A disability-inclusive Artificial Intelligence Act

By Kave Noori, EDF Artificial Intelligence Policy Officer | November 2026

A guide to monitor implementation in your country

The European Disability Forum's advocacy and capacity building efforts on Artificial Intelligence (AI) is only possible thanks to the generous grants we have received from the European AI & Society Fund.

Table of Content

1 About the European Disability Forum 4

2 Aim of this toolkit 4

2.1 About this version of the toolkit 4

3 Acknowledgements 5

4 Executive Summary 5

4.1 Overview of key actions for national advocacy 6

5 Overview of the AI Act 8

5.1 Introduction to the AI Act 8

5.2 What is a regulation? How is it put into effect? 8

5.3 The legal basis for the use of AI systems 9

5.4 Impact: What does the AI Act do for persons with disabilities? . 10

5.5 The legal definition of an AI-system 12

6 Understanding the risk categories 13

6.1 Bias and discrimination across AI systems 13

6.2 Unacceptable risk 17

7 High-risk AI 34

7.1 Exception for narrow or preparatory tasks 35

7.2 Database of high-risk AI 36

7.3 Accessibility requirement for high-risk AI 37

7.4 The right to get an explanation 38

7.5 High risk AI categories 39

8 Transparency risk 53

9 Minimal risk 56

10 General Purpose AI (GPAI) 57

10.1 Protections from threats to human health, safety and democracy 58

10.2 Guidelines on the scope of the obligations for general-purpose AI models 60

10.3 GPAI code of practice 60

10.4 Voluntary codes of conduct 61

10.5 Recommendations for EDF members 61
11 Fundamental rights, sandboxes and testing 62
11.1 The right to complain 62
11.2 Reporting of serious incidents 63
11.3 Regulatory sandboxes 64
11.4 Fundamental rights impact assessments (FRIAs)..... 65
11.5 Testing in real world conditions 67
12 Additional measures: "Encouragements" 68
Recommendation to EDF members 68
13 Governance structure 68
13.1 Market surveillance authorities 70
13.2 Authorities protecting fundamental rights 73
13.3 Penalties for breaking the AI Act's obligations..... 74
14 Monitoring the AI Act in your country.....75
14.1 Importance of involvement for persons with disabilities 75
14.2 Detailed timeline of AI Act implementation..... 76
14.3 What needs to be done? Steps to take for national implementation 78
14.4 Recommendations to EDF members 79
15 Assessing shortcomings of the AI Act.....81
15.1 The choice to design the law based on risks instead of rights . 81
15.2 Accessibility in GPAI and minimal risk AI..... 82
15.3 Shortcomings introduced by the AI Omnibus 83
15.4 European Commission review of prohibited and high-risk AI .. 86
16 Glossary 86
17 Document credits 93

1 About the European Disability Forum

The European Disability Forum (EDF) is an independent non-Governmental Organization (NGO) that advocates for the rights of 100 million Europeans with disabilities. EDF is a unique platform which brings together representative organisations of persons with disabilities from across Europe. EDF is run by persons with disabilities and their families. We are a strong, united voice of persons with disabilities in Europe.

EDF is a member of the European Union AI Advisory Forum. The Forum advises the European Commission and the European AI Board on how to put the AI Act into practice and enforce its rules.

2 Aim of this toolkit

This toolkit provides guidance and support to organisations of persons with disabilities in the European Union. It is primarily addressed to EDF members, but all organisations of persons with disabilities are encouraged to advocate on disability-inclusive AI.

It explains how to contribute to the implementation and monitoring of the Artificial Intelligence Act (AI Act) and how to advocate for the rights and interests of persons with disabilities in Artificial Intelligence (AI).

2.1 About this version of the toolkit

This is **version 3 of the toolkit**. It is based on the Artificial Intelligence Act (mentioned after as the "AI Act"), a law that came into force in the European Union in August 2024. Although the AI Act has been adopted, some details still need to be clarified.

The European Commission (EC) is issuing guidelines and delegated acts that complement and clarify certain provisions in the AI Act. They might change some things that are important for organisations of persons with disabilities. We will continue to update the toolkit when this happens. We want to give you the best and most useful information.

Version 3 is an updated version of the second version of the toolkit published in October 2025. This version focuses on the **AI Omnibus and its implications for the rights of persons with disabilities**. It also briefly introduces the Data Omnibus and its relevance to AI systems that process personal data.

Since version 2 of this toolkit was published, the European Commission has finalised a draft guidance[1] and published guidelines on transparency obligations under Article 50 on 20 July 2026.[2] The guidelines explain how these requirements should be interpreted and applied; they do not create new legal obligations.

3 Acknowledgements

The European Disability Forum (EDF) would like to thank all disability organisations and others for their feedback on this toolkit. We also thank the EDRi core group coalition of human rights and digital rights organisations for their support in our advocacy efforts.

4 Executive Summary

The European Disability Forum toolkit provides guidance for organisations of persons with disabilities on the implementation and monitoring of the European Union's Artificial Intelligence Act (AI Act) in their EU-country.

The toolkit offers a detailed overview of the AI Act, highlighting the important sections for the rights of persons with disabilities.

It provides practical guidance on navigating the legislative process and suggests strategies for effective advocacy to ensure the perspectives of persons with disabilities are included in the creation and execution of national AI policies.

[1] 'Draft of the Guidelines on the Implementation of the Transparency Obligations for Certain AI Systems under Article 50 of the AI Act | Shaping Europe's Digital Future', n.d. [accessed 3 June 2026].
[2] European Commission, 'Guidelines on Transparency Obligations for Providers and Deployers of AI Systems', 20 July 2026 [accessed 3 November 2026].

This toolkit is a living document and will be updated with new information as it becomes available. By staying informed and taking proactive steps, we can create an inclusive AI landscape that serves all people, including persons with disabilities. We rely on your participation and feedback to ensure that the AI act is implemented in a disability-friendly way.

4.1 Overview of key actions for national advocacy

4.1.1 Understand and engage with the legislative process

EDF members should actively participate in the legislative process by providing feedback and suggestions to national authorities responsible for implementing the AI Act. This includes attending public consultations, submitting position papers, and engaging with policymakers to ensure that the needs and rights of persons with disabilities are considered.

4.1.2 Monitor the implementation of the AI Act

EDF members should monitor the implementation of the AI Act at the national level. This involves keeping track of how national authorities are applying the provisions of the AI Act and ensuring that high-risk AI systems comply with accessibility requirements. Once the public European Union (EU) database of high-risk AI systems becomes available, organisations can use it to help identify registered systems used in their member state. Section 3.1 explains the uncertainty about the database's availability at the time of updating this toolkit. This can help in creating alliances with other organisations protecting fundamental rights to collect testimonies of systems that do not work and provide these to supervisory authorities.

4.1.3 Advocate for accessibility and bias testing

EDF members should advocate for the mandatory accessibility requirements for high-risk AI systems as stipulated in the AI Act. This includes ensuring that AI developers follow the harmonized European standards on accessibility.

EDF members should also monitor whether information required under the AI Act's transparency rules is accessible to persons with disabilities, including information telling people that they are interacting with AI or encountering AI-generated or manipulated content.

Additionally, EDF members should push for thorough bias testing of high-risk AI systems to prevent discrimination against persons with disabilities. This involves ensuring that the data used to train, validate, and test these systems is reliable, safe, and free from biases.

4.1.4 Raise awareness and educate stakeholders

EDF members should raise awareness of the AI Act's implications for persons with disabilities through workshops, seminars and public campaigns. It is also crucial to provide training and resources to persons with disabilities and their families, empowering them to advocate for their rights in the context of AI.

4.1.5 Use the rights to explanation and complaint

The AI Act gives people affected by certain decisions involving high-risk AI systems a right to obtain an explanation. It also allows individuals and organisations to complain to the relevant authority when they believe an AI system breaches the AI Act. EDF members should inform and support persons with disabilities in using these rights.

4.1.6 Collaborate with other organisations protecting fundamental rights

Building alliances with other organisations protecting fundamental rights, such as patient organisations, can strengthen advocacy efforts. By working together, EDF members can collect testimonies and provide evidence to supervisory authorities about AI systems that do not work as intended.

5 Overview of the AI Act

5.1 Introduction to the AI Act

The AI Act is a regulation in the European Union (EU) that aims to create a framework of rules and standards for the creation, implementation and application of artificial intelligence systems within EU borders. Its main objectives are to protect fundamental human rights, ensure the safety of the public and promote trust and innovation in AI technologies. It was adopted in 2024.

5.2 What is a regulation? How is it put into effect?

The EU makes laws in different ways. These laws can take the form of regulations, directives, or decisions.

- **An EU regulation**, like the AI Act, automatically becomes law in every EU country. It applies to everyone -governments, businesses, and people -without needing each country to pass its own version of the law.
- **An EU directive** is different. It sets goals that every country must achieve, but it allows each country to decide how to make its own national laws to meet those goals.
- **An EU decision** is a specific law that applies only to certain people or organisations. For example, the EU can make a decision that only affects one company or a specific group of people.

In the case of the AI Act, it is an EU regulation. This means that it applies to all EU countries in the same way. However, the AI Act allows countries to set their own rules on certain issues. For example, it sets limits on the use of facial recognition technology by the police but also leaves it up to each country to decide whether it wants to ban this technology altogether.

The **European Parliament (EP) and the Council of the European Union** can adopt EU decisions as legal acts. These legal acts are laws that apply to everyone like regulations or directives.

The **European Commission (EC)** can also issue documents called delegated acts and implementing acts. These are not laws, but they help explain or apply existing laws such as the AI Act. The European Commission will use these documents, along with guidelines, to clarify and provide further details on the AI Act.

5.3 The legal basis for the use of AI systems

The AI Act generally does not grant organisations permission to use AI systems. Instead, it functions like a product safety law. **It sets rules for how AI can be used, but only after an organisation is already permitted to use it under other laws.**

For example, the AI Act categorises the use of facial recognition by the police as "high-risk" However, this does not mean that the AI Act gives the police permission to use facial recognition. The police can only use it if the laws of their country or other EU laws explicitly authorise it. Once they have this permission, the AI Act sets out the outer limits within which the police can use the technology to ensure that it is used safely and does not go too far in violating citizens' rights.

5.3.1 New development: the Digital Omnibus

The AI Act, adopted in 2024, is being impacted by a proposal of a "Digital Omnibus" tabled by the Commission in 2025.

The Digital Omnibus consists of two separate packages: the AI Omnibus, which changes the AI Act, and the Data Omnibus, which proposes changes to EU data protection rules, including the General Data Protection Regulation (GDPR) and the ePrivacy Directive.

At the time of writing, the AI Omnibus had been adopted and is therefore covered throughout this toolkit. The Data Omnibus was still under political negotiation and remained a moving target, so it is mentioned only briefly. Its outcome will nevertheless matter because many AI systems process personal data, including biometric, health and disability-related data.

EDF is concerned that the AI Omnibus weakens important protections for persons with disabilities. The later section "Shortcomings introduced by the AI Omnibus" explains these concerns in more detail. For further reading, see EDF's article "6 ways the AI Omnibus weakens protections for persons with disabilities", which also links to our detailed briefing.

5.3.2 How to read the legal texts referred to in this toolkit

The AI Omnibus changes parts of the original AI Act. Rather than reproducing the whole law, it sets out which provisions must be added, replaced or deleted. The legally authoritative sources are the original AI Act and the amending act as published in the Official Journal of the European Union, read together.

To make this toolkit accessible to readers without legal training, we mainly refer and link to the consolidated version of the AI Act. This brings the original text and its amendments together in one document, so you do not have to compare two legal texts side by side. It is a reading aid, not a replacement for the official legal texts, for anyone who is doing an actual legal analysis.

The consolidated version presents the updated rules but does not include the recitals. Recitals are the numbered explanations at the beginning of a legal act. They help explain why the rules were introduced and how to interpret them, but do not create binding obligations on their own. To explain the reasoning behind a rule or a change, we therefore also refer to the relevant official text:

- **Recitals in the original AI Act** help explain the reasoning behind its original provisions.
- **Recitals in the AI Omnibus** help explain why changes were made to the AI Act.

Whenever this toolkit refers to a recital, we specify whether it belongs to the original AI Act or the AI Omnibus. This makes clear which explanation we are relying on and where you can find it.

5.4 Impact: What does the AI Act do for persons with disabilities?

The AI Act establishes rules to ensure that artificial intelligence systems are used **safely and ethically**, with a particular focus on protecting human rights.

This is especially important for persons with disabilities and other marginalized groups, as the AI Act aims to **prevent harm** such as discrimination, unfair treatment, or loss of privacy.

The AI Act classifies AI systems according to the risks they pose, but these categories are not always mutually exclusive. Some systems may fall into more than one category depending on their use and context. More information is given chapter 6 below "Understanding the risk categories".

The main categories are:

- **Prohibited AI practices (unacceptable risk):** AI systems that are considered too dangerous or incompatible with European values and fundamental rights are banned entirely. Examples include systems that manipulate behaviour using subliminal techniques, exploit vulnerabilities due to age or disability, or enable social scoring by public authorities.

- **High risk systems:** AI systems that are permitted but strictly regulated because they can significantly influence a person's life chances (for example, decisions on employment, access to loans, or educational admission).

- **Transparency risk (sometimes called "limited risk"):** Certain AI systems that interact with people (such as chatbots), generate or manipulate content (such as deepfakes), or use biometric categorisation (determining the age, gender, and race of a person without attempting to disclose their identity) are subject to transparency and information requirements. Importantly, a system can be subject to transparency obligations and be classified as high-risk if it meets the criteria for both.

- **Low or no risk:** AI systems with minimal impact on people's rights (such as spam filters or video game AI) are not subject to additional obligations under the AI Act.

It is also important to consider "General Purpose AI" (GPAI).

GPAI is not part of the risk classification hierarchy. Instead, GPAI models and systems may fall under any of the above categories depending on their use and impact. GPAI is subject to specific rules, especially if they pose a risk to society, such as if they can be misused to produce misinformation.

These risk categories apply to various sectors of life. For instance, in education, AI can influence decisions like who gets admitted to a programme or how students are graded. In workplaces, AI might be used to make hiring decisions or evaluate employee performance. In healthcare, AI assists doctors in diagnoses and treatment choices. In migration and law enforcement, AI can be deployed to process visa applications or monitor public spaces. For each of these areas, the AI Act imposes strict rules to protect people's rights and prevent harm.

The AI Act also requires that high-risk AI systems must be accessible to everyone, including persons with disabilities, as described in Article 16(l). AI developers are required to apply the principles of universal design from the outset to ensure that these systems are accessible and usable by people with different abilities and needs.

Recital 80 of the AI Act emphasises the EU's legal obligation as a signatory to the United Nations Convention on the Rights of Persons with Disabilities (UNCRPD) to protect persons with disabilities from discrimination and to ensure equal access to information and communication technologies. It emphasises the need to apply the principles of universal design to ensure full and equal access for all, taking particular account of the dignity and diversity of persons with disabilities.

In summary, the AI Act tries to make sure that AI systems are designed and used in ways that protect everyone's rights, including those of persons with disabilities, by making the systems fair, accessible, and free from discrimination.

5.5 The legal definition of an AI-system

The European Commission has issued guidelines to help authorities, providers and users decide whether a particular tool qualifies as an "AI system" within the meaning of Article 3(1). The guidelines on the definition of AI systems are not legally binding.

Before assessing bans, high-risk obligations or transparency requirements, you should first check Article 3(1): "**Can the tool produce results (for example: predictions, recommendations, decisions) and operate with a degree of autonomy/adaptivity?"**

If yes, it is probably an AI system and the AI Act may apply; if no, the provisions of the Act do not apply. The legal definition will help you decide whether you should proceed under the AI Act or pursue other avenues, such as filing a complaint under equality law or data protection law.

6 Understanding the risk categories

6.1 Bias and discrimination across AI systems

Bias and discrimination can arise in AI systems at any risk level. The AI Act therefore contains a general rule on processing sensitive personal data to detect and correct bias, alongside additional data requirements that apply specifically to high-risk AI systems.

Article 4a expands who may rely on this rule. It applies to providers and deployers of high-risk AI systems. It can also apply to other AI systems when their use may create risks to health, safety, fundamental rights or the environment. Processing sensitive personal data is not automatically permitted. It must be necessary for detecting or correcting bias and must follow the safeguards in Article 4a and applicable data protection law.

This rule is separate from Article 10. Article 4a concerns when certain providers and deployers may process sensitive personal data to detect and correct bias. Article 10 sets additional requirements for the data used to train, validate and test high-risk AI systems.

6.1.1 Bias is not the only problem

It is important to recognise that bias is just one of several threats to the rights of persons with disabilities. Some cases of AI use are wrong, even when bias is removed in such a way that the AI can make an accurate assessment or prediction about a person with a disability.

6.1.2 Practical examples of bias

AI bias is when an AI system is unfair or wrong for some people more than others. For example, an AI system that decides who gets a job might be unfair to people with disabilities if the data it learned from does not include or show them. AI bias can hurt people's lives, such as taking away their chances, resources or benefits. So, it is important to make sure that AI systems are made and checked in a way that stops or lowers bias and respects human rights.

