EUROPEAN POLICY GUIDELINES ON AI AND ALGORITHM-DRIVEN DISCRIMINATION

for equality bodies and other national human rights structures



In collaboration with
the Interfederal Centre for Equal Opportunities (Unia), Belgium,
the Non-Discrimination Ombudsman (YVV), Finland,
and the Commission for Citizenship and Gender Equality (CIG), Portugal

Kris Shrishak
Soizic Pénicaud

Co-funded
by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Co-funded and implemented
by the Council of Europe

EUROPEAN POLICY GUIDELINES ON AI AND ALGORITHM-DRIVEN DISCRIMINATION

for equality bodies and other national human rights structures

Kris Shrishak
Soizic Pénicaud

Council of Europe

This publication was produced with the financial support of the European Union and the Council of Europe. Its contents are solely the responsibility of the authors. The views expressed herein can in no way be taken to reflect the official opinion of either the European Union or the Council of Europe.

The reproduction of extracts (up to 500 words) is authorised, except for commercial purposes, as long as the integrity of the text is preserved, the excerpt is not used out of context, does not provide incomplete information or does not otherwise mislead the reader as to the nature, scope or content of the text. The source text must always be acknowledged as follows: "© Council of Europe, year of the publication". All other requests concerning the reproduction/ translation of all or part of the document should be addressed to the Publications and Visual Identity Division, Council of Europe (F-67075 Strasbourg Cedex or publishing@coe.int).

All other correspondence concerning this document should be addressed to the Hate Speech, Hate Crime and Artificial Intelligence Unit of the Council of Europe's Inclusion and Anti-Discrimination Programmes Division, Council of Europe, F-67075 Strasbourg Cedex, E-mail: anti-discrimination@coe.int

Cover and layout: Publications and Visual Identity Division Council of Europe

Photos: Shutterstock

© Council of Europe, December 2025

Contents

ABBREVIATIONS	**5**
ACKNOWLEDGEMENTS	**7**
EXECUTIVE SUMMARY	**8**
INTRODUCTION	**10**
Context of the guidelines	10
Aim of the guidelines	11
Methodology	11
Structure of the guidelines	12
PART I	**13**
1. GENERAL CONTEXT OF THE AI ACT	**14**
2. PROHIBITIONS	**17**
2.1. Introduction to prohibited AI practices	17
2.2. AI systems that manipulate, deceive or exploit vulnerabilities of people	19
2.3. Social scoring	23
2.4. Risk assessment of committing a criminal offence	26
2.5. Scraping to build or expand facial recognition databases	28
2.6. Emotion recognition	30
2.7. Biometric categorisation	32
2.8. Remote biometric identification	34
3. HIGH-RISK AI SYSTEMS	**39**
3.1. Classification of high-risk AI systems	39
3.2. Amending the list of high-risk use-cases	43
3.3. Risk management system requirements	45
3.4. Data governance requirements	47
3.5. Fundamental rights impact assessment (FRIA)	50
3.6. EU database for high-risk AI systems listed in Annex III	54
4. TRANSPARENCY OF AI SYSTEMS REQUIREMENTS	**61**
4.1. Context and significance	61
5. ENFORCEMENT	**64**
5.1. Powers of bodies protecting fundamental rights	64
5.2. Remedies	68
5.3. Co-operation mechanisms	71
PART II	**77**
6. STANDARDS DIRECTIVES	**78**
6.1. General context	78
6.2. Changes to mandate and resourcing	79
6.3. Changes to powers	82
7. THEMATIC FOCUS	**90**
7.1. Thematic focus: Law enforcement, migration, asylum and border control	90
7.2. Thematic focus: Education	95
7.3. Thematic focus: Employment	96
7.4. Thematic focus: Social security and employment support services	98
REFERENCES	**101**

