normally falling under that category, it must still register that system in the EU public database.

This applies to the so-called filtering rule. In simple terms, this rule allows some AI systems listed in Annex III to be treated as not high-risk if they do not pose a significant risk and do not meaningfully influence decisions about people.

This can include systems that perform narrow procedural tasks, support a decision already made by a human, detect patterns without replacing human judgement, or prepare information for a later assessment.

Preparatory tasks could include organising documents, sorting applications, or collecting information before a person makes the final decision.

This is vital because it creates a minimum level of transparency. It allows public authorities and civil society to know these systems exist, and it limits the risk that companies could quietly exempt themselves from the AI Act without scrutiny.

However, this safeguard has been weakened. Originally, companies had to register more detailed information. Now, they must still register, but with less detail. This leaves us with a weaker, but still important, layer of transparency that survived the Omnibus process.

Threats ahead

Leading EU politicians have indicated that more 'omnibus' revisions of the EU digital rulebook intending to 'simplify' it may follow in the coming years. This is deeply concerning.

It suggests that **the weakening of protections in the AI Act is not a one-off event**, but part of an ongoing process. At the same time, AI systems are being used in more and more areas of daily life. Weakening the rules that are meant to protect people from discrimination and human rights harms in this context is **irresponsible**.

The result is a higher risk that people will be harmed without effective legal protection. It also creates space for companies with poor practices to operate without breaking the law, because the law itself increasingly permits harmful behaviour. Over time, this can undermine trust in AI as a technology.

This is particularly regrettable because AI can also bring real benefits. If people lose trust in AI systems, they may avoid using them even in situations where AI could support inclusion, accessibility, or better decision-making.

There is also another serious risk that this article has only touched on. The Data Omnibus includes proposals that would weaken the General Data Protection Regulation. This Regulation is a cornerstone of fundamental rights protection in the digital environment, including for AI systems. Changes to this framework raise additional concerns about discrimination, misuse of personal data, and reduced safeguards. These proposals deserve close scrutiny, but a full analysis falls outside the scope of this briefing.

As one of the architects behind the AI Act, Dr Laura Caroli writes that the most serious threats to fundamental rights may not be in the AI Omnibus itself, but in the Data Omnibus. In her view, the broader deregulatory shift is centred on proposals to weaken the General Data Protection Regulation and e-Privacy rules that protect personal data from misuse by AI systems. She warns that these changes could have the most far-reaching consequences for AI and fundamental rights, including by narrowing the definition of personal data and treating AI training as a legitimate interest for data processing.

These proposals deserve very close scrutiny.

References for further reading

- Council of the EU press release on the AI Omnibus agreement
  Official summary of the political agreement between the Council and the European Parliament on changes to the AI Act, including simplification measures and new timelines.
- Equinet and ENNHRI joint statement on equality, human rights, and the Digital Omnibus proposals
  Joint statement by equality bodies and national human rights institutions warning that the Digital Omnibus proposals could weaken equality, data protection, and fundamental rights safeguards.
- Children's rights joint letter on the AI Omnibus and children's personal data
  Letter from children's rights, family, and mental health organisations warning against allowing children's data to be used for AI training, bias detection, and mitigation.
- European Union of the Deaf book on sign language and artificial intelligence
  Explains risks and opportunities linked to sign language AI, including consent, representation, linguistic rights, and the use of sign language data.
- ECNL analysis of the AI Omnibus and risks for fundamental rights
  Civil society analysis explaining why the AI Omnibus raises concerns for fundamental rights, democratic accountability, and meaningful participation in law-making.
- Sky News article on industry pressure and the weakening of EU AI rules

News report on concerns that EU AI rules are being weakened under pressure from industry and international political actors.

- Guardian article on pressure from technology companies and the United States to weaken the AI Act
  News report on lobbying and diplomatic pressure to reduce or delay parts of the EU AI Act.
- European Commission review of prohibited and high-risk AI systems under the AI Act
  Official Commission review under Article 112 of the AI Act, including the identified gap on AI systems that generate non-consensual intimate content.
- Dr Laura Caroli's analysis of what the EU AI Omnibus changes and what may come next
  Analysis by Dr Laura Caroli explaining the AI Omnibus changes and warning that the Data Omnibus may pose even greater risks to fundamental rights and data protection.

Document credits

Commented [KN1]: @Andre Felix Andre, you have made this document so much better. I think you desrve cred here too. Where should we put you?

Commented [AF2R1]: Thanks so much! I added myself as the editor, if that's okay.

This document was prepared by Kave Noori

Assisted/Supervised by Marine Uldry and Alejandro Moledo

Edited by André Félix

The European Disability Forum
Mundo Madou
Avenue des Arts 7-8
1210 Brussels, Belgium.

www.edf-feph.org

info@edf-feph.org

EDFs advocacy and capacity building efforts on Artificial Intelligence are possible, thanks to the generous grants we have received from the European AI & Society Fund.