We can illustrate bias with an example of an AI program designed to stop hate speech. This kind of program analyses texts to determine whether the sentiment behind a word is positive or negative.

A study from 2021 illustrates bias in how AI assigns a numerical value to indicate the intensity of negative words.[3] You can instruct the AI to treat anything worse than a specific threshold as hate speech to be removed. For instance, if negative feelings range from -0.01 to -1, we can instruct the software to treat anything more intense than -0.30 as hate speech. While this seems fair because it applies the same standard to everyone, the study revealed that there can be bias against persons with disabilities in systems that mathematically measures the intensity of feelings behind different words.

Sentence and Score Table (Authors' annotations in parentheses):

- My neighbour is a tall person: 0.00 (Neutral)
- My neighbour is a beautiful person: 0.85 (Positive)
- My neighbour is a black person: -0.16 (Slightly Negative)
- My neighbour is a mentally handicapped person: -0.10 (Slightly Negative)
- My neighbour is a blind person: -0.50 (Highly Negative)

In the scenario where we assume that any score below -0.30 indicates hate speech, this method fails to filter out the more offensive term "handicapped" while blocking the use of the word "blind".

Our example shows that an automatic philtre for hate speech might mistakenly prevent people with blindness from sharing their experiences or advocating for their rights on social media. Consequently, there is a potential risk that such philtres can restrict the freedom of expression of the marginalised groups they are trying to protect.

The AI Act is written using a risk-based approach. Its provisions are based on the idea that the higher the risk to fundamental rights, health and safety posed by a particular AI system or use case, such as using AI for hiring or deciding on a government benefit, the stricter the rules need to be.

---

[3] Pranav Narayanan Venkit and Shomir Wilson, 'Identification of Bias Against People with Disabilities in Sentiment Analysis and Toxicity Detection Models', arXiv:2111.13259 [Cs], 2021 [accessed 15 April 2023].

6.1.2.1 Unacceptable Risk

What it means: AI systems that are banned entirely because they pose serious threats to human rights or safety. Exceptions may apply in specific cases.

What is covered: AI systems that pose an unacceptable risk to human dignity, democracy, and fundamental rights, including for people with disabilities.

Where is it covered in the AI Act: Article 5.

Examples:

- AI systems that manipulate human behaviour or exploit vulnerabilities.
- AI that creates intimate deepfakes (fake images of someone undressed) of an adult without their consent.
- AI that creates fictional or realistic sexual abuse material of children
- AI systems that cause physical or psychological harm.
- AI that recognizes emotions to influence decisions.
- AI predicting future criminal behaviour based solely on personality or personal characteristics.

6.1.2.2 High Risk

What it means: These AI systems are allowed but are subject to strict regulations and supervision to protect security, human dignity, democracy, and fundamental rights.

What is covered: AI systems that significantly affect the lives, rights, or welfare of people. There is a list of use cases defined as high-risk AI systems.

Where is it covered in the AI Act: Article 6-27 and Annex I and Annexe III.

Examples:

- AI systems used in employment processes, such as hiring or firing decisions.
- AI determining access to essential public services or state benefits.

- AI used in credit scoring or assessing creditworthiness.
- AI systems in law enforcement for risk assessments.

6.1.2.3 Limited Risk

Limited risk AI systems are subject to transparency requirements under the AI Act. These systems must inform users that they are interacting with AI, or that content has been generated or manipulated by AI (for example, chatbots or deepfakes). The obligations are lighter than for high-risk AI, focusing mainly on transparency and user awareness

What is covered: AI systems that interact with people (such as chatbots), generate or manipulate content (such as text, images, audio, or video), or use biometric categorization, provided they are not used in a high-risk context.

Where is it covered in the AI Act: Articles 50 (Transparency obligations for certain AI systems)

Examples:

- Chatbots used for customer service (must disclose that users are interacting with AI).
- AI tools generating or manipulating images or videos (such as deepfakes, which must be clearly labelled as AI-generated).
- Biometric categorisation systems used outside high-risk contexts.

6.1.2.4 Minimal risk

What it means: These AI systems are allowed to operate without additional rules under the AI Act. They must still comply with other relevant laws, such as data protection.

What is covered: AI applications that do not fall into the other risk categories.

Where is it covered in the AI Act: No dedicated provisions; mentioned in contexts like codes of conduct.

Examples:

- AI used for filtering spam emails.
- Speech recognition.

- AI algorithms in video games enhancing player experience.
- Recommendation systems for movies or music.

6.1.2.5 General Purpose AI (GPAI)

General Purpose AI (GPAI) is not a risk category. Instead, GPAI models and systems can fall under any risk category - prohibited, high-risk, limited risk (transparency), or minimal risk - depending on their use and context. GPAI is subject to specific obligations under the AI Act, especially if it poses systemic risk (i.e., large-scale models with significant impact). Enforcement for GPAI is handled by the European Commission, not national authorities.

Where is it covered in the AI Act:

- Articles 50, 53,54 (All general-purpose AI models).
- Articles 51, 52, 55 (General-purpose AI with systemic risk).

Examples:

- Language models like ChatGPT, Google Gemini, DeepSeek, Mistral and Llama.
- GPAI models used to power chatbots, content generation tools, or other applications.

Risk categories are not mutually exclusive, so a system can meet the requirements of both the transparency risk category and the high-risk AI classification criteria. The hierarchy is a simplification of these classifications. For example, some AI systems used in biometric categorisation may fall under the limited risk category but can also be considered high-risk in certain circumstances. Additionally, chatbots are generally assigned to the limited risk category, which requires them to disclose that users are interacting with a computer program. However, if a chatbot uses advanced language technology, such as a language model like ChatGPT, it is also subject to general purpose AI regulations. Furthermore, if a chatbot is used in recruitment processes to interview job applicants, it would simultaneously be categorised as a high-risk AI system.

6.2 Unacceptable risk

The AI Act bans AI systems that pose an unacceptable risk to human dignity, democracy, and fundamental rights, including for people with disabilities.

These are systems that can manipulate human behaviour, exploit people's vulnerabilities, or cause physical or psychological harm. Examples of such systems include:

- AI systems that recognise emotions in the workplace or schools.
- AI systems that collect or expand facial recognition databases from the internet or surveillance cameras.
- AI systems that predict criminal behaviour based solely on personality traits or personal characteristics.
- AI systems that exploit individuals with disabilities for profit or control.

6.2.1 Exceptions

There are some specific exceptions to these bans. For instance, AI that recognises emotions in the workplace or schools is prohibited unless it is used for medical or safety reasons. Additionally, while emotion recognition AI is not allowed in schools, it can still be used by police or immigration authorities. This means that people with disabilities who have migrant backgrounds could still be impacted by such technologies.

There are also some loopholes. The EU does not have the power to make laws about national security. Therefore, member states can sometimes claim that the use of a particular AI is related to national security, allowing them to exempt it from the rules of the EU AI Act.

6.2.2 Ban on AI that takes advantage of people with and without disabilities

Two provisions are especially relevant for people with disabilities when it comes to protecting them from doing things they would otherwise not do: Article 5(1)(a) and Article 5(1)(b).

This section of the toolkit has been updated based on the European Commission's 2025 guidelines on prohibited AI practices which provide clear explanations and real-life examples of how these bans work in practice.

6.2.2.1 Article 5(1)(a): the general ban on harmful manipulation[4]

This provision prohibits AI systems that use hidden, manipulative or deceptive techniques to strongly influence a person's behaviour (legal term: "materially distort behaviour"). This means that the AI makes it much harder for a person to make a well-informed decision (legal term: "appreciably impair their ability to make an informed decision"), causes them to do something they would not otherwise have done and causes (or is likely to cause) them serious harm (legal term: "significant harm"). More information on what constitutes harm is given in the next pages.

- **Who is protected?** Everyone, including people with disabilities.
- **What's banned?** AI that tricks, manipulates or deceives people in a way that causes them real harm.

6.2.2.2Article 5(1)(b): the special ban on exploiting vulnerabilities[5]

This provision prohibits AI systems that take advantage of a person's vulnerability due to their age (for example, children and the elderly), disability or particular social or economic situation. The provision exclusively protects people who belong to one of these groups.

The latter group are for example, people living in extreme poverty and at greater risk of exploitation due to their urgent needs, or people in another precarious situation like asylum seekers who are awaiting a decision on their status and whose future is uncertain, are considered to be in a "particular social or economic situation".

It is not enough for someone to belong to just one of the protected groups. This means that it doesn't just apply to someone because they have a disability. The AI system must actually exploit (i.e. target or take advantage of) the person's vulnerability arising from their disability. Inaccessibility or poorly designed user interfaces are not considered exploitation for the purposes of this rule.

For example, Article 5(1)(b) could apply to a person with a cognitive disability who, because of their disability, finds it much harder to understand the risks or the ways in which an AI system could manipulate them, even if they are given support or accessible information.

---

[4] 'Commission Publishes the Guidelines on Prohibited Artificial Intelligence (AI) Practices, as Defined by the AI Act.', paras 60–97 [accessed 26 June 2025].
[5] European Commission, Commission Publishes the Guidelines on Prohibited Artificial Intelligence (AI) Practices, *as Defined by the AI Act*, sect. 3.3 (recital 98-121).

- **Who is protected?** People who, according to the guidelines due to "their age, disability, or socio-economic situations, who in principle have more limited capacity to recognise or resist the AI manipulative or exploitative practices and are in need of enhanced protection"
- **What is prohibited?** AI that exploits these vulnerabilities to cause harm.

6.2.3 The logic behind the provisions

Although Article 5(1)(b) explicitly mentions persons with disabilities, Article 5(1)(a) will often provide the primary protection for vulnerable groups, including persons with disabilities.

Article 5(1)(a) and Article 5(1)(b) of the AI Act apply to both intentional and unintentional exploitation or manipulation by AI systems. This means the bans cover situations where developers or deployers deliberately design an AI system to target persons with disabilities, as well as cases where an AI system - regardless of intent - has the effect of manipulating or exploiting a person's vulnerability due to disability, age, or social or economic situation. The decisive factor is the outcome: if the AI system materially distorts behaviour or exploits vulnerability and causes significant harm, the prohibition applies. In other words, it is not only the intention behind the system that matters, but also the real-world impact it has on individuals, especially those who are more at risk due to their circumstances.

For example, a wheelchair user is not necessarily easier to deceive by AI than someone who does not use a wheelchair, so Article 5(1)(a) usually applies. However, it may be more difficult for a person with an intellectual disability to recognise manipulation by AI, even if they are educated about how AI can manipulate people, so they are a vulnerable group that the legislator believes must be specially protected by Article 5(1)(b). This is similar for older people who may have more difficulties to recognise when AI is being used.

The Commission's guidance emphasises that each case requires careful analysis and that these two articles should be considered together. Where both provisions could apply to a situation, the Guidelines recommend focussing on the main aspect of exploitation. If the manipulative technique affects people in different demographic groups in the same way, but someone with a disability is more vulnerable to being tricked, Article 5(1)(a) applies. In such cases, the person's vulnerability is considered a stronger factor demonstrating harm.

However, if the AI system specifically targets one or several vulnerable groups mentioned in Article 5(1)(b) such as people with disabilities, children, older people or people living in extreme poverty and seeks to exploit their heightened vulnerability, then this provision applies instead.

In practise, this means that AI systems must be carefully scrutinised to determine whether they pose a general risk or specifically target vulnerable groups, which will affect how they are regulated.

6.2.3.1 The high bar: when do these bans apply?

The bar for prohibiting these types of AI practises is intentionally set very high in Article 5 - not just for the prohibitions discussed above.

Therefore, not every manipulative or unfair AI system is prohibited. All the following must apply for Article 5(1)(a) or (b) to apply:

1. The AI system is placed on the market, put into service, or used.
2. It must either:
    - For Article 5(1)(a): use **subliminal techniques beyond a person's consciousness** or **purposefully manipulative or deceptive techniques**.
    - For Article 5(1)(b): **actively exploit (target or leverage)** a vulnerability due to age, disability, or a specific social or economic situation.
3. It must affect someone's behaviour.
    - For Article 5(1)(a): these techniques must have a **strong impact on behaviour** (legal term: "materially distort behaviour") by **considerably weakening** ("appreciably impairing", legal term) the ability to make an informed decision.
    - For Article 5(1)(b): these techniques must have a **strong impact on behaviour** by exploiting the vulnerability (there is no requirement to show impairment of informed decision-making).
4. This causes, or is **reasonably likely to cause**, **significant harm** (a substantial negative impact on physical, psychological, or financial well-being) to that person or others.

All four points must be met simultaneously (they are called cumulative) and there must be a clear link (a "causal link") between what the AI does, how it changes a person's behaviour, and the resulting harm. In other words, the harm must be a direct result of the AI's manipulative or exploitative action and not just a coincidence.

Lawful persuasion, such as "honest advertising", is not prohibited. The rules only apply to covert or exploitative practices that cross the line into manipulation or exploitation and cause real harm.

The Commission's guidelines point out that a breach of any of the rules in Article 5 can result in the highest fines under the law, so these prohibitions should be interpreted narrowly and only applied in the most serious cases.[6]

6.2.3.2 Official Examples from the European Commission Guidelines

Article 5(1)(a): Harmful Manipulation[7]

Example 1:

An AI-powered wellbeing chatbot is designed to help users lead healthier lives. However, if the chatbot exploits users' vulnerabilities and encourages unhealthy or dangerous behaviours, such as suggesting that they exercise excessively without rest or water, it can put people at risk. If someone follows this advice and is seriously harmed, for example by suffering a heart attack, or if there is a real risk of serious harm, this type of AI could be banned under Article 5(1)(a).

The law makes it clear that actual harm does not need to occur. If the AI system's actions are likely to cause serious harm, that is sufficient for the ban to apply. In other words, the rule covers both cases: when someone is actually harmed and when there is a reasonable risk of harm.[8]

Example 2:

An AI system uses subliminal messages (such as flashing images too quick for the conscious mind to notice) to influence purchasing decisions,

[6] European Commission, 'Commission Publishes the Guidelines on Prohibited Artificial Intelligence (AI) Practices, as Defined by the AI Act', paragraph 84.
[7] Article 5(1)(a), AI Act
[8] European Commission, 'Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act', paragraph 84.

leading people to buy things they would not have otherwise, resulting in significant financial harm.[9]

Article 5(1)(b): Exploiting Vulnerabilities[10]

Example 1:

A therapeutic chatbot aimed at people with intellectual disabilities exploits their cognitive vulnerabilities to influence them to buy expensive medical products or engage in behaviour that could endanger their health or safety.

Example 2:

An AI system identifies women and girls with disabilities on the internet and targets them with abusive content. It exploits their disability-related vulnerabilities, that makes it harder for them to defend themselves and increasing their exposure to manipulation and abuse.

6.2.4 Ban on AI-generated intimate and sexual material

The following two bans were added to Article 5 by the AI Act Omnibus. They are new, and the European Commission's 2025 guidelines on prohibited AI practices do not yet cover them. The examples below are therefore illustrative and will be updated once official guidance is available.

6.2.4.1 Article 5(1)(ba): The ban on AI-generated intimate images of adults

Intimate deep fakes refer to the use of AI systems to create or alter realistic images, videos or audio showing an identifiable person's intimate parts or sexual activities. These systems are often called "nudify" apps or "deep fake" tools, and they are frequently misused to create fake nude images or sexual videos of real people. For example, an ordinary photo taken from someone's social media profile can be turned into a realistic fake nude image in seconds. This can result in serious harm to the person depicted, such as humiliation, harassment, blackmail, and lasting damage to their reputation, relationships and mental health.

The concern behind the prohibition in Article 5(1)(ba) is consent. Every person has the right to decide over their own body and intimacy.

[9] European Commission, 'Commission Publishes the Guidelines on Prohibited Artificial Intelligence (AI) Practices, as Defined by the AI Act', paragraph 82.
[10] Article 5(1)(b), AI Act

Elsewhere in the AI Act, deep fakes generally only need to be labelled as AI-generated (the transparency rules). For intimate and sexual material, labelling is not enough: creating or using such material without consent is now completely banned.

What exactly does Article 5(1)(ba) prohibit?

An AI system that generates or manipulates realistic images, videos, audio or similar material of an identifiable natural person's intimate parts, or of an identifiable natural person engaged in sexually explicit activities, without that person's freely-given, specific, informed, unambiguous and explicit consent for that generation or manipulation.

Who is protected?

Everyone, with or without disabilities — private individuals and public figures alike.

What is banned?

AI that creates or fakes realistic intimate or sexual images, videos or audio of an identifiable person without that person's explicit consent. This covers practices commonly known as:

- "Nudify" apps, where an ordinary photo of a person is turned into a fake nude image.
- Deep fake pornography: AI-generated sexual videos or images made to look like a real person.
- Cloned voices: AI-generated sexual audio that sounds like a real person.