Abbreviations

ADM	Automated decision making
AFAR	Algorithmic fairness for asylum seekers and refugees
AI	Artificial intelligence
AI Act	Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence
AVMSD	Audiovisual Media Services Directive (2010/13/EU)
CCTV	Closed-circuit television
CJEU	Court of Justice of the European Union
CNIL	La Commission nationale de l'informatique et des libertés (French data protection authority)
The Commission	European Commission
Convention 108+	The Council of Europe Modernised Convention No. 108 for the Protection of Individuals with Regard to the Processing of Personal Data
CSOs	Civil society organisations
DMA	Digital Markets Act
DPA	Data protection authority
DPIA	Data protection impact assessments
DSA	Digital Services Act
EB	Equality body
ECRI	European Commission against Racism and Intolerance
EEA	European Economic Area
Equinet	The European Network of Equality Bodies
EU	European Union

Abbreviations

FARI	AI for the Common Good Institute
Framework Convention	Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225)
FRIA	Fundamental rights impact assessment
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679)
HUDERIA	Methodology for the risk and impact assessment of AI systems from the point of view of human rights, democracy and the rule of law
LEA	Law enforcement authority
LED	Law Enforcement Directive
Medical Device Regulation	Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices
MSA	Market surveillance authority
NHRS	National human rights structure(s)
OCR	Optical character recognition
Unia	Interfederal Centre for Equal Opportunities
PEReN	Le Pôle d'expertise de la régulation numérique (The Centre of Expertise for Digital Platform Regulation)
RBI	Remote biometric identification systems
STEM	Science, technology, engineering and mathematics

For a glossary, see the EU AI Act, Article 3 on definitions

Acknowledgements

This report was prepared in the context of the "Upholding equality and non-discrimination by Equality bodies regarding the use of artificial intelligence in public administrations" project, which is funded by the European Union via the Technical Support Instrument and co-funded by the Council of Europe. The project is implemented by the Council of Europe in co-operation with the European Commission, the Interfederal Centre for Equal Opportunities (Unia, Belgium), the Non-Discrimination Ombudsman (Finland) and the Commission for Citizenship and Gender Equality (Portugal).

The report was authored by Kris Shrishak (international consultant, Council of Europe) and Soizic Pénicaud (international consultant, Council of Europe).

The Council of Europe wish to extend their gratitude to the project's beneficiary institutions and to the European Commission for their sustained engagement throughout the drafting process, and in particular to: Nele Roekens and Nadine Brauns (Interfederal Centre for Equal Opportunities, Unia, Belgium); Tiina Valonen and Ville Rantala (Non-Discrimination Ombudsman, YVV, Finland); Carla Peixe, Ana Martinho Fernandes, Alexandra Andrade and Susana Miguel (Commission for Citizenship and Gender Equality, CIG, Portugal), and Massimiliano Santini (Reform and Investment Task Force, Secretariat-General, European Commission) as well as to Menno Ettema, Sara Haapalainen, Ayça Dibekoğlu, and Delfine Gaillard (Anti-discrimination Department, Council of Europe).

Special thanks to Louise Hooper (international consultant, Council of Europe) for her expert input and peer review of the draft, and Milla Vidina (Equinet, European Network of Equality Bodies) for her constructive feedback.

The report also benefited from the contributions of national experts from equality bodies and civil society organisations who participated in interviews in spring 2025. Their perspectives enriched the analytical and operational sections of these guidelines.







Executive summary

The European policy guidelines on AI and algorithm-driven discrimination set out how equality bodies and, where relevant, other national human rights structures (NHRS), can use their mandates under European legal frameworks – in particular Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (EU AI Act) – to safeguard fundamental rights and address risks of discrimination in the deployment of AI and automated decision-making (ADM) systems, especially in the public sector. At a time when such systems are increasingly deployed across public and private services, these institutions play a critical role in safeguarding fundamental rights and addressing risks of discrimination.