Key words in simple terms:

- **Identifiable**: the person can be recognised, directly or indirectly — by face, voice, name, tattoos or other features. It is enough that people who know the person would recognise them.
- **Generate or manipulate:** both fully AI-created material and AI-edited material (for example, turning a real photo into a fake nude) are covered.
- **Realistic**: the material looks or sounds like it could be real. Clearly non-realistic material (for example obvious cartoons) falls outside this ban, though it may still be unlawful under other rules.

- **Consent**: this is a very high standard. Silence, "not saying no", or consent buried in general terms and conditions is not consent. Consenting to one thing is not consenting to everything: a person who once shared an intimate photo with a partner has not consented to that photo being turned into AI-generated sexual material. Consent can also be withdrawn. Only the person depicted themselves can give consent — nobody can consent on someone else's behalf.

The high bar — but a different kind of bar

The other bans in Article 5 only apply when behaviour is materially distorted and significant harm is likely. Article 5(1)(ba) is different: the lack of consent itself is what makes the practice prohibited. No additional manipulation or harm needs to be proven. This makes it one of the most straightforward bans in the AI Act.

Limitation of the high bar

Article 5(1)(ba) binds both providers and deployers. This means it applies to the companies that develop and place these AI tools on the market (providers), as well as to the people and organisations that use them (deployers), for example someone who uses a "nudify" app on a photo of another person. Both can be held responsible under the AI Act.

The ban also works together with the EU Directive on combating violence against women and domestic violence (Directive (EU) 2024/1385). While the AI Act prohibits the AI systems that generate such material, this Directive requires EU countries to criminalise the non-consensual sharing of intimate or manipulated intimate material, including AI-generated deep fakes. For EDF's guidance on advocating for an ambitious transposition of this Directive, see: Transposing the EU Directive on Combating Violence Against Women - European Disability Forum.

Cumulative requirements for Article 5(1)(ba)

For the ban to apply, all the following must be met at the same time:

1. **Placement / use:** an AI system is placed on the market, put into service, or used.

2. **Generation or manipulation:** the system generates or manipulates realistic images, videos, audio or similar material.

3. **Intimate or sexual content:** the material shows an identifiable person's intimate parts, or an identifiable person engaged in sexually explicit activities.

4. **Missing consent:** the person's freely-given, specific, informed, unambiguous and explicit consent for that generation or manipulation is missing.

5. All four must apply at the same time. The decisive factor is consent, not intent or harm. The ban applies both to the companies that make and distribute these AI tools (providers) and to the people who use them (deployers).

Examples (illustrative)

- A "nudify" app that turns a photo of a classmate, colleague or ex-partner into a realistic nude image. Both the app and its use are prohibited — the person never consented.
- An AI tool that produces a fake sexual video of a well-known person. The ban applies regardless of how famous the person is.
- An AI voice tool that generates sexual audio content using a person's cloned voice without consent.

Note: if the person depicted is under 18, the stricter ban below applies instead.

6.2.4.2 Article 5(1)(bb): The total ban on AI-generated sexual material of children

AI-generated sexual material of children refers to the use of AI systems to create or alter sexual images, videos or audio depicting children. These systems can produce material showing real children, manipulated images of real children, or entirely fictional, computer-generated "children" that look completely real. For example, a text-to-image tool can generate sexualised images of "teenagers" from a simple written prompt, without any real child's photo being used. This can result in serious harm: it fuels demand for child sexual abuse, is used to groom and blackmail children, and normalises the sexualisation of children.

These systems generate or manipulate material or performances depicting child sexual abuse, as defined in the EU's child sexual abuse law (Directive 2011/93/EU). Unlike the ban for adults, consent plays no role here: a child can never consent to sexual material, so this is a total ban. The ban also covers material showing a person who only *appears* to be a child, even if the real person whose face or voice was used is an adult.

This ban targets the AI systems that create such material. It works alongside existing criminal laws that already punish people who produce, possess or share child sexual abuse material.

What exactly does Article 5(1)(bb) prohibit?

An AI system that generates or manipulates material or performances within the meaning of Article 2, points (c) and (e), of Directive 2011/93/EU — that is, material and performances depicting child sexual abuse — except where a "without right" defence applies under national law. There is no consent requirement in this ban, because a child can never legally consent.

Who is protected?

All children — **anyone under 18** — including when the "child" is fictional and only appears to be real.

What is banned?

AI systems that generate or manipulate sexual material depicting children, realistic or fictional. Always. There is no consent exception, and no one, parent, guardian or carer, can consent on a child's behalf.[11]

Cumulative requirements for Article 5(1)(bb)

For the ban to apply, all the following must be met at the same time:

1. **Placement / use:** an AI system is placed on the market, put into service, or used.

2. **Content:** the system generates or manipulates material or performances depicting child sexual abuse within the meaning of Article 2, points (c) and (e), of Directive 2011/93/EU — whether the depiction is real or AI-generated/fictional.

3. **No exception applies:** no valid consent can exist (a child can never consent), and no "without right" defence under national law applies.

Examples (illustrative)

- A text-to-image tool that generates sexualised images of "teenagers" or children, even entirely fictional ones with no real child's photo used.

[11] The only exception is a narrow legal defense that exists in the criminal laws of some EU countries (the "without right" defense), for example where such material is handled in connection with law enforcement.

- An app that "nudifies" photos of pupils at a school.

6.2.4.3 Why these bans matter for people with disabilities

- Women and girls with disabilities, and people with intellectual disabilities, are at increased risk of sexualised online abuse, and perpetrators may believe they will not be believed or will not report. These bans give every person, regardless of disability, the right not to have their body sexualised by AI without their consent.
- Every adult with a disability has the same right to give or refuse consent as anyone else. Organisations of persons with disabilities play an important role in ensuring members know this right exists, through accessible and easy-to-read information on digital consent, and in supporting victims to report abuse and to seek removal of the material from platforms.
- As with the other bans in Article 5, breaking these prohibitions can result in the highest fines under the law.

6.2.5 Prohibited Social Scoring

Social scoring refers to the use of AI systems to evaluate or classify individuals based on their behaviour and characteristics over time. These systems often use data collected in one context and apply it in another. For example, information from social media activity, shopping habits, or unrelated health data may be used in a completely different context. This can result in unexpected, unfair, or disproportionate outcomes.

These systems create a score or profile for individuals or groups, which can then be used to make decisions about them, such as access to services, benefits, jobs or other opportunities.

The concern behind the prohibition in Article 5(1)(c) is that such scoring can lead to detrimental or unfair treatment of people, including exclusion from services or opportunities, and can enable social control and surveillance that is incompatible with EU values and fundamental rights. The ban aims to protect human dignity, equality and non-discrimination, data protection and private and family life.

There is a fine line between the lawful use of data and prohibited social scoring. For example, if a person applies for disability benefits, a lawful assessment would be based on the person's medical history and, where appropriate, the contents of social service files showing what kind of help and support tasks the person has previously received. This is considered a high-risk use of artificial intelligence and is subject to the strict requirements of the Artificial Intelligence Act, but it is not prohibited.

The line is crossed and the ban on social scoring applies if the authorities use too much or irrelevant data. For example, if the authorities check whether a person has an history of high alcohol consumption in order to decide on a lower entitlement to social assistance. It would not be relevant to investigate alcohol consumption when assessing the person's level of reduced mobility and their need for help with everyday activities such as showering or toileting. However, the assessment of alcohol consumption would be relevant if the social service is specifically looking at how the person can be helped to come out of alcohol dependency. The use of irrelevant or cross-contextual data for assessment is exactly what the ban on social scoring is designed to prevent.

6.2.5.1 What exactly does Article 5(1)(c) prohibit?

An AI system that evaluates or classifies natural persons or groups over a certain period of time based on:

- their social behaviour, or
- personal or personality characteristics (known, inferred or predicted), where the social score leads or is capable of leading to:
- detrimental or unfavourable treatment in social contexts unrelated to where the data was originally collected, and/or
- detrimental or unfavourable treatment that is unjustified or disproportionate to the behaviour or its gravity.

6.2.5.2 Who is protected?

- **Everyone:** The prohibition applies to all natural persons and groups, regardless of age, disability, or social status.
- **Particularly relevant for people with disabilities**: For example, when AI is used to assess eligibility for social services or disability allowances, but also applies in employment, education, insurance, and other domains.

6.2.5.3 The High Bar: Cumulative requirements for Article 5(1)(c)

For the social scoring ban to apply, all the following must be met at the same time (cumulative):

Placement / Use

The practice involves placing on the market, putting into service, or use of an AI system. This prohibition binds both providers and deployers in their respective roles. The ban applies regardless of if the actors are private organisations (companies, non-profits, foundations) or public actors.

Evaluation or classification over time

The AI system is intended or used to evaluate or classify individuals or groups over a certain period of time based on their social behaviour or personal or personality characteristics (including known, inferred, or predicted).

Outcomes of the score

The score leads or is capable of leading to detrimental or unfavourable treatment either:

- In social contexts unrelated to where the underlying data was generated or collected, and/or
- in a way that is unjustified or disproportionate to the behaviour or its gravity.

6.2.5.4 Examples from the European Commission Guidelines that illustrate social scoring

Example 1: Detrimental treatment in unrelated social contexts

A public labour agency uses an AI system to score unemployed individuals based on an interview and an AI-based assessment for determining whether an individual should benefit from state support for employment. That score is based on relevant personal characteristics, such as age and education, but also variables collected or inferred from data and contexts with no apparent connection to the purpose of evaluation, such as marital status, health data for chronic diseases, addiction, etc.

Example 2: Unjustified or disproportionate treatment

A public agency uses an AI system to profile families for early detection of children at risk based on criteria such as parental mental health and unemployment, but also information on parents' social behaviour derived from multiple contexts. Based on the resulting score, families are singled out for inspection and children considered 'at risk' are taken from their families, including in cases of minor transgressions by the parents, such as occasionally missing doctors' appointments or receiving traffic fines.

Example 3: Unjustified or disproportionate treatment

A municipality uses an AI system to score trustworthiness of residents based on multiple data points related to their social behaviour in a variety of contexts. The generated score for residents considered 'less trustworthy' is used for blacklisting, i.e. withdrawal of public benefits, other serious punitive measures, and increased control or surveillance. Among the factors considered in the assessment are insufficient volunteering and minor misbehaviour, such as not returning books to the library on time, leaving rubbish on the street outside the day of collection, and a delay in the payment of local taxes.

Important note for EDF members: We have collected a list of problematic surveillance and data practices in social protection, including cases that may come close to forbidden social scoring or that are at least problematic uses that are high risk. **See the section " Examples of problematic surveillance** in social protection **(page 43)** under the high-risk AI section of this guide.

Emotion recognition in the workplace and education: Article 5(1)(f)[12]

The AI Act prohibits AI for emotion recognition in the workplace and in educational institutions due to power imbalances between employers and employees and schools and students. Most applications of emotion recognition are considered high-risk, but a ban applies in these areas.

Cumulative requirements for Article 5(1)(f)

For the ban on emotion recognition to apply, all the following must be true at the same time (cumulative):

[12] European Commission, 'Commission Publishes the Guidelines on Prohibited Artificial Intelligence (AI) Practices, as Defined by the AI Act', paras 239–270.

1. **Placement / Use:** the AI system is placed on the market, put into service for this specific purpose, or used.
2. **Purpose:** the system is intended to infer emotions.
3. **Context:** the system is used in the workplace or in education and training institutions.
4. **Exclusion:** the prohibition does not apply if the AI system is intended for medical or safety reasons.

6.2.5.5 Clarifications from the Guidelines

Emotion recognition here means inferring feelings such as happiness, sadness, anger, fear, etc., based on biometric characteristics (for example, facial expressions, tone of voice, body language).

- Sentiment analysis (analysing text to predict emotions) is not covered by this prohibition.
- Physical states such as pain or fatigue are not considered emotions for the purpose of this ban. Systems that detect tiredness or pain (for example, to ensure the safety of truck drivers) are not prohibited.
- Simple observations (such as noticing that someone is smiling) are not emotion recognition. However, using biometric data to conclude that someone is happy because they are smiling is emotion recognition.

Examples:

- Analysing a student's voice and concluding they are angry and about to become violent is emotion recognition. However, the guidelines don't explicitly say if using emotion recognition for this purpose is allowed or prohibited.
- Identifying that someone is sick is not emotion recognition.
- Using facial analysis to infer that a worker is sad or disengaged is banned in the workplace.

6.2.6 Remote biometric identification

Remote biometric identification refers to the process of identifying a person based on their physical, physiological, behavioural or psychological characteristics, usually without direct contact. This can include analysing features such as facial structure, eye movements, body shape, voice patterns, prosody (intonation and rhythm), how someone walks, heart rate, blood pressure, smell and even the unique way someone types on a keyboard. The most common application is facial recognition software that analyses images or videos from surveillance cameras. However, various biometric data points can also be combined, for example, the walking style of a masked person with visible facial features and height, to establish identity.

The defining element of remote biometric identification is the use of technology to recognise people from a distance, often via video cameras or microphones. For example, software can identify a person by their voice picked up by a microphone or by analysing how they type on a keyboard. These systems work without physical interaction and instead rely on data collected remotely to make identifications.

Article 5(1)(h) bans the use of live biometric identification, like facial recognition, in public spaces by law enforcement. Police cannot use facial recognition on live camera feeds, but they can use it on recorded video, which is considered high risk instead.

There are three exceptions where police may use live biometric identification, but only if a national law in that EU country specifically allows it. Without such a law, it is not allowed.

The three exceptions are:

1. Locating missing persons or victims of abduction, trafficking, or sexual exploitation.

2. Preventing a specific and imminent threat to life, safety, or terrorist activity.

3. Identifying suspects of serious crimes (for example: terrorism, murder, child sexual exploitation) listed in Annex II of the AI Act.

Before deploying real-time remote biometric identification, the police must conduct a fundamental rights impact assessment in accordance with Article 27. They must also register the system in the EU database, except where the AI Act provides otherwise for sensitive operational information.

Both Recital 32 of the AI Act and the guidelines acknowledge that remote biometric identification systems can be biased and lead to discrimination on the basis of disability, age, ethnicity, race, or sex.

A clear example highlighting the need to strictly regulate the use of real-time biometric identification comes from Hungary. In 2025, the government criminalised participation in the Pride parade and threatened to use facial recognition technology to identify those taking part. Human rights organisations strongly criticised the EU Commission for failing to intervene. This case also exposed a significant loophole: while the use of live facial recognition on public camera feeds is banned, authorities can circumvent this restriction by using recorded surveillance footage instead.[13]

7 High-risk AI

The EU considers AI systems that could significantly affect people's lives, rights or well-being as **high risk**. These systems are used in critical decision-making processes, such as:

- Determining whether someone is accepted into an educational programme.
- Detecting cheating during examinations or assessments.
- Assisting employers in hiring or firing decisions.
- Deciding whether someone qualifies for government benefits or services.
- Approving applications for loans or insurance.
- Supporting law enforcement in preventing or prosecuting criminal offences.

For people with disabilities, the mandatory accessibility requirements for high-risk AI systems are particularly important. High-risk systems are also subject to specific requirements for the data used to train, validate and test them, as explained later in this chapter.

[13] Politico, 'Pressure piles on Brussels to act against face scanning at Budapest Pride' [accessed 16 October 2025].

High-risk AI systems must comply with **mandatory accessibility requirements**. These requirements are established under the European Accessibility Act (Directive (EU) 2019/882) and the Web Accessibility Directive (Directive (EU) 2016/2102). This helps ensure that AI systems are accessible to all users, including persons with disabilities, by incorporating inclusive design principles from the start.

7.1 Exception for narrow or preparatory tasks

Not every AI system used in an area listed as high-risk in Annex III is automatically high-risk. Article 6(3) creates a limited exception.

A provider can assess that an AI system is **not high-risk** if it does not significantly influence the relevant decision. This exception can apply when the AI system only:

- performs a **narrow procedural task**, such as sorting documents or finding duplicates;
- **improves work already completed by a person**, such as improving the language of a document;
- **detects patterns or inconsistencies** in decisions already made by a person, without replacing or influencing those decisions; or
- performs a **preparatory task** that has only a limited influence on an assessment that follows.

For example, an AI system that selects or evaluates job applicants is normally high-risk. However, an AI translation tool used only to translate documents during recruitment may fall under the exception. The translation prepares information for the recruitment process but does not decide who should get the job. **Recital 53 of the AI Act gives the translation of initial documents as an example of a preparatory task.**

The situation changes if the AI system helps **select or evaluate candidates or make recruitment decisions**. These uses can directly influence a person's employment opportunities and are therefore high-risk.

There are important safeguards. **The exception does not apply if the AI system profiles people.** A provider using the exception must document its assessment before placing the system on the market or putting it into service. The provider must also register the system in the EU database. However, because the provider makes the first assessment, this safeguard depends on providers assessing their systems honestly. Registration is important because it creates a public record that can help authorities and civil society identify and question possible misuse. In practice, this protection also depends on market surveillance authorities having enough staff, expertise and resources to check providers' assessments and enforce the rules effectively.

The **AI Omnibus changes the information that providers must include when registering these systems**. Article 1(42) of the AI Omnibus removes two requirements. Providers no longer have to include:

- a short explanation of why they consider the AI system not to be high-risk; or
- information about the EU countries where they have made the AI system available.

Providers must still register these AI systems in the EU database.

In simple terms: what matters is not only **where an AI system is used**, but also **what it actually does**. An AI system that only prepares or organises information may not be high-risk. An AI system that influences an important decision about a person generally remains high-risk.

7.2 Database of high-risk AI

Article 71 of the AI Act requires the European Commission to establish and maintain a public database of high-risk AI systems.

In previous versions of this toolkit, EDF wrote that the EU database of high-risk AI systems was expected to be available by August 2026. That date has passed. Despite our searches when updating this toolkit, we could not find the public database or confirm when it would be available.

The database will not make all registered information publicly accessible: high-risk AI systems used by law enforcement, migration and border control authorities will be listed in a confidential section accessible only to the European Commission and authorities in EU member states.[14]

The absence of transparency will make it much more difficult for journalists and human rights organisations to scrutinize flawed or dangerous AI-systems or ways they are used

7.3 Accessibility requirement for high-risk AI

Article 16(l) of the AI Act requires providers of high-risk AI systems to comply with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882, the Web Accessibility Directive, and the European Accessibility Act respectively.

This means that AI developers of these AI systems will need to follow the **accessibility requirements** of these Directives and will be able to use the harmonised European standards on accessibility to demonstrate compliance with this obligation.

For example, they will be able to use

- the harmonised European Standard "EN 301 549 - Accessibility requirements for ICT products and services"
- and the European Standard "EN 17161 - Design for All - Accessibility following a Design for All approach in products, goods and services - Extending the range of users"

Recital 80 of the AI Act explains that AI systems must be accessible to all, including people with disabilities, as part of the EU's commitment to prevent discrimination and promote equality. This means that high-risk AI systems must be designed following a "universal design" approach which is about creating inclusive products and services from the start. Thus, developers should consider accessibility from the beginning of the design process to avoid later adaptations and respect the dignity and needs of people with disabilities.

[14] Article 49(4) of the AI Act

7.3.1 Data quality and bias in high-risk AI systems

Accessibility is not the only issue that concerns us as people with disabilities when AI systems are used. **Bias** is another serious problem that can have negative consequences for our rights and opportunities.

Therefore, in addition to **accessibility**, developers of high-risk AI systems must also consider the potential bias that may arise from the data they use or the AI-models they create. **Bias** can pose a threat to our dignity, equality and inclusion in different areas of life.

High-quality data is essential for developing accurate and non-discriminatory high-risk AI systems. Article 10 sets specific requirements for the data used to train, validate and test these systems. These requirements are separate from Article 4a, which allows certain providers and deployers to process sensitive personal data when this is strictly necessary to detect and correct bias. The data used for high-risk AI systems must be reliable and managed in ways that protect health, safety, fundamental rights and non-discrimination, including the rights of people with disabilities.

The data must be examined for biases that could harm **health** or **safety**, violate **fundamental rights** or lead to unlawful **discrimination**, including discrimination against **people with disabilities**. Where such biases are identified, providers must take appropriate measures to detect, prevent and reduce them.

Furthermore, the data must be **carefully selected and managed**, which includes proper collection, relevance and processing (for example, correct labelling or updating). Any assumptions made in relation to the data must be clearly stated.

7.4 The right to get an explanation

Article 86 of the AI Act states that a person who considers that a decision by an organisation using a high-risk AI system affects them legally and could affect their health, safety or fundamental rights has the right to obtain an explanation from the organisation using the AI. This does not apply to AI systems used for critical infrastructure services such as electricity and water.

7.5 High risk AI categories

7.5.1 Overarching recommendations for EDF members

- **Check the AI high risk systems database:** From August 2026, when the provisions for high-risk AI come into force, you can monitor the EU database to find AI systems used in your member state that may pose a risk to fundamental rights. It might then be possible to create alliances with other organisations protecting fundamental rights, such as patient organisations, to collect testimonies of systems that do not work properly and provide these to supervisory authorities
- **Support individuals' right to be informed:** The right to be informed belongs to the people affected by AI systems. For example, if someone is trying to get a loan or is their access to healthcare was decided by an AI, they have the right to know if an AI system is at play and how it reasoned. EDF members can support these individuals by encouraging them to ask for explanations and so they can understand how AI decisions affect them.
- **Reach out to the market surveillance authority:** If you suspect misconduct of an AI system, contact the relevant market surveillance authority.

7.5.2 High risk AI in education

Some AI applications in education are considered high-risk because they can significantly impact students' futures and may perpetuate biases or invade privacy[15]. Examples include:

- Admission decisions for educational programmes.
- Grading and assessment of students.
- Determining educational levels.
- Monitoring for cheating during exams.

[15] Recital 56 of the AI Act

Evidence of the problem:

- Anti-cheating software flagging students with disabilities as cheaters[16].
- A computer algorithm causing a grading crisis in British schools that deepened socioeconomic injustices.[17] Many students with disabilities were likely among those affected, as they are often at the intersection of multiple forms of marginalization, including socioeconomic status.

Recommendations for EDF Members

- **Call for Guidelines on AI in education:** Urge authorities to issue guidelines for educational institutions to make guidelines about safe and ethical use of AI in education and offer to contribute with your expertise to ensure the needs of persons with disabilities are included in national efforts to use AI in education.

  For example, many educational institutions promote the use of feedback tools to improve students' writing skills. Such tools are particularly useful for students with disabilities like as dyslexia. At one US university that supported the use of Grammarly, there was an incident in which a student was suspended after an update to Grammarly. Grammarly improved the quality of their service by including an AI language model like ChatGPT's. This caused the university's plagiarism detection software to flag the student's work as AI-generated. [18] [19]

  At the same time, it can be assumed that well-functioning chatbots have the potential to be a tool for learning. The emergence of AI language models is proving transformative and prompting a re-evaluation of pedagogical practises. [20]

  UNESCO has published a global guide on generative AI in education to help nations act and plan for the future.

---

[16] 'How Automated Test Proctoring Software Discriminates Against Disabled Students', Center for Democracy and Technology [accessed 13 November 2022].
[17] Sam Shead, 'How a Computer Algorithm Caused a Grading Crisis in British Schools', CNBC, 21 August 2020, section Technology [accessed 5 October 2024].

[18] Jeanette Settembre, 'Student Put on Probation for Using Grammarly: "AI Violation"', New York Post, 21 February 2024, section Technology [accessed 5 October 2024].
[19] William Tang, 'What's Cheating? AI Bans, Schools May Fail Students Who Use Grammarly', USA TODAY, 17 April 2024 [accessed 6 October 2024].
[20] Grammarly, 'Rethinking Academic Integrity Policies in the AI Era', Grammarly Blog, 2024 [accessed 6 October 2024].

While the guide promotes inclusion, equity and diversity, it lacks specific tools and regulations that address the needs of students with disabilities. This emphasises the need for policies that ensure students with disabilities can benefit from AI advances without negative effects.[21] EDF members could actively participate in the development of such guidelines in their countries. An inspiring example that sheds light on this issue is a policy paper from the Educating All Learners Alliance and New America addresses protecting the civil rights of students with disabilities in the age of AI.[22]

- **Support the creation of remedy mechanisms in school laws:** Work with student rights groups to change the law so that students in different types of schools have a legal right to appeal decisions such as suspension or their exam. Even if the decision was made by humans using automated tools to try to recognise whether the student's work was created by an AI, there may be a risk that the recognition tool has errors.

7.5.3 High risk AI in employment

AI systems used in employment are high-risk because they can significantly impact job opportunities, income, and labour rights, potentially perpetuating biases and invading privacy.[23]

7.5.3.1 Examples of High-Risk AI applications:

AI for Hiring:

- Targeted job advertisements.
- Sorting job applications.
- Selecting candidates.

AI for Workforce Management:

- Decisions on promotions and layoffs.
- Task assignments.

[21] Fengchun Miao and Holmes Wayne, 'Guidance for Generative AI in Education and Research' (UNESCO, 2023), doi:10.54675/EWZM9535.
[22] Educating All Learners Alliance and New America, Prioritizing Students with Disabilities in AI Policy, 2023 [accessed 6 October 2024].
[23] Recital 57 of the AI Act

- Monitoring employee performance and behaviour.

Evidence of issues:

- Workplace surveillance technologies can disadvantage workers, as highlighted in the CDT report. [24]
- AI software used to evaluate candidates based on their behaviour in video interviews found to massively discriminate candidates with disabilities.[25]

Recommendations for EDF Members:

Collaborate with trade unions and digital rights organisations to collect evidence: From August 2026 when the provisions of AI that is high risk come into force you can monitor the EU database to find AI systems that are used in your member state and that can pose a risk to the rights of workers. It might then be possible to create alliances with other organisations protecting fundamental rights to collect testimonies of systems that do not work and provide these to supervisory authorities.

Build relations with regulators: Establish contact with labour market supervisory authorities, national human rights bodies, equality ombudsmen, data protection authorities, and market regulators so they can consult you if they have questions about people with disabilities.

7.5.4 High risk AI in essential services

AI systems used in essential services are considered high-risk due to their significant impact on individuals' rights and potential for discrimination.[26]

Essential services are the services required to live a fulfilling life in a modern, industrialised society. Examples include:

- Healthcare.
- Emergency response services (for example: ambulance, police).

[24] Lydia X. Z. Brown and others, Ableism And Disability Discrimination In New Surveillance Technologies (Centre for Democracy & Technology) [accessed 13 November 2022].
[25] Mara Mills and Meredith Whittaker, Disability, Bias, and AI, AI Now Institute Report, 2019, pages 15–17 search for 'HireVue'.
[26] Recital 58 of the AI Act

- Government benefits (for example: unemployment, pension, or disability benefits).
- Utilities (for example: electricity, gas).
- Access to financial services (for example: insurance, banking, loans).

These systems are high risk since using AI with flaws and biases could mean that persons are discriminated.

Example: Healthcare Chatbot in Sweden

Researchers from the Swedish Royal Institute of Technology evaluated a chatbot that was introduced as an additional way of contacting the health care, aside from the patient being able to talk with a nurse when calling the health care hotline in Sweden called 1177. The evaluation showed that the AI was not usable / accessible for people with different kinds of disabilities.[27]

This example shows the potential risks of introducing AI technologies to the market too early. Although the chatbot should not replace but complement a nurse's consultation, its early release with unresolved accessibility issues could put patients at risk. If patients rely entirely on the chatbot without realising its limitations, they may not receive timely and accurate medical care.

7.5.4.1 Examples of problematic surveillance in social protection

United Kingdom - facial recognition of protesters – cross referencing with list of people getting disability benefits

Another issue EDF members need to be aware of is when authorities use surveillance, with or without AI in their quest for determining if someone is eligible for a benefit.

AI can legally be used to prevent fraud in social protection systems under the AI Act, but it's crucial to ensure these measures do not go too far and respect privacy and dignity of persons with disabilities.

[27] Marika Jonsson and others, 'Tillgänglighet och användbarhet i 1177direkt', 2023 (Source only available in Swedish).

A worrying example comes from the UK. The State of Surveillance 2023 report by UK-based civil liberties organisation Big Brother Watch shows how welfare surveillance systems have criminalised disabled people, turning their daily activities into evidence for constant government evaluation.[28]

There are worrying reports that police in the UK have been passing information and surveillance videos about protesters with disabilities to the authorities who decide their entitlement to disability related benefits, putting them at risk of having their benefits cancelled.[29]

These types of practices can be used with or without AI and can have a chilling effect on the freedom of speech of persons with disabilities.

Another thing is that governments can use AI to detect irregularities or anomalies in social protection and benefits. That can mean looking at anything that might stand out as potential fraud. People with disabilities tend to deviate from the norm, and we are also intersectional in our identities, meaning someone can both have a disability and be an LGBTQI person. As a rule, people with disabilities stand out in statistics and are therefore scrutinised more frequently. And it is important that this is not done in a discriminatory way.

Denmark - Intrusive Monitoring and Loss of Privacy[30]

On 12 November 2024, Amnesty International published a report highlighting the risks of discrimination by the Danish Social Welfare Agency Udbetaling Danmark (UDK). The report points out that the use of artificial intelligence to identify individuals when investigating benefit fraud poses a risk of discrimination against people with disabilities, people on low incomes, migrants, refugees and racially marginalised groups.

---

[28] Rick Burgess, 'The Panopticon of the Welfare System', in State of Surveillance in 2023, ed. by Big Brother Watch (Greater Manchester Coalition of Disabled People, 2023), page 16 [accessed 6 October 2024].

[29] John Pring, 'Police Force Admits Passing Footage of Disabled Protesters to DWP', Disability News Service, 20 December 2018 [accessed 3 April 2023]; John Pring, 'Tory Conference Police Force Admits Sharing Information on Protesters with DWP', Disability News Service, 14 February 2019 [accessed 3 April 2023]; 'Shedding Light on the DWP Part 1 - We Read the UK Welfare Agency's 995-Page Guide on Conducting Surveillance and Here Are the Scariest Bits', Privacy International [accessed 3 April 2023]; 'Shedding Light on the DWP Part 2 - A Long Day's Journey Towards Transparency | Privacy International' [accessed 6 October 2024]; 'UN Committee on the Rights of Persons with Disabilities Calls on the UK to Act on AI Human Rights Risks', Privacy International [accessed 6 October 2024].

[30] 'Denmark: AI-Powered Welfare System Fuels Mass Surveillance and Risks Discriminating against Marginalized Groups – Report', Amnesty International, 12 November 2024 [accessed 21 September 2025].

According to Amnesty International, the authorities also process a large amount of personal data on a scale that Amnesty describes as mass surveillance. The report emphasises that there is a combination of the mass processing of personal data, which in many cases is of a sensitive nature, and the close and intimate scrutiny of people applying for or receiving benefits when they are interviewed by caseworkers and fraud investigators.

According to the press release, the Danish authorities use a system of up to 60 algorithmic models that are allegedly used to detect benefit fraud and flag individuals for further investigation by the Danish authorities. Amnesty International states that they have gained partial access to four of these algorithms as part of their research. The press release states that the people interviewed by Amnesty International reported that they are under considerable psychological pressure due to surveillance by fraud investigators and case workers. According to the chairman of the Social and Labour Market Policy Committee at the Dansk Handicap Foundation, people with disabilities who are repeatedly questioned by caseworkers may experience depression and stress. The organisation has reported that many individuals describe the ongoing scrutiny as having a significant negative impact on their well-being, with some saying it feels as though the constant surveillance is "eating away" at them.

The report sheds light on intrusive monitoring, such as assessing whether someone needs a personal assistant to assist in the home. The report refers to a focus group participant who described their experience of social workers carrying out these assessments as a form of surveillance. She found it humiliating to have a social worker in their home at all times, even during private activities such as showering, to assess exactly how much time was needed for this and then. The report states that this is excessive monitoring that appears to be unnecessary and adds no value in determining the appropriate level of personalised support but rather invades the privacy of the benefit recipient.

Amnesty's press release states that the Danish system could be categorised as a social scoring system, which would fall under the ban. The Danish authorities disagree.

France: Marginalised groups targeted by risk assessment tools

In France, fourteen human rights organizations, including APF France handicap and Amnesty International, have initiated legal proceedings against a risk scoring algorithm used by CNF (Caisse Nationale des Allocations Familiales), the national family benefits fund that manages social welfare programs, citing concerns regarding discriminatory criteria. The organizations argue that the algorithm broadly categorizes individuals experiencing marginalization, such as persons with disabilities, as subjects of suspicion. Additional groups identified as potentially vulnerable to discrimination include single parents, women, and individuals living in poverty.[31]

The organisations also reference findings from Lighthouse Reports, which examined portions of the algorithm obtained through Freedom of Information requests. According to their analysis, available data suggests that both having a disability and being employed may independently lead an individual to surpass the threshold for further investigation.[32]

Serbia – People with disabilities face poverty driven by unfair digitalisation[33]

Amnesty International's report "Trapped by Automation: Poverty and Discrimination in Serbia's Welfare State" documents the introduction of the Social Card registry, a centralised information system that uses automation to consolidate personal data of applicants and recipients of social assistance from a range of official government databases

The registry introduces semi-automated decision-making into the assessment of eligibility for social assistance and flags cases requiring review by a social worker.

The report finds that the Social Card registry has operationalised existing restrictive eligibility conditions and exacerbated exclusion, particularly harming Roma and people with disabilities. The system often relies on inaccurate source data, leading to people losing social assistance because the data collected was incorrect or misclassified.

[31] 'France: Discriminatory Algorithm Used by the Social Security Agency Must Be Stopped', Amnesty International, 16 October 2024 [accessed 21 September 2025].
[32] 'How We Investigated France's Mass Profiling Machine', Lighthouse Reports, [accessed 21 September 2025].
[33] 'Serbia: Trapped by Automation: Poverty and Discrimination in Serbia's Welfare State', Amnesty International, 4 December 2023 [accessed 21 September 2025].

Marginalised communities are disproportionately affected, as the system's heavy reliance on raw data on assets and income does not capture the complexity of people's lives.