The guidelines are organised into two main sections. The first section focuses on the key provisions of the EU AI Act that are most relevant for equality bodies and NHRS, and explains how these can be used in practice.

1. Prohibited AI systems - The guidelines explain the explicit prohibitions laid down in Article 5 for AI systems that are considered incompatible with Union values and fundamental rights, including the right to non-discrimination. These prohibitions cover, among others and in certain conditions, AI systems that manipulate, deceive, exploit vulnerabilities, systems used for social scoring or criminal risk assessments, the scraping of images to build or expand facial recognition databases, as well as systems for emotion recognition, biometric categorisation and real-time remote biometric identification.

2. High-risk AI systems - The guidelines clarify how AI systems used in critical areas such as biometrics, law enforcement, welfare and social security, employment, education and access to essential services may be classified as "high risk" and therefore subject to strict obligations on risk management, data governance, documentation, human oversight and fundamental rights impact assessments. They outline what equality bodies and NHRS should take into account when engaging with classification decisions and when reviewing compliance with these obligations from an equality and non-discrimination perspective.

3. Transparency and databases - The guidelines describe how new transparency requirements and EU-level databases – in particular the EU database for certain high-risk AI systems – can create opportunities for oversight. Registration and logging obligations can help equality bodies and NHRS to identify where AI systems are used to for the purpose of their monitoring and inquiries, and to support individuals who may be affected.

4. Enforcement - The guidelines examine the role of bodies protecting fundamental rights listed under Article 77 AI Act, the remedies available to individuals, and the co-operation mechanisms and opportunities between equality bodies, data protection authorities, market surveillance authorities and other regulators and actors. They provide policy recommendations on how equality bodies and NHRS can use their complaint-handling, inquiry, litigation, advisory and awareness-raising powers to prevent, detect and redress algorithmic discrimination within this multistakeholder co-operation framework.

Across this first section, the roles and responsibilities of equality bodies and NHRS are explicitly articulated with targeted policy recommendations on how these institutions can prevent, detect and respond to algorithmic discrimination, such as through promoting equality, conducting awareness raising, supporting complaints, taking legal action and working closely with national competent authorities in the broader AI oversight system.

The second section of the guidelines has two pillars. First, it analyses the new EU Directives on standards for equality bodies ("Standards Directives") and explains how their provisions on mandate, independence, resources and powers – including promotion, access to justice and data collection – can be mobilised to address discrimination risks linked to AI and ADM systems. Second, it offers thematic entry points of AI use in sectors often covered by the mandates of equality bodies: law enforcement, migration, asylum and border control, welfare and social security, employment and education. For each sector, it links concrete uses of AI to the relevant provisions of the AI Act (prohibitions, high-risk classifications, transparency and registration requirements) and outlines where sector-specific safeguards and the involvement of equality bodies and NHRS are essential.

The guidelines are designed to be adaptable to different national contexts and to support equality bodies and NHRS in advising policymakers and regulators, engaging with Council of Europe standards such as Convention 108+ and the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, and ensuring that AI and ADM systems are developed and used in line with European equality and non-discrimination law.



Introduction

Context of the guidelines

Public administrations across Europe are using artificial intelligence (AI) and/or automated decision-making (ADM) systems in a wide range of policy areas, including migration, welfare, justice, education, employment, tax, law enforcement or healthcare. Such systems are also deployed in critical areas of the private sector, such as banking (e.g. credit scoring applications) and insurance. Although AI and ADM systems present significant risks of discrimination, challenges remain in identifying and mitigating these risks. The recent report "Legal protection against algorithmic discrimination in Europe: current frameworks and remaining gaps" (Xenidis 2025), drafted as part of the European Union–Council of Europe project, highlights critical issues: lack of awareness of discrimination risks, lack of transparency and lack of meaningful information about the use of AI/ADM systems by public authorities, challenges in access to justice and a lack of standardised governance practices. Thus, equality bodies (EBs) and other national human rights structures (NHRS) have a key role in promoting fundamental rights-compliant deployment of AI/ADM systems by public sector organisations.