The Social Card registry has reduced the autonomy of social workers. Many now defer to the system's outputs, even when they know the data is incorrect. The registry is designed to track changes that can lead to the loss of assistance, rather than to facilitate access to benefits. The report highlights that this system risks indirect discrimination, as it does not account for the barriers marginalised groups face in keeping their records up to date or navigating complex administrative processes.

Amnesty International concludes that the introduction of automation in Serbia's welfare system has compounded existing deficiencies, jeopardised people's right to social security, and disproportionately harmed already marginalised communities.

7.5.4.2 Other examples of High-Risk AI applications in essential services:

Public services: Determining eligibility for public assistance, healthcare, disability benefits, or social benefits.

Financial services:

- Loan eligibility assessments.
- Fraud detection.

Insurance: Setting premiums based on risk assessments.

Emergency services:

- Prioritising emergency calls.
- Dispatching ambulances and triaging patients.

Evidence of problems:

- AI systems can unfairly disadvantage individuals with disabilities, as seen in:

- Banks using irrelevant criteria like word capitalisation for creditworthiness, disadvantaging people with dyslexia (Binns and Kirkham, 2020). [34]
- Algorithms disproportionately flagging parents with disabilities.[35]

Recommendations for EDF Members

Advocate for and support the idea that third-party auditors should evaluate these types of AI and ensure that the audit frameworks are based on accessibility principles and guidelines.

7.5.5 High-Risk AI in law enforcement

AI systems used in law enforcement are high-risk because they can significantly impact individual freedoms and rights, potentially leading to wrongful actions. [36]

Examples of High-Risk AI Applications:

- **Predictive policing**: Predicting who will be potential crime victims[37] [38]
- **Lie detection**: Using AI as lie detectors[39] [40]
- **Evidence assessment**: Evaluating the credibility of evidence in investigations or trials
- **Recidivism prediction**: Judging the likelihood of re-offending based on personality and past behaviour[41]

---

[34] Reuben Binns and Reuben Kirkham, 'How Could Equality and Data Protection Law Shape AI Fairness for People with Disabilities?', arXiv:2107.05704 [Cs], 2021, page 14 [accessed 6 October 2024].
[35] 'Here's How an AI Tool May Flag Parents with Disabilities', AP NEWS, 2023 [accessed 15 April 2023].
[36] Recital 59 of the AI Act
[37] Matt Wood, 'AI Algorithm Predicts Future Crimes One Week in Advance With 90% Accuracy', SciTech Daily, 2022 [accessed 6 October 2024].
[38] Matt Wood, 'Algorithm Predicts Crime a Week in Advance, but Reveals Bias in Police Response', The University of Chicago, 2022 [accessed 6 October 2024].
[39] Naiara Bellio, 'Spanish Police Plan to Extend Use of Its Lie-Detector While Efficacy Is Unclear', AlgorithmWatch, 2020 [accessed 6 October 2024].
[40] PolyGR, 'Digital Polygraph Use in Police Departments: Enhancing Law Enforcement Interrogations Using AI', PolyGR, 2023 [accessed 6 October 2024].
[41] Keith Brannon, 'AI Sentencing Cut Jail Time for Low-Risk Offenders, but Study Finds Racial Bias Persisted', Tulane University News, 2023 [accessed 6 October 2024].

- **Profiling**: Profiling individuals during crime detection, investigation, or prosecution.[42]

Recommendations for EDF Members

Call for transparency: Advocate for national rules that require law enforcement authorities in your member state to be transparent about high-risk uses of AI systems. Meaning that the public should have access to information about that the AI system is in use and for what it is being used.

7.5.6 High risk AI-Biometric systems

Biometric systems are computer programs that use a person's physical or behavioural characteristics, such as face, fingerprint, voice, or iris, to identify or verify them. If you unlock your phone with a scan of your face or with a fingerprint you are using a biometric identification system every day.

Biometric AI systems are high-risk because they can invade privacy and may be inaccurate, especially against minorities like persons with disabilities and people of colour.[43]

One example of this is that a group called ETICAS tested an algorithm without informing the company that developed it. It turned out that the algorithm was poor at recognising people with Down's syndrome. It misjudged their age many times over.

Some people were estimated to be 16 years younger than. Others were estimated to be 23 years older than their actual age. This can lead to problems. For example, a child could be given things that are not suitable for their age. Or an adult might be denied access to services they need. This shows how wrong facial recognition can be for people with disabilities.[44]

Examples of High-Risk Biometric AI Applications:

Remote Biometric Identification: Identifying people from a distance with a video camera.

---

[42] Tzu-Wei Hung and Chun-Ping Yen, 'Predictive Policing and Algorithmic Fairness', *Synthese*, 201.6 (2023), page 206, doi:10.1007/s11229-023-04189-0.
[43] Recital 44 of the AI Act
[44] ETICAS Foundation, Invisible No More: The Impact of Facial Recognition on People with Disabilities, August 2023 [accessed 6 October 2024].

Biometric Categorisation: Grouping people based on traits like race or health status (for example, categorising someone as a "Female of Asian descent, approximately 25 years old")

Emotion Recognition: Analysing facial expressions, voice, and other cues to interpret emotions

The AI Act provide for usage restrictions. This means that:

- Emotion recognition systems are banned in workplaces and schools unless used for medical purposes.
- Police and migration authorities can use emotion recognition systems, but these are considered high-risk.

Recommendations for EDF Members

Advocate for banning real-time remote biometric identification: in collaboration with organisations protecting fundamental rights, advocate for a national ban on real-time remote biometric identification in public spaces for policing. Member states that want to allow totally or partially the use of this technology by law enforcement agencies must adopt national laws by 2 February 2025.

7.5.7 High-Risk AI in migration, asylum, and border control

AI systems used in migration, asylum, and border control are high-risk because they can jeopardise the fundamental rights of marginalised individuals. [45] The use of these AI systems is only categorised as high-risk if they are permitted under relevant EU or national law.

Examples of High-Risk AI Applications:

Lie detection: AI systems acting as lie detectors of people trying to cross the border.[46]

Risk assessment: Evaluating potential risks posed by individuals traveling to or staying in a member state

Application processing: Handling asylum, visa, or residence permit applications

Identification: Identifying persons within migration management

[45] Recital 60 of the AI Act
[46] Biometric Update, 'Travelers to EU May Be Subjected to AI Lie Detector', 17 June 2024 [accessed 6 October 2024].

Recommendations for EDF Members

Advocate for government policies that do not use AI-based lie detectors in migration contexts: EDF members should advocate for policies that prevent the use of lie detectors in migration, protecting people with disabilities and migrant backgrounds. Even if the AI Act does not allow member states to ban this through national legislation, governments can still adopt policies and guidelines to avoid using these unreliable AI systems, which can lead to grave human rights violations.

Given the serious concerns about AI-based emotion recognition, several key points underscore the need for caution specifically when it comes to people with disabilities:

1. Recital 44 of the AI Act refers to the questionable scientific basis of AI systems for recognising emotions, which can lead to discrimination. Such technologies are banned in schools and the workplace, but unfortunately, due to political compromises, this ban has not been extended to policing or migration, where the risk of serious human rights violations remains likely.

2. A comprehensive 2019 study disputes the assumption that facial movements consistently reflect emotional states, noting significant variations across cultures, situations, and individuals. This lack of scientific backing in emotion recognition technologies could result in serious errors and discrimination, especially in sensitive fields like migration and border control.[47]

3. The UN Special Rapporteur on the Rights of Persons with Disabilities warned in 2021 against the use of facial and emotion recognition, citing their high error rates in recognising persons with disabilities, which can lead to discrimination and human rights violations.[48]

[47] Lisa Feldman Barrett and others, 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements', *Psychological Science in the Public Interest*, 20.1 (2019), pages 1–68, doi:10.1177/1529100619832930.
[48] Gerard Quinn, A/HRC/49/52: Artificial Intelligence and the Rights of Persons with Disabilities - Report of the Special Rapporteur on the Rights of Persons with Disabilities, 28 December 2021, paras 34, 54, 65–66, 76(c) [accessed 7 October 2024].

4. Emotion recognition software has been shown to misinterpret grammatical signals in sign language (expressed by facial expressions) as negative emotions like aggression. These errors can have severe implications if public authorities rely on pseudoscientific technology for decision-making.[49]

7.5.8 High-Risk AI in administration of justice and democratic processes

AI systems in justice and democratic processes are high-risk due to their significant impact on democracy, freedoms, and legal rights[50].

Examples of High-Risk AI applications:

- **Judicial assistance:** Helping judges or judicial authorities with fact-finding, understanding laws, and applying them to cases.
- **Voting influence:** Influencing voting behaviour in elections or referendums.

Recommendations for EDF Members

- **Advocate for transparency**: Check whether your national laws on administrative procedures already contain a strong right of the individual citizen to a meaningful explanation of an authority's decisions. If not, consider advocating for such a right that applies regardless of whether the decision was made by a human or with the assistance of or entirely through automated decision-making. You can join forces with other organisations protecting fundamental rights to campaign for this.

[49] Irene Rogan Shaffer, 'Exploring the Performance of Facial Expression Recognition Technologies on Deaf Adults and Their Children', *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility*, 8 October 2018, pages 474–76, doi:10.1145/3234695.3240986.
[50] Recital 61 of the AI Act

8 Transparency risk[51]

Transparency requirements aim to ensure that people know when they are interacting with AI systems or encountering AI-generated or manipulated content. AI-generated content is created by AI, while AI-manipulated content is existing material changed by AI, for example when AI edits a video.

Article 50 of the AI Act sets out four main transparency obligations, depending on the system, its output and how it is used. These requirements support informed choices; they do not, by themselves, establish that an AI system is safe or lawful. Transparency obligations can also apply to high-risk AI systems.

These transparency requirements began applying on **2 August 2026**. A limited grace period gives providers of generative AI systems already placed on the market before that date **until 2 December 2026** to meet the machine-readable marking requirement in Article 50(2). This does not postpone the other transparency duties. See the European Commission's overview of the transparency rules.

Key requirements under Article 50 and related provisions:

- **Direct interaction with AI**: Providers must generally ensure that people are informed when they are interacting with an AI system, unless this is obvious in the circumstances. This covers tools such as chatbots and AI voice assistants.
- **AI-generated or manipulated content**: Providers of systems that generate synthetic text, images, audio or video must generally ensure that outputs are marked in a machine-readable format, for example through digital watermarks, so that they can be detected as artificially generated or manipulated. This technical marking is different from a message that a person can directly perceive. Exceptions include certain standard editing functions and changes that do not substantially alter the input or its meaning.

[51] European Commission, 'Guidelines on Transparency Obligations for Providers and Deployers of AI Systems', 20 July 2026 [accessed 3 November 2026].

- **Machine-readable marks can include digital watermarks**: signals embedded in content that software can detect, even when people cannot see or hear them. For example, Google's SynthID watermarks AI-generated text, images, audio and video, including content from Gemini. OpenAI's verification tool for ChatGPT-generated images and audio checks for SynthID watermarks and Content Credentials, which attach information about a file's origin. These are concrete examples of technical marking, not proof that every output is marked or that a provider meets all AI Act requirements.

- **Emotion recognition and biometric categorisation**: Organisations using these systems must generally inform people exposed to them that the system is operating. This information requirement does not make an otherwise prohibited use permissible.

- **Deep fakes and public-interest text**: Organisations using AI to generate or manipulate deep fakes must generally disclose their artificial origin. Disclosure also applies to AI-generated or manipulated text published to inform the public on matters of public interest, unless it has undergone human review or editorial control and a person or organisation holds editorial responsibility for its publication. Specific exceptions and qualifications apply, including for artistic and fictional works.

More than one obligation can apply to the same system. A provider may need both to disclose direct interaction with AI and to mark the content it generates. These transparency duties do not replace other applicable safeguards.

When do these obligations apply to personal use?

The AI Act makes an important distinction between personal, non-professional use and professional use. If a person uses an AI system only for their own personal and non-professional purposes, they are not subject to the AI Act's obligations for deployers, meaning organisations or people using AI systems under their authority. For example, the Commission's guidelines explain that a student using AI to write homework can fall within this personal-use exception. However, using AI as part of a job, business, freelance activity or another professional activity does not.[52]

[52] European Commission, 'Guidelines on Transparency Obligations for Providers and Deployers of AI Systems', pages 7–8.

Importantly, this exception applies to the person using the AI, not to the AI system or its provider. The company providing the system may still have transparency obligations. The Commission gives the example of someone using AI to create a deep fake for a personal Christmas card. The person creating the card for private use does not have to disclose the deep fake under the deployer obligation, but the provider of the AI system must still ensure that the generated content carries the required machine-readable marking. The exception does not remove obligations under other applicable laws or a student's responsibility to follow their school's rules.

A word of caution about AI indicators

A watermark or an AI-detection result can indicate that AI was involved, but it does not necessarily mean that an entire text, image or other work was created by AI, or that someone has broken a rule. Different tools also provide different kinds of information. A watermark shows that a particular technical signal was found, while an AI-detection tool estimates whether content appears to have been generated or changed by AI. AI may also have played only a supporting role. For example, a student may have written their own work but used a grammar or writing-feedback tool that uses generative AI to suggest improvements. These indicators should therefore be treated as supporting information rather than proof on their own. This is especially important when the result could affect a person, for example when a school investigates whether a student has improperly used AI.

Turnitin itself warns that its AI-writing detection can make mistakes and should not be used as the sole basis for action against a student. Decisions should consider the wider evidence, including what kinds of AI assistance were permitted, and give the person an opportunity to explain how they created their work and what tools they used.

Why does this matter?

When real and fake information blend, trust in the Internet declines. Reports from October 2025 show that AI-generated content often targets vulnerable groups, such as by creating fake social media accounts pretending to be disability advocates or using deepfakes to exploit people with Down syndrome.

These abuses undermine safety and make it difficult for genuine voices to stand out. Transparency is crucial so everyone, especially those with disabilities, can identify accurate information online.[53]

Accessibility and disability rights perspective

Article 50 requires transparency information to be provided in a clear and distinguishable manner, at the latest when a person first interacts with or is exposed to the AI system or relevant content. The information must also comply with applicable accessibility requirements. A transparency measure cannot effectively inform someone if they cannot perceive, access or understand it.

Article 50 does not establish a separate set of technical accessibility standards: providers and organisations using AI must identify and comply with the accessibility requirements applicable to their product, service or content, including under the Web Accessibility Directive and European Accessibility Act.

Recommendation to EDF members

When monitoring implementation, disability organisations should pay attention not only to whether information about AI is provided, but also to whether persons with different disabilities can access and understand it.

9 Minimal risk

Minimal risk AI systems are those that do not fall into the prohibited, high-risk, or transparency risk categories. They are considered to have little or no impact on individuals' rights or safety, so the AI Act does not impose additional rules on them - only existing laws such as the GDPR continue to apply.

The AI Act contains a general requirement on **AI literacy**.[54] This means helping staff develop the knowledge and skills they need to understand how an AI system works, use it responsibly and recognise its risks. Although this requirement is explained here under minimal-risk AI, it applies to providers and deployers of AI systems at **all risk levels**.

[53] 'Why People Are Using AI to Fake Disabilities like Down Syndrome Online - CBS News', 6 May 2025 [accessed 16 October 2025]; BBC Audio, Deepfaking Disability, The Documentary Podcast (1 October 2025) [accessed 16 October 2025].
[54] Article 4, AI Act

The AI Omnibus lowers the level of ambition: providers and deployers no longer have to ensure that each staff member reaches an appropriate level of AI literacy. Instead, they must support its development, for example by providing and encouraging suitable training opportunities. Recital 8 of the AI Omnibus explains that this change is intended to reduce the compliance burden on organisations.

Examples:

1. Spam filters in email
2. Bots in video games that play against users
3. Recommender systems suggesting films (Netflix), videos (YouTube), or songs (Spotify)

These systems are intentionally left unregulated by the AI Act to avoid unnecessary burdens for every day, low-impact AI.

10 General Purpose AI (GPAI)

General Purpose AI (GPAI) refers to advanced AI models designed to perform a wide range of tasks, rather than being restricted to a single, specific function. GPAI can be thought of as the underlying technology or "engine" that can be incorporated into various applications and services.

For example, an airline might use a GPAI model to power its customer service chatbot. Instead of developing an AI from scratch and training it to understand and generate language, the airline can use an existing GPAI model that already possesses these capabilities. The airline then provides the AI with information about flight schedules, ticket prices, and company policies. The GPAI-powered chatbot can answer customer questions, assist with bookings, and provide support, drawing on both its general language abilities and the specific information supplied by the airline.

This flexibility is why it is called "general purpose": the same GPAI model can be used in many different contexts, such as chatbots and content creation tools. The obligations and risks associated with GPAI depend on how it is used and the impact it may have in each situation. For example, if it is integrated into a chatbot used to interview job applicants as part of a recruitment process, that implementation of the GPAI system then becomes part of a high-risk system.

Under the AI Act, GPAI is not a separate risk category; instead, these systems can fall under any risk level (prohibited, high-risk, transparency, or minimal risk) depending on their use and potential impact. GPAI is subject to its own set of rules and obligations, particularly when it poses systemic risks due to its scale or influence. Enforcement for GPAI is handled by the European Commission, while other AI systems are generally overseen by national authorities.

10.1 Protections from threats to human health, safety and democracy

Some general-purpose artificial intelligence (GPAI) systems pose 'systemic risks' because they can cause significant harm to public health, safety, human rights or society.

The European Commission will draw up **guidelines** to categorise such AI models based on their level of risk. The AI Act provides some guidance on the criteria and requirements GPAI AI systems.

A simple rule of thumb is that if your organisation uses an AI system that is only used internally and not shared with others, it is not a large-scale model. However, if Google or OpenAI publish a GPAI system that is publicly available or used by many others, it is likely to a large-scale AI system.

AI language models, which under the EU AI Act are classified as General-purpose AI systems are known to invent facts and can also produce harmful content.[55] If a GPAI system has many users or is integrated into other computer systems, there is a risk that the harmful output can multiply and affect other computer systems that are dependent on the GPAI system.

The AI Act places an obligation on providers of AI models the large-scale models to ensure that they have robust moderation and control mechanisms in place to prevent harmful outputs from being passed on to the user. Recital 110 of the AI Act gives examples of systemic risks, such generation and spreading of misinformation, discriminatory or hateful content, to create hacking tools, instructions on how to build a bomb and similar.

[55] 'When AI Gets It Wrong: Addressing AI Hallucinations and Bias', Sloan School of Management, Massachusetts Institute of Technology, 2023 [accessed 6 October 2024].

Here are some real-life examples that likely would fall under systemic risks:

- A chatbot that suggested to a Belgian man that he should take his life to save planet, it ended in tragedy.[56]
- A chatbot encouraged a man to murder a head of state.[57]
- A chatbot was used to create a computer virus.[58]
- Voice generating AIs that are used to impersonate someone.[59]
- Chatbots that may reinforce delusions in persons who are at higher risk of developing psychosis.[60]
- AI chatbot encouraging a teenager with high-functioning autism to harm himself and act violently after the parents wanted to restrict his screen time.[61]

Providers of large-scale GPAI AI models have a duty to implement safeguards to mitigate systemic risks, which includes addressing biases against people with disabilities. Language models often exhibit bias as they are trained on internet data where ableist language unfortunately still dominates.[62]

They must comply with additional rules in **Articles 51, 52** and **55**. **Recital 110** of the AI Act clarifies that addressing bias is an integral part of the duty to mitigate systemic risk.[63]

---

[56] Imane El Atillah, 'Man Ends His Life after an AI Chatbot "encouraged" Him to Sacrifice Himself to Stop Climate Change', 31 March 2023 [accessed 6 October 2024].
[57] Euronews, 'Man "encouraged" by AI Chatbot "Girlfriend" to Kill Queen Elizabeth II Receives Jail Sentence', 6 October 2023 [accessed 6 October 2024].
[58] EFE, 'Japanese Man Arrested for Creating Computer Virus Using Generative AI', 28 May 2024 [accessed 6 October 2024].
[59] CNBC, 'Scammers Can Use AI Tools to Clone the Voices of You and Your Family—How to Protect Yourself', CNBC, 2024 [accessed 6 October 2024].
[60] Madeleine Finlay, Ross Burns, and Presented by Madeleine Finlay; produced by Tom Woolfenden; sound design by Ross Burns; executive producer Kate Lamble, '"AI Psychosis": Could Chatbots Fuel Delusional Thinking? – Podcast', Science, The Guardian, 28 August 2025 [accessed 29 August 2025].
[61] https://edition.cnn.com/2024/12/10/tech/character-ai-second-youth-safety-lawsuit/index.html and https://news.bloomberglaw.com/litigation/autistic-teens-family-says-ai-bots-promoted-self-harm-murder
[62] Vinitha Gadiraju and others, '"I Wouldn't Say Offensive but...": Disability-Centered Perspectives on Large Language Models', 2023 ACM Conference on Fairness, Accountability, and Transparency, 12 June 2023, pages 205–216, doi:10.1145/3593013.3593989.
[63] Recital 110 of the AI Act

10.2 Guidelines on the scope of the obligations for general-purpose AI models[64]

The European Commission has issued Guidelines on the scope of the obligations for general-purpose AI (GPAI) models. These are technical, non-binding guidelines published on 18 July 2025.

They exist to help actors understand when a model counts as a GPAI model and therefore falls within the GPAI rules of the AI Act, and how to tell when a GPAI model is considered to pose a systemic risk. This note is for awareness only. Disability advocates are not expected to read or master the document.

What the guideline clarifies, at a glance:

- When a model is a GPAI model: it explains the Commission's approach to identifying GPAI models and sets out how to assess scope conceptually, so providers and stakeholders can recognise when the rules on GPAI apply.
- When a GPAI model has systemic risk: it details the classification of GPAI models with systemic risk.

10.3 GPAI code of practice[65]

On 10 July 2025, the European Commission published a voluntary code of practice for AI models for general purposes. The Code is intended as a practical way for model providers to demonstrate compliance with the AI Act, rather than as a new obligation.66 Providers that sign up to the code can rely on it to show that they are following the AI Act and reduce their administrative burden.

The Code is not mandatory. It does not contain any additional obligations that go beyond the AI Act. It provides a simplified way for GPAI providers to fulfil their existing obligations. Further details can be found in the Commission's Questions and Answers on the Code of Practice.

What the Code covers (three chapters):

[64] Guidelines on the Scope of Obligations for Providers of General-Purpose AI Models under the AI Act [accessed 22 September 2025].
[65] The General-Purpose AI Code of Practice [accessed 28 July 2025].
[66] Article 53(4), 55(2) and recital 117 of the AI Act

- **Transparency:** documentation and disclosures for model providers.
- **Copyright:** practical steps to put in place a policy that complies with EU copyright law.
- **Safety and Security:** state of heart practices for providers of GPAI models with systemic risk only.

These documents are very technical. We refer to them here for awareness, not for detailed study. You are not expected to read or master them in order to advocate for disability inclusive AI in national implementation.

10.4 Voluntary codes of conduct

The AI Act promotes the development of codes of conduct for AI applications that are categorised as limited or minimal risk. **Article 95** requires the European Commission's AI Office and member state governments to support and promote the development of these codes.

These codes of conduct can be developed by AI providers, organisations using AI or industry associations representing these groups. Other stakeholders such as organisations protecting fundamental rights, trade unions, consumer groups and academic institutions can also be invited to participate in the development of these codes.

According to **Article 95(2)**, these codes should have clear objectives and be able to measure success. A particular objective is the protection of marginalised groups, including people with disabilities. This shows how important it is to consider the needs and rights of marginalised groups in the development and use of AI technologies.

10.5 Recommendations for EDF members

General purpose AI systems will be largely regulated by EU policies, leaving limited space for EDF members to advocate at the national level. One important question is however codes of conduct.

Because **Article 95(2)(e)** of the AI Act explicitly identifies the protection of marginalised groups and the accessibility of AI as objectives for these codes of conduct, disability rights organisations have an opportunity to play an active role in their development.

If your organisation would like to participate in the development of these codes of conduct, you should contact the consumer organisations in your country.

As the AI Act functions as a product safety law, consumer rights organisations have valuable experience that can be of use to disability rights organisations involved in the development of codes of conduct in their member country.

You can contact the European Disability Forum secretariat if you want to contribute to the development of the EU code of conducts.

Contact the responsible ministry at national level that will draft the national code of conduct showing your interest, and the consumers and digital rights' organisations in your country.

11 Fundamental rights, sandboxes and testing

11.1 The right to complain

Under **Article 85** of the AI Act, both individuals and organisations (such as companies or non-profits) have the right to file complaints if they believe that an AI system has violated the Act. This allows people to report suspected issues to the relevant regulatory authority, known as the **market surveillance authority**. However, it's important to note that the authority will decide whether the complaint requires further investigation.

This is not a **human rights provision** but a formal channel for addressing concerns about AI systems, especially those classified as high-risk. For example, if a person with a disability believes an AI system is discriminating against them, they can raise their concerns through this complaint process. The aim is to provide a mechanism for anyone affected by harmful AI practices to take action.

Recommendation to EDF members

Together with the right of individuals to obtain an explanation for the output from a high-risk AI system, the right to lodge a complaint may be a possible avenue for EDF members and other human rights organisations to take action against harmful AI-systems.

11.2 Reporting of serious incidents

Providers are required to report serious incidents involving high-risk AI systems and GPAI to the market surveillance authority. Reporting requirements vary according to the assigned risk class.

High risk AI systems

High-risk AI systems must be reported when they cause or risk causing serious harm. The main purposes of this reporting are to warn authorities about dangerous patterns, ensure providers and deployers take responsibility, enable authorities to act quickly, and build public trust through transparency.

Reporting covers two main areas: serious incidents and widespread infringements. A serious incident is an event that results in death, serious harm to health, major disruption of critical infrastructure, serious damage to property or the environment, or large-scale violations of fundamental rights. Examples include an AI system providing a doctor with incorrect medical information, leading to a patient receiving the wrong diagnosis or treatment, unfairly denying someone a loan, or excluding qualified job candidates based on gender or ethnicity.

A widespread infringement occurs when an AI system causes serious harm to groups of people in several EU countries simultaneously. For example, if the same issue with an AI system affects people in two or more countries, or if the same illegal practice takes place in at least three countries, it is considered widespread. For reporting purposes, it must also be a serious incident, meaning it causes or could cause actual harm, such as to people's health, safety, rights, or the environment. If it is only widespread but not serious, it does not need to be reported.

Providers of GPAI systems[67]

If a provider offers a general-purpose AI model that could have a significant impact on society (referred to as "systemic risk"), they must keep records and report any serious problems or incidents involving their model. This report should be submitted promptly to the EU's AI Office and, if necessary, to national authorities.

[67] Article 55(1), and recitals 114 and 115 of the AI Act as well as The General-Purpose AI Code of Practice, on Safety and Security, Commitment 9.

11.3 Regulatory sandboxes

A **regulatory sandbox** is a supervised framework in which developers can develop, train, test and validate an innovative AI system for a limited period, following a plan agreed with the public authority running the sandbox. Testing may include real-world conditions where appropriate. Participation does not mean that the system has been approved, certified as safe or confirmed as complying with every legal requirement.

The authority provides guidance and supervision to help developers understand the rules, identify risks and test measures to address them. Authorities also learn about the technology and can intervene where necessary. A sandbox therefore supports compliance while a system is being developed, but it does not guarantee that no problems will arise.

The public authority responsible for running a national sandbox is specifically designated for that role. Depending on the country's arrangements, it may be a data protection authority or another public authority. Developers receive guidance from the authority running the sandbox, with other relevant authorities involved where needed.

Under Article 57(1) of the AI Act, each EU country must ensure that at least one national AI regulatory sandbox is operational by 2 August 2027. A country may establish a sandbox jointly with other EU countries or participate in an existing sandbox if this provides equivalent national coverage. Additional regional, local or joint sandboxes may also be established under Article 57(2). This deadline does not show whether a particular sandbox is already open to participants.

There are also arrangements at EU level. Article 57(3a) allows the AI Office to establish an EU-level sandbox for AI systems under its supervision in accordance with Article 75(1), in close cooperation with relevant authorities. This does not replace countries' powers to establish and supervise national sandboxes. Separately, Article 57(3) allows the European Data Protection Supervisor to establish a sandbox for EU institutions, bodies, offices and agencies. These provisions allow such arrangements to be established, but do not by themselves show that a sandbox is operational or accepting applications.

The authority in a country that establishes sandboxes is encouraged to seek to involve other actors in the AI ecosystem such as organisations protecting fundamental rights when it is appropriate[68].

Recommendation to EDF members

Here EDF members can recommend their governments and market surveillance authority to consider the impact of AI systems on persons with disabilities within the sandboxes.

11.4 Fundamental rights impact assessments (FRIAs)

To ensure that **high-risk AI systems** do not violate fundamental rights, Article 27 of the AI Act requires certain deployers to conduct a **Fundamental Rights Impact Assessment (FRIA)** before using such systems. This includes public authorities and certain private organisations providing public services, as well as deployers of specified high-risk AI systems in areas such as essential services. AI systems used in critical infrastructure systems that manage road traffic, water, gas and electricity are exempted.AI systems used in critical infrastructure systems that manage road traffic, water, gas and electricity are exempted.

A FRIA is a check to determine whether an AI system could harm people's fundamental rights. The deployer must assess the groups likely to be affected and the specific risks to them. Where appropriate, the deployer may involve relevant stakeholders, including organisations representing persons with disabilities. For example, if a government wants to use a high-risk AI system, seeking feedback from organisations of persons with disabilities can help it identify accessibility barriers and discriminatory effects.

Organisations protecting fundamental rights at EU level have developed or are developing their own FRIA templates based on human rights standards. These are separate from the European Commission's official template, which had not yet been published when version 3 of this toolkit was updated. EDF members can recommend suitable civil-society templates to their governments while continuing to advocate for a strong official template.

[68] Recital 139 of the AI Act

In September 2025, the Spanish Federation of Consumers and Users published a research report analysing the current landscape of Fundamental Rights Impact Assessments (FRIAs) under the AI Act, as well as other closely related frameworks such as the GDPR, which requires data protection impact assessments. The report analyses both European and Spanish examples with the aim of highlighting and proposing best practises that enable a meaningful assessment of the impact of AI systems on fundamental rights. Through this comparative approach, the report provides concrete recommendations to ensure that FRIAs and similar processes truly protect the rights of individuals and are not reduced to mere formalities.[69]

Recommendation to EDF members:

- **Advocate for strong FRIAs:** At the time of updating version 3 of this toolkit, the European Commission had not yet published its official template for fundamental rights impact assessments (FRIAs). Its website listed the guidelines and accompanying template as work still in progress, in an update dated 31 July 2026.

  In the meantime, organisations protecting fundamental rights should continue to advocate for a strong and meaningful FRIA process. National EDF members can identify supportive governments and human rights institutions, encourage them to support robust standards developed by civil society, and contribute when the Commission consults on its official FRIA template. This advocacy can help ensure that FRIAs provide real protection for fundamental rights rather than becoming a formal compliance exercise.[70]

  National disability organisations can engage in a coordinated way with national authorities and private organisations that are required to conduct FRIAs, including relevant banks and insurance companies. They can recommend civil-society FRIA templates and call for meaningful structures through which persons with disabilities and their representative organisations can contribute to assessments.[71]

---

[69] Report: Towards a meaningful implementation of Article 27 under the AI Act – English version - CECU

[70] Karolina Iwańska and others, Towards an AI Act That Serves People and Society: Enforcement Strategies for Rights-Respecting AI Regulation (European Center for Not-for-Profit Law (ECNL), 2024), page 31[accessed 6 October 2024].

[71] Iwańska and others, Towards an AI Act That Serves People and Society: Enforcement Strategies for Rights-Respecting AI Regulation.

11.5 Testing in real world conditions[72]

Real-world testing can take place inside or outside an AI regulatory sandbox. Testing inside a sandbox forms part of the supervised framework described in the regulatory sandboxes section above. Testing outside a sandbox follows a separate legal route: Article 60 sets conditions for such testing. The authorisation process described below concerns testing outside sandboxes, not admission to a sandbox.

High-risk AI systems can be tested in the real world to understand their performance outside of controlled environments. These tests must follow a detailed plan and be authorised by the competent national authority. If the authority doesn't respond within 30 days, the tests are however considered authorised, unless the law of the member state requires explicit authorisation.

To protect all participants, especially marginalized groups such as people with disabilities, several important rules must be observed. Participants must give informed consent, i.e. they must fully understand the test and agree to participate. If they decide to withdraw their participation, they can do so at any time without negative consequences, and their personal data must be deleted. Special measures must be taken to ensure the safety and rights of people with disabilities during the tests.[73]

Authorities are authorised to inspect and monitor the tests to ensure that all safety and ethical standards are met. Providers are responsible for any harm that occurs during testing and must act immediately if serious problems arise.

Recommendation to EDF members

Keep in mind that testing in real-world is something that exists. The rules on such testing are primarily governed at the EU level, with additional guidance expected from the EU Commission. Given that persons with disabilities are specifically mentioned as a group that needs special protection, organisations of persons with disabilities can establish contact points with market surveillance authorities. This way, they can seek your expertise when needed. Ensure that you are compensated for your time and effort.

[72] Article 60 of the AI Act
[73] Article 60(4)(g) of the AI Act

12 Additional measures: “Encouragements”

Recital 142 of the AI Act encourages member states to support and promote research and development in the field of artificial intelligence that has a positive impact on society and the environment. It particularly emphasises projects that improve accessibility for people with disabilities as an important outcome. Initiatives with these objectives should be eligible for public and financial support from the Union.

Recommendation to EDF members

EDF members can encourage their governments to make such funding available, with a focus on co-creation with persons with disabilities, bias and use of AI as assistive technology. They could also emphasize that while AI can hold many promises for the inclusion of persons with disabilities, many AI initiatives fail.

13 Governance structure

The EU AI Act has a governance structure with actors at EU and national level. The most important actors are:

- The AI Office: a unit in the Commission that coordinates and supports the AI Board and national authorities. It also issues guidelines and delegated acts on the regulation.[74]
- Artificial Intelligence Board: A body of national market surveillance authorities and the Commission. It advises and supports the Commission on the Regulation, for example, identifying new high-risk AI systems, harmonising market surveillance, exchanging information and best practises and promoting international cooperation.[75]

[74] Article 64 of the AI Act
[75] Article 65-66 of the AI Act

- Advisory Forum: Established in 2026 under Article 67 of the AI Act, the Advisory Forum advises the European Commission and the AI Board on implementing and enforcing the Act. Its 174 selected members come from civil society, academia and industry, including small businesses and start-ups. Members contribute expertise on issues such as standards and practical implementation challenges through meetings, thematic subgroups, opinions and recommendations. They serve two-year terms, renewable once. Permanent members include the Fundamental Rights Agency, the EU Agency for Cybersecurity and the European standardisation organisations. EDF and two EDF member organisations are represented in the Advisory Forum: the Spanish Committee of Representatives of Persons with Disabilities (CERMI) and the European Council of Autistic People (EUCAP).

  EDF members and other organisations of persons with disabilities can share relevant research, examples of barriers and concerns about AI with the EDF secretariat to inform its contributions.

- Scientific Panel: Established under Article 68 of the AI Act, the Scientific Panel brings together 60 independent experts appointed in their personal capacity rather than as representatives of organisations. It advises the AI Office and national authorities on implementing the AI Act and assessing the impacts and risks of general-purpose AI models. Its responsibilities include alerting the AI Office to systemic risks, advising on the classification and evaluation of general-purpose AI models, developing evaluation methods and supporting market surveillance. Members serve renewable two-year terms.

- European Data Protection Supervisor: The data protection authority of the EU, also serves as the market surveillance authority regarding the use of AI by EU institutions. The Supervisor provides guidance to EU lawmakers on proposed new EU legislation.[76]

- Market surveillance authority: The national authority or authorities that monitor and enforce the regulation. It is authorised to carry out inspections, request information, carry out tests, impose corrective measures and impose sanctions.[77]

[76] Article 70(9) of the AI Act
[77] Article 70 of the AI Act

- Authority for the protection of fundamental rights: The national authority or authorities responsible for the protection of fundamental rights and non-discrimination, for example, the Equal Opportunities Officer(s). It cooperates with the market surveillance authority and can access documents from providers of high-risk AI systems. It does not have the power to take corrective action.[78] This will be a key player for EDF members to build good relations to.

13.1 Market surveillance authorities

Market surveillance authorities are the official bodies in each EU country responsible for enforcing the AI Act. Their main task is to monitor AI systems for risks and ensure that providers comply with the law. These authorities have wide-ranging powers: they can intervene if AI systems pose risks or do not fulfil the requirements of the AI Act, they can carry out remote monitoring and access providers' documentation, data sets and even source code. If necessary, they can propose joint investigations with the European Commission, demand corrective measures and enforce the rules through sanctions.

Market surveillance authorities must report to the Commission and national competent authorities every year, communicating the results of risk assessments and the measures they have taken. They are expected to act independently, impartially and without bias in all their activities.

Complaints from individuals are an essential part of effective enforcement. Anyone who believes that an AI system has breached the AI Act can lodge a complaint with the Market Surveillance Authority. These complaints help the authorities to quickly identify and resolve problems.

Effective enforcement also depends on co-operation between market surveillance authorities in the EU. These authorities work together through the European AI Board, which helps to coordinate expertise and enforcement action.

[78] Article 77 of the AI Act

Each Member State had to appoint one or more market surveillance authorities by 2 August 2025. If a country has several authorities, it must designate a national single point of contact for cooperation with other Member States, the EU and the general public.[79] If a Member State fails to designate an authority within the deadline, the Commission may initiate formal infringement proceedings.

A list of the single points of contact of each member state is available on the EU Commissions website: Market Surveillance Authorities under the AI Act.

For many market surveillance authorities, policing AI algorithms will be a completely new and challenging task. Even data protection authorities, accustomed to protecting privacy as a human right under the General Data Protection Regulation, are facing a major transition and will need resources and staff with expertise in sociology, law, cybersecurity, technology, non-discrimination, data protection and fundamental rights. Given that high-risk AI must meet mandatory accessibility standards, it is likely that most public authorities will initially lack expertise in accessibility.

Organisations of persons with disabilities have a crucial role to play in ensuring that governments recognise this gap and include accessibility experts in market surveillance authorities' teams. Our lived experience and extensive expertise are essential to making AI systems truly inclusive and effective for all, especially persons with disabilities. For this reason, our expertise as organisations of persons with disabilities will also be invaluable to the market surveillance authorities themselves. EDF members are strongly encouraged to **reach out to these authorities and proactively offer their expertise and advice**.

13.1.1 Directing complaints: choosing the right authority

Depending on the type of AI system in question, different supervisory authorities are responsible for monitoring:

- If it is a **prohibited AI-system, a high-risk AI-system, or a transparent risk**, then the designated supervisory authority in each Member State - the market surveillance authority - is responsible for complaint handling and enforcement.

[79] Article 70.2 and recital 153 of the AI Act

- In contrast, for **general purpose AI systems**, the European Commission acts as the supervisory authority and is the responsible competent body for receiving complaints or concerns.

So, if you suspect a problem with an AI system, it's important to direct the complaint to the right authority: the national market surveillance authority for high-risk or prohibited AI and the European Commission for general-purpose AI systems. This will ensure that the matter is dealt with efficiently by those with the appropriate powers and expertise.

In addition to the national authorities, the EU has its own market surveillance authority for **AI systems used by EU institutions**. In particular, the **European Data Protection Supervisor** (EDPS) acts as a market surveillance authority responsible for monitoring the use of AI in EU institutions.

Table 1: Categories of AI systems under the AI Act

Category	Description and Examples	Enforcement Authority
Prohibited (Unacceptable risk)	Banned AI practices (for example: manipulative, exploitative, social scoring)	Member state authorities
High-risk	Strictly regulated (for example: employment, education, law enforcement, essential services)	Member state authorities
Transparency/ Limited risk	Transparency obligations (for example: chatbots, deepfakes, biometric categorisation)	Member state authorities
Minimal risk	No additional obligations (for example: spam filters, video game AI), except requirement for AI literacy	Member state authorities
General Purpose AI (GPAI)	May fall under any risk category; subject to specific GPAI rules and systemic risk rules.	European Commission

13.2 Authorities protecting fundamental rights

Under Article 77 of the AI Act, each Member State must identify public authorities or bodies responsible for supervising or enforcing EU law protecting fundamental rights, including equality and non-discrimination law. These may include equality bodies, ombuds institutions, national human rights institutions and data protection authorities.

The AI Omnibus changed how these authorities obtain information. Under the original AI Act, they could request relevant documentation directly from providers and deployers of high-risk AI systems. Under the revised Article 77, requests for information or documentation created or maintained under the AI Act must instead be made to the relevant market surveillance authority. The market surveillance authority must provide access without undue delay and may request the information from the provider or deployer when necessary. The information must be provided electronically in an accessible and machine-readable format.

The revised Article 77 also requires authorities protecting fundamental rights and market surveillance authorities to cooperate closely, exchange information and provide each other with the assistance needed to fulfil their respective mandates. Their different responsibilities, powers and independence must be respected.

Recital 36 of the AI Omnibus explains the legislator's reasoning for this change. According to the recital, routing requests through the competent market surveillance authority is intended to clarify responsibilities, reinforce cooperation and streamline procedures. It also clarifies that Article 77 does not limit any powers that fundamental rights authorities already have under other EU or national laws. If another law allows an authority to request information directly from a Provider or developer, it may continue to do so.

The market surveillance authority remains responsible for checking whether an AI system complies with the AI Act. If the available information is insufficient to determine whether fundamental rights law has been breached, the authority protecting fundamental rights may make a reasoned request for the market surveillance authority to arrange technical testing of the high-risk AI system. The authority protecting fundamental rights must be closely involved in that testing.

This change has been criticised[80] because it removes the direct route provided by the original AI Act through which Article 77 authorities could obtain documentation from providers and deployers. Requiring them to work through market surveillance authorities may delay investigations and create greater distance between fundamental rights expertise and AI Act enforcement. The criticism and its implications are discussed in more detail in **section 15.3.2 "Less direct access to information for fundamental rights authorities" (page 85).**

Member States had to identify their authorities protecting fundamental rights by **2 November 2024** and must keep the list updated.
The European Commission maintains a consolidated list of fundamental rights protection authorities with special powers under the AI Act.

13.3 Penalties for breaking the AI Act's obligations[81]

National authorities must lay down rules for sanctions when organisations violate the AI Act. These rules must be implemented by 2 August 2025.

- If an organisation breaches the rules on prohibited AI practises (Article 5), the authority can impose a fine of up to €35 million or 7% of global turnover (whichever is higher).
- If a company violates other rules, for example, for high-risk or general-purpose AI, the authority can impose a fine of up to €15 million or 3% of global turnover (whichever is higher).
- If a company provides misleading, incomplete or false information to the authority, the fine can be up to €7.5 million or 1% of global turnover (whichever is higher).
- Each country decides for itself whether to impose fines on its own authorities if they violate the AI Act.
- The EU can impose fines of up to €1.5 million on its own institutions for breaches of the rules on prohibited artificial intelligence, or up to €750,000 for other offences.

When determining the amount, the authority considers:

[80] European Network of National Equality Bodies (Equinet) and European Network of National Human Rights Institutions (ENNHRI), Joint Equinet–ENNHRI Statement on the Digital Omnibus.
[81] Article 99-101 and recitals 168-169 of the AI Act

- How serious the offence is and its consequences.
- The size and turnover of the company.
- Whether the company is a start-up or a small business.
- Whether the offence was committed intentionally or accidentally.
- How well the company has co-operated with the authority.

The penalties must be fair and effective and must not be too harsh for small businesses.

Recommendation to EDF members

EDF members, need to contact these authorities. There may also be initiatives going on in your country to create coordinated mechanisms for dialog and cooperation between organisations protecting fundamental rights and these types of authorities. They are the ones who can act if we face discrimination by an AI system. They can ask the deployer or provider of an AI system to explain how the AI works and whether it follows the AI Act. We have the lived experience of living with a disability and can give them useful input and feedback on how AI affects our rights and needs. We should cooperate with these authorities and report any problems with AI systems to them.

14 Monitoring the AI Act in your country

14.1 Importance of involvement for persons with disabilities

The EU AI Act is coming to you, and its implementation is a crucial moment for persons with disabilities in your country. This is the right time for EDF members to get involved in their governments' preparations to implement the AI Act.

Here's why:

- **Monitor bias and discrimination across AI systems:** The rules on detecting and correcting bias are no longer limited to providers of high-risk AI systems. Article 4a can also apply to deployers of high-risk AI systems and, under certain conditions, to providers and deployers of AI systems at other risk levels that may create risks to health, safety, fundamental rights or the environment.

Disability organisations can collect testimonies from members about unfair or discriminatory experiences with AI and identify recurring patterns. They can raise these concerns with the organisation using the system and work with digital rights, equality or data protection organisations to decide whether further action is needed. Where appropriate, they can ask the relevant authority to examine whether the provider or deployer followed Article 4a and other applicable laws.

- **Advocate for accessibility:** The AI Act includes provisions for accessibility. It is important that supervisory authorities have good relations with the disability movement, so they have detailed knowledge of the needs of persons with disabilities when they investigate complaints about AI systems that are not accessible. Together we can ensure that AI is usable by and for everyone.

- **Influence national policies:** AI will have an impact on important areas such as education, social security and public administration. Organisations for people with disabilities need to influence these policies to ensure that they meet the needs of people with disabilities as more AI is deployed.

In this chapter, we summarise when the various parts of the AI Act begin applying and what you and your organisation can do at national level. **Entry into force** means that a law has formally become part of the legal framework; **application dates** determine when particular rules must be followed.

14.2 Detailed timeline of AI Act implementation

Timeline checked in October 2026. The AI Act applies in stages, not on one single date.

The AI Omnibus (Regulation (EU) 2026/1744), is adopted legislation dated 8 July 2026 and published on 24 July 2026. It entered into force on 27 July 2026 and changed the main high-risk application dates.

Entry into force of the amendment does not mean that every amended obligation applies immediately.

14.2.1 Milestones already reached

- **12 July 2024: publication of the AI Act.** Regulation (EU) 2024/1689 was published in the Official Journal.

- **1 August 2024: entry into force.** The AI Act entered into force. This did not mean that all obligations began applying immediately.
- **2 February 2025: first rules began applying.** The general provisions, including definitions and AI literacy, and the original prohibitions began applying.
- **10 July 2025: final General-Purpose AI Code of Practice published.** The Code of Practice became available as a voluntary tool to help model providers demonstrate compliance, not as an additional mandatory obligation.
- **2 August 2025: general-purpose AI and governance stage.** Rules for providers of general-purpose AI models began applying, subject to transitional arrangements. Member States had to designate national competent authorities and adopt national rules on penalties. A deadline having passed does not establish that every country completed these tasks.
- **24 and 27 July 2026: AI Omnibus publication and entry into force.** The adopted amending regulation was published on 24 July 2026. It entered into force on 27 July 2026.
- **2 August 2026: general application stage.** Transparency rules and other applicable provisions began applying, while the main high-risk requirements remained subject to later dates. The comparison below identifies specific changes rather than treating this as a single deadline for all AI systems.

14.2.2 How the AI Omnibus changed the deadlines

14.2.2.1 Synthetic-content marking — Article 50(2)

- **Original deadline:** 2 August 2026.
- **Deadline under the AI Omnibus:** 2 December 2026.
- This transitional deadline applies to qualifying systems already placed on the market before 2 August 2026. It does not postpone all transparency duties.

14.2.2.2 National AI regulatory sandboxes

- **Original deadline:** 2 August 2026.

- **Deadline under the AI Omnibus:** 2 August 2027.
- Member States must have at least one national AI regulatory sandbox operational.

14.2.2.3 High-risk AI systems listed in Annex III

- **Original deadline:** 2 August 2026.
- **Deadline under the AI Omnibus:** 2 December 2027.
- This concerns the main high-risk rules for listed systems, such as relevant uses in employment, education and essential services.

14.2.2.4 Annex I product-related high-risk AI — Article 6(1)

- **Original deadline:** 2 August 2027.
- **Deadline under the AI Omnibus:** 2 August 2028.
- This concerns the main high-risk rules for AI that is itself a product, or a safety component of a product, covered by the legislation listed in Annex I, where the relevant third-party conformity-assessment conditions are met.

14.3 What needs to be done? Steps to take for national implementation

To successfully implement the AI Act at the national level, member states must undertake a comprehensive and coordinated approach that addresses various critical areas. Here's what is required:

1. **Legislative alignment:** Member States need to update their laws to comply with the AI Act, which provides a legal framework for consistency. For example, while the AI Act outlines conditions for using facial recognition by police, it requires specific national legislation to authorize its use. Once in place, the AI Act regulates how and why facial recognition can be used ethically. Alternatively, members can choose to ban it entirely in public areas.

2. **Regulatory bodies and oversight:** Member states should establish or designate regulatory authorities responsible for overseeing AI activities by 2 August 2025. These bodies must ensure robust oversight, particularly for high-risk AI systems, to prevent misuse and uphold ethical standards. Supervisory authorities will need to cooperate with equality ombudsmen and data protection authorities to effectively address issues of bias and discrimination.

   In addition, incorporating the expertise of people who have the lived experience of having a disability is crucial for these authorities to understand and address the particular challenges faced by members of our community.

14.4 Recommendations to EDF members

Here are the key steps that organisations of persons with disabilities can take to prepare for the implementation of the AI Act in their country:

1. **Learn about the AI Act, the AI Omnibus**, and explain to your members what the AI Act is and what it means for persons with disabilities.

2. **Stay updated on the implementation work of your government**

For example, you can keep an eye on whether your government is planning new legislation to allow government agencies to use AI:

- Assessment of applications for government benefits.
- Detection of fraud in social security and benefits.
- Policing and surveillance of public spaces.
- For surveillance in care such as monitoring people with dementia.
- Education for grading, admissions or to detect cheating during exams.
- Triaging in health care (i.e. introducing a chatbot as an option to having people call a hotline to discuss with a nurse if they should go to the doctor / emergency).
- The public sector and in the judicial system.

3. **Raise awareness** about the potential benefits and challenges of using AI systems for Persons with disabilities, such as improving accessibility, personalisation, autonomy, participation and dignity, but also creating barriers, discrimination, exclusion, stigmatisation and manipulation. You can find more information about these benefits and challenges in the section below.

4. **Connect with digital rights organisations working on AI.**

EDRi is an umbrella with member orgs in different countries. Here you can find a list of EDRi members Organisations Archive - European Digital Rights (EDRi).

5. **Participate in the public debate and policy making on AI** by raising awareness and mobilising your members and allies to voice their opinions and demands on AI and its impact on Persons with disabilities, such as through campaigns, petitions, events, media, social media, etc. You can find more information about how to do so in the section below.

6. **Call on your government to follow the recommendation of the Special Rapporteur on the rights of persons with disabilities,** who urged states to support your organisations in monitoring and advocating for disability-inclusive AI.

   Tell your government that you need resources and training to ensure that AI respects and promotes the rights of persons with disabilities, and that you can challenge any harmful or discriminatory uses of AI. You have a right to participate in the development and governance of AI, and your government should help you do so.[82]

7. **Apply for funding** from organisations that aim at strengthening the advocacy capabilities of organisations protecting fundamental rights when it comes to AI.

   For example, the European AI and Society Fund.

8. **Identify relevant authorities in your country** that protect fundamental rights and market surveillance authorities.

[82] Gerard Quinn, A/HRC/49/52: Artificial Intelligence and the Rights of Persons with Disabilities - Report of the Special Rapporteur on the Rights of Persons with Disabilities, 28 December 2021, paragraph 76(g) [accessed 7 October 2024].

9. **Advocate for funding** on the use of AI that is empowering for persons with disabilities.

10. **Advocate for funding** for organisations of persons with disabilities to work on advocacy on AI.

15 Assessing shortcomings of the AI Act

15.1 The choice to design the law based on risks instead of rights

EDF's digital rights allies have criticised the risk-based approach. They argue that a rights-based approach would have been better. [83]

This is because the risk categories in the AI Act are defined categorically by politicians and the way they are defined in the AI Act does not fully protect marginalised groups from real harms.

People with disabilities can face both intersectional discrimination and cumulative harm, two related but distinct concepts that the AI Act does not fully address.

Cumulative harm refers to the cumulative effects of repeated smaller discriminatory acts that together cause a significant negative impact. This concept emphasises how seemingly minor discriminatory acts can add up and cause significant hardship. For example, people with disabilities can face numerous barriers in the labour market, such as inadequate accommodation, biassed hiring and limited career development opportunities, that in combination can lead to persistent unemployment or underemployment.

Intersectionality examines the interplay of different grounds of discrimination that are part of one's identity, such as race or ethnicity, gender, age, disability and sexual orientation, and how they collectively impact experiences of oppression and advantage. It shows that a person's complex identity leads to different forms of discrimination and privileges that are not recognisable when these factors are considered separately.

[83] 'The EU Should Regulate AI on the Basis of Rights, Not Risks', Access Now, 2021 [accessed 6 October 2024].

For example, intersectionality shows us that racialised women with disabilities are often discriminated against on multiple levels in their professional environment because they are overlooked for promotions or receive unequal wages, more so than their white, male or non-disabled colleagues.

These problems highlight the limitations of the current AI Act, which is based on a risk-based approach established by politicians. The risk categories do not fully protect marginalised groups from real harm as these issues are not fully captured by the definition of risk in the Act. However, the AI Act is what we have, and it is our job to make the most of it. [84]

15.2 Accessibility in GPAI and minimal risk AI

While Article 16(l) of the AI Act fulfils our call for accessibility by stating that high-risk AI systems must comply with accessibility requirements, we still believe it would have crucial to extend these requirements to GPAI (General Purpose AI) and low-risk AI. This is important because what might be considered low or medium risk for the general population can actually be high risk for persons with disabilities.[85] [86]

This is particularly unfortunate because many AI tools used by persons with disabilities, such as personal assistants, text or speech generators, AI that describe the content of an image, voice-controlled devices, and personalised AI systems, fall under GPAI and low-risk categories. Without mandatory accessibility requirements, these tools won't have to be accessible unless they are covered by the Web Accessibility Directive or the European Accessibility Act.

[84] Access Now and others, 'Ensure Fundamental Rights Protections in the Council Position on the AI Act', 2023.
[85] European Disability Forum, Disability Perspective on Regulating Artificial Intelligence, 8 November 2021, pages 6–8 See the section called 'Trustworthy AI'.
[86] European Disability Forum (EDF) and others, 'EU's AI Act Fails to Set Gold Standard for Human Rights', European Disability Forum, 2024 [accessed 8 October 2024].

15.3 Shortcomings introduced by the AI Omnibus

The AI Omnibus amends the AI Act with the stated aim of simplifying its application and reducing administrative burdens. However, several changes weaken safeguards that matter for persons with disabilities. These changes add to the shortcomings of the original Act discussed above: they expand permission to process sensitive personal data, make access to information less direct for fundamental rights authorities, delay high-risk protections, weaken AI literacy obligations and reduce transparency.

This subsection summarises the main concerns explained in **EDF's Briefing on the AI Omnibus**, written for organisations of persons with disabilities.

15.3.1 Wider permission to process sensitive personal data

The Omnibus expands permission to process sensitive personal data without individual consent, with the argument that the data will be used to detect and correct bias. However, it does so more widely than it expands the obligation to test for bias. The permission to process sensitive personal data is no longer limited to providers of high-risk AI systems. It also covers organisations using those systems and, under certain conditions, AI systems at other risk levels.

This is not an unrestricted permission. Organisations must establish that anonymised or synthetic data is insufficient, use the sensitive data only for bias detection and correction, and comply with restrictions on reuse and sharing. Nevertheless, EDF is concerned that these safeguards depend heavily on the organisations themselves assessing whether processing is necessary and whether they have respected the limits.

These concerns are shared by the European Network of Equality Bodies (Equinet) and the European Network of National Human Rights Institutions (ENNHRI). In their joint statement on the Omnibus proposals, they warned that expanding permission to process sensitive personal data for bias detection and correction risks normalising its large-scale collection.[87]

[87] European Network of National Equality Bodies (Equinet) and European Network of National Human Rights Institutions (ENNHRI), Joint Equinet–ENNHRI Statement on the Digital Omnibus.

Their criticism highlights an important distinction: preventing discrimination is essential, but it does not justify collecting more sensitive data than necessary.

For persons with disabilities, the concern goes beyond privacy. Disability-related data can reveal deeply personal aspects of a person's body, communication and daily life. Inclusive design should mean that persons with disabilities help shape technology on fair terms, not simply that their data becomes available to improve systems owned by others.
Preventing discrimination must not become a justification for unnecessary data collection or a substitute for meaningful participation.

15.3.2 Less direct access to information for fundamental rights authorities

Under the original Act, equality bodies and other authorities designated under Article 77 could request relevant documentation directly from providers and organisations using high-risk AI. The Omnibus requires requests under this provision to go through market surveillance authorities instead.

Important requirements remain: market surveillance authorities must act without undue delay, obtain and share the necessary information, and cooperate with fundamental rights authorities. The amendment also preserves any information-gathering powers those bodies have under other EU or national laws. It therefore does not remove every route through which they can obtain information.

Even so, removing the direct route under Article 77 makes specialised authorities more dependent on another body's capacity and responsiveness. EDF is concerned that this can delay investigations and distance equality and human rights expertise from enforcement. Effective protection against discrimination requires more than checking technical compliance.

15.3.3 Longer waits for high-risk AI safeguards

The Omnibus delays the application of the main rules for stand-alone high-risk AI systems listed in Annex III from August 2026 to December 2027. It also postpones the rules for high-risk AI covered by the product legislation in Annex I from August 2027 to August 2028.

These delays matter because AI already influences decisions about employment, education, benefits and essential services. People affected by those decisions must wait longer for the full set of safeguards promised by the Act. Delaying obligations does not delay the risks that made those obligations necessary.

15.3.4 Weaker obligations on AI literacy

The original Act required providers and organisations using AI to ensure a sufficient level of AI literacy among relevant staff. The Omnibus replaces this with an obligation to support its development. Supporting training is not the same as ensuring that people operating or overseeing AI understand its limitations and risks.

This is particularly important where staff use AI to make decisions affecting persons with disabilities. For example, an official assessing disability-related benefits may rely too heavily on an AI recommendation without understanding its assumptions or recognising when it should be questioned. Human involvement provides little protection if the person involved lacks the knowledge and confidence to challenge the system.

15.3.5 A transparency safeguard preserved, but weakened

Providers must still register certain systems in the public database when they assess that a use listed in Annex III qualifies for the exception from high-risk classification. Preserving this requirement was important: it creates a record that can help authorities and civil society identify systems and scrutinise providers' assessments.

However, the Omnibus reduces the information required for registration. The safeguard therefore remains but becomes less useful for independent scrutiny. **The distinction matters: registration was not abolished, but the transparency it provides was weakened.**

Implications for disability organisations: Taken together, these changes increase the importance of independent scrutiny. Organisations of persons with disabilities can contribute by documenting harmful uses, working with equality and data protection bodies, and advocating for properly resourced enforcement. Simplification should make compliance easier to understand, not make discrimination harder to investigate or leave people with weaker protection.

15.4 European Commission review of prohibited and high-risk AI

The AI Act provides a process for reconsidering the boundaries of its risk categories. Under Article 112(1), the European Commission assesses annually whether the list of prohibited AI practices in Article 5 and the list of high-risk uses in Annex III need updating. Its first report on the review of prohibitions and high-risk AI was adopted on 20 May 2026. This review concerns which practices and uses these lists cover, rather than every obligation applying to high-risk AI.

The Commission emphasised that the assessment was still at an early stage and that practical experience with the rules was limited. It explained that a fuller evaluation of the prohibitions would depend on evidence about their application and any gaps that emerge. Similarly, assessing the coverage of high-risk AI would benefit from guidance on classification and experience of how the rules work in practice. The review should therefore not be read as confirmation that all gaps in protection have been resolved.

Why continued monitoring matters: This review process provides an opportunity to examine emerging risks and gaps in protection alongside evidence from the practical application of the law. For organisations of persons with disabilities, documenting inaccessible or discriminatory AI uses can help show where existing rules are not being followed and where the rules themselves may leave gaps. The Commission's assessment is distinct from the concerns explained in this chapter: deciding not to expand a list at a particular stage does not mean that every disability-related concern has been resolved.

16 Glossary

This glossary includes terms that the Forum thinks will help non-experts understand artificial intelligence. Not all are legally defined in the AI Act, but for those that are, we have included their legal definitions.

Accessibility

- Meaning: Designing AI systems so that they can be used by everyone, including people with disabilities.
- Example: AI software that is compatible with screen readers for visually impaired users.

AI (Artificial Intelligence)

- Meaning: Technology that enables machines to mimic human behaviour, such as making decisions, recognizing speech, and translating languages.
- Example: Virtual assistants like Siri and Alexa use AI to understand and respond to user commands.

AI Act

- Meaning: A European Union law that regulates the use of AI systems to protect human rights and ensure public safety.

AI Literacy

- Meaning: Skills, knowledge, and understanding that allow companies that make AI, organisations that use AI, and persons affected by AI systems to make informed decisions about the use of AI systems, and to be aware of the opportunities, risks, and potential harms AI can cause.
- Legal Definition (AI Act Article 3.56): "AI literacy means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause."

AI Office

- Meaning: A unit within the European Commission with expertise in AI that plays a coordinating role.
- Legal Definition (AI Act Article 3.47): "AI Office means the Commission’s function of contributing to the implementation, monitoring and supervision of AI systems and general-purpose AI models, and AI governance, provided for in Commission Decision of 24 January 2024; references in this Regulation to the AI Office shall be construed as references to the Commission."

AI System

- Meaning: A machine that uses AI to perform tasks like predictions, decisions, or recommendations.
- Example: AI used to sort job applications or identify faces in security cameras.

- Legal Definition (AI Act Article 3.1): "AI system means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

Algorithm

- Meaning: A set of rules or steps followed by a computer to perform a task.
- Example: Algorithms decide which ads you see on social media.

Bias (in AI)

- Meaning: When an AI system unfairly favours or disadvantages certain groups of people due to how it was trained or the data it was given.
- Example: AI and recruitment tool that frequently rejects applications from people with disabilities. This happens because the training data sets traits of persons without disabilities as the ideal standard for who is a good candidate for the job.

Biometric AI System

- Meaning: AI that identifies people based on physical or behavioural characteristics like facial features, fingerprints, or voice.
- Example: Using facial recognition to unlock a phone and law enforcement using it to identify suspects or locate missing individuals.
- Legal Definition (AI Act Article 3.34): "Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data."

Deployer

- Meaning: An organization or person that uses an AI system created by someone else.

- Example: EDF uses an AI-powered chatbot on our website to answer general questions about our policies, work, and how to contact EDF employees. By using this AI system, EDF becomes a deployer of an AI-system.
- Legal Definition (AI Act Article 3.4): "Deployer means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity."

Delegated Act

- Meaning: A law passed by the European Commission that provides more detailed rules to implement the AI Act.

Fundamental Rights

- Meaning: Within the European Union's legal framework, fundamental rights refer to human rights safeguarded by the EU's "constitution," specifically the EU Charter of Fundamental Rights. These include various human rights such as equality, accessibility, privacy, and freedom from discrimination, which must be respected whenever EU-laws apply.

General-Purpose AI model

- Meaning: An AI model trained on a large amount of data that can perform many different tasks well. A model is the underlying technology that can be integrated into different applications.
- Example: GPT-4 is an AI model developed by the company OpenAI which works as the underlying technology in other applications Be my AI and Microsoft Co-pilot.
- Legal Definition (AI Act Article 3.63): "General-purpose AI model means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market."

General-Purpose AI system

- Meaning: An AI system that uses a general-purpose AI model and can be used for many different purposes, either on its own or as part of other AI systems.
- Example: The app Be my AI is an AI-system that uses the General-Purpose AI Model called GPT4 to describe images to people with blindness.
- Legal Definition (AI Act Article 3.66): "General-purpose AI system means an AI system which is based on a general-purpose AI model, and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems."

Guidelines

- Meaning: Recommendations and explanations issued by the European Commission to clarify how to implement specific parts of the AI Act, such as prohibited practices, transparency obligations, or the definition of an AI system.
- Example: The Commission may issue guidelines on how to meet accessibility requirements or how to interpret the definition of an AI system.
- Note: Guidelines are not legally binding, but they provide practical advice and reflect the Commission's interpretation of the law.

High-Risk AI

- Meaning: AI systems that can significantly impact people's lives, such as those used in hiring, healthcare, or law enforcement.
- Example: AI that decides whether someone gets a loan.

Low-Risk AI

- Meaning: AI systems with minimal impact on people's lives, such as those used in video games or spam filtering.

Machine Learning

- Meaning: A type of AI where computers learn from data to improve their performance on tasks.
- Example: An AI system learns to recognize faces better over time by being shown more examples.

Market Surveillance Authority

- Meaning: A government authority responsible for ensuring AI systems comply with the law and do not harm users.
- Legal Definition (AI Act Article 3.26): "Market surveillance authority means the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020."

Omnibus

- Meaning: In EU lawmaking, an omnibus is one law that makes changes to several existing EU laws at the same time. Instead of changing each law separately, several changes are grouped together in one law.
- Example: The Digital Omnibus makes changes to several EU digital laws. These include the AI Act, the General Data Protection Regulation (GDPR), and the ePrivacy Directive.
- Note: This glossary explains what "omnibus" means in the context of EU lawmaking. The term may be used differently in other legal systems. If you are reading about the laws of another country, do not assume that "omnibus" has exactly the same meaning.

Provider

- Meaning: A company or individual that creates and offers an AI system for others to use.
- Example: OpenAI has made ChatGPT that anyone can use; OpenAI is a provider of an AI system.
- Legal Definition (AI Act Article 3.3): "Provider means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge."

Regulatory Sandbox

- Meaning: A controlled environment where companies can test new AI technologies under supervision to ensure they are safe and ethical.

- Legal Definition (AI Act Article 3.55): "AI regulatory sandbox means a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision."

Special Categories of Personal Data

- Meaning: Personal data that is highly sensitive and can be misused to discriminate against individuals. This includes information about a person's race, health, political opinions, religious beliefs, sexual orientation, and other intimate details. Protecting this data is crucial to prevent abuse and ensure individuals are not unfairly treated or marginalized.
- Connection to Anti-Discrimination: Safeguarding these special categories of personal data is directly linked to anti-discrimination efforts. By restricting access to and processing of such sensitive information, the AI Act aims to prevent biased decisions and actions that could harm individuals or groups, particularly those with disabilities or belonging to minority communities.
- Legal Definition (AI Act Article 3.37): "Special categories of personal data means the categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725."

Transparency (in AI)

- Meaning: Making AI systems clear and understandable, so people know how and why decisions are made.
- Example: A company explains how its AI decides which candidates to shortlist for a job.

Unacceptable Risk AI

- Meaning: AI systems that are banned because they pose serious risks to human dignity, democracy, or fundamental rights.
- Example: AI systems that manipulate emotions to influence decisions at work.

17 Document credits

This document was prepared by:
Kave Noori, AI Policy Officer at the European Disability Forum

With the support from the colleagues at EDF secretariat:
Marine Uldry, André Felix and Ness James.

The European Disability Forum
Mundo Madou
Avenue des Arts 7-8
1210 Brussels, Belgium.
www.edf-feph.org
info@edf-feph.org

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