New legal frameworks, including the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law[1] and the European Union's AI Act,[2] aim to protect fundamental rights and prevent discrimination in AI systems. At the same time, the European Union has adopted two new directives introducing minimum standards to strengthen the role and capacities of equality bodies in Europe (henceforth "the Standards Directives").[3] Proper implementation of these new frameworks is key to ensuring their effectiveness.

Aim of the guidelines

Against this backdrop, these policy guidelines aim to equip equality bodies and other NHRS, especially in the European Union, to tackle discrimination in AI/ADM systems, by:

- updating them on their responsibilities regarding the changing regulatory environment on artificial intelligence, including how it directly or indirectly affects their mandate;
- offering them specific guidelines, recommendations and examples of good practices for overseeing the application and implementation of the new regulations, while linking them to existing regulation;
- acting as a resource for equality bodies and NHRS to assist and advise national stakeholders, such as policymakers and regulators, in relation to human rights, equality and non-discrimination.

These guidelines focus in particular on AI/ADM systems in the public sector.

Methodology

These guidelines provide an overview of the new missions, mandates of opportunities for equality bodies and NHRS in light of new regulations, as well as broad guidelines that are adaptable to every national context.

The guidelines draw from, and build on:

- desk research and legal analysis;

1. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (Vilnius, 5 September 2024), henceforth "the Council of Europe Framework Convention".
2. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, henceforth the "AI Act".
3. Council Directive (EU) 2024/1499 of 7 May 2024 on standards for equality bodies in the field of equal treatment between persons irrespective of their racial or ethnic origin, equal treatment in matters of employment and occupation between persons irrespective of their religion or belief, disability, age or sexual orientation, equal treatment between women and men in matters of social security and in the access to and supply of goods and services, and amending Directives 2000/43/EC and 2004/113/EC, Directive (EU) 2024/1500 of the European Parliament and of the Council of 14 May 2024 on standards for equality bodies in the field of equal treatment and equal opportunities between women and men in matters of employment and occupation, and amending Directives 2006/54/EC and 2010/41/EU, henceforth "the Standards Directives".

- the findings of a report conducted as part of the European Union–Council of Europe project (Xenidis 2025);
- five semi-structured interviews with representatives of civil society organisations and equality bodies who were chosen based on their expertise on the topic.

The EU has recently adopted other regulations in the field of digital governance. These include, for example, the "Digital Services Package", composed of the Digital Services Act[4] (DSA) and the Digital Markets Act[5] (DMA), which focuses on the regulation of online services. These regulations, and the DSA in particular, also touch upon the need to protect fundamental rights in the digital sphere in terms of risk identification and mitigation: for instance, Article 34 of the DSA on risk assessment by providers of very large online platforms and of very large online search engines and Article 35 on the mitigation of those risks both include risks of discrimination. However, the DSA and the DMA do not cover uses of AI systems in the public sector. As these guidelines focus particularly on AI/ADM systems in the public sector, they do not directly touch upon the DSA and the DMA.

Structure of the guidelines

The first part of the guidelines is structured around the articles in the AI Act which are most critical for equality bodies and other NHRS, either because they directly or indirectly affect their mandate, or because they imply significant changes for other institutions, regulators or governance frameworks. For each of these articles, links are made with existing regulations on data protection (the European Union General Data Protection Regulation,[6] the European Union Law Enforcement Directive[7] and the Council of Europe Convention 108+ for the Protection of Individuals with regard to Automatic Processing of Personal Data), and the Council of Europe Framework Convention.

The second part of the guidelines offers an overview of the Standards Directives, which are relevant for equality bodies in the context of equality in AI systems, and thematic entry points for the sectors of law enforcement; migration, asylum and border control; welfare and social security; employment; and education, where uses of AI systems pose significant risks in terms of discrimination. Each theme marks the AI Act articles which are relevant for the sector.

4. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, henceforth "Digital Services Act".
5. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, henceforth "Digital Markets Act".
6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, henceforth "General Data Protection Regulation" or GDPR.
7. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, henceforth the "Law Enforcement Directive" or LED.

PART I



1. General context of the AI Act

The AI Act lays down "a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union", to "promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union."[8]

The AI Act came into force on 2 August 2024, and its different requirements will apply gradually over time until full implementation in 2030. As it is a regulation, the AI Act is directly applicable and does not need transposition into national law. However, many steps, including national governance and regulatory apparatus need to be established through national implementation laws. At the time of writing this, the implementation of the AI Act is in the early stages, and a considerable amount remains to be clarified.

8. AI Act, Recital 1.

While the AI Act offers new opportunities for equality bodies and NHRS to prevent and redress discrimination in AI systems, several of its characteristics should be kept in mind while reading these guidelines.

First, the definition of AI systems. Guidelines on the definition of an artificial intelligence system established by the AI Act were issued by the Commission on 6 February 2025. As noted by various commentators these are not binding law and may result in some confusion.[9] Organisations might claim that some ADM systems used in the public sector[10] could fall outside the scope of the AI Act, despite presenting risks related to anti-discrimination.[11] Such claims could rely on wrongly interpreting the definition. For instance, the AI Act states that an AI system "may exhibit adaptiveness",[12] has "varying levels of autonomy"[13] and has the "capability to infer."[14] Equality bodies and NHRS are strongly urged to use an interpretation of the definition of AI systems that is independent of the specific AI technique (such as machine learning or natural language processing) and that considers autonomy and adaptiveness as optional characteristics.[15]

Second, research and development is out of scope of the AI Act. "[A]ny research, testing or development activity regarding AI systems or AI models prior to their being placed on the market or put into service"[16] is not regulated by the AI Act. This allows even prohibited AI practices to be researched, tested and developed as long as they are not placed on the market or put into service. However, once placed on the market or put into service, the AI practice falls within the scope of this regulation. Merely labelling a deployment as an experiment or a study would not suffice to avail the research and development exception. "Testing in real world conditions"[17] of high-risk AI systems outside AI regulatory sandboxes, but not prohibited AI practices, are allowed temporarily and will not be deemed as placing on the market or put into service if they fulfil specific conditions.[18] Thus, it is important for EBs to address testing of high-risk AI systems based on the pre-existing legal toolbox.

Third, the AI Act will only apply to systems that have been placed on the market or put into service after the general date of application, barring "substantial modification" to already deployed AI systems. An exception exists for high-risk AI systems that

9. Kris Shrishak (2025), *EU's AI Act: Tread the Guidelines Lightly*, Tech Policy Press, available at www.techpolicy.press/eu-ai-act-tread-the-guidelines-lightly/; Algorithm Audit (February 2025) "Implementation of the AI Act: definition of an AI system", available at https://algorithmaudit.eu/knowledge-platform/knowledge-base/guidelines_ai_act_implementation/.
10. Lighthouse Reports (2023), *France's Digital Inquisition*, available at www.lighthousereports.com/investigation/frances-digital-inquisition/, both accessed 7 November 2025.
11. For a detailed analysis of this, see Xenidis 2025.
12. AI Act, Art. 3 (1).
13. AI Act, Art. 3 (1).
14. AI Act, Recital 12.
15. Kris Shrishak (2025), *EU's AI Act: Tread the Guidelines Lightly*, Tech Policy Press, available at www.techpolicy.press/eu-ai-act-tread-the-guidelines-lightly/; See also Algorithm Audit (2025), AI Act Implementation Tool, available at https://algorithmaudit.eu/technical-tools/implementation-tool/.
16. AI Act, Art. 2 (8).
17. AI Act, Art. 3 (57).
18. AI Act, Art. 60 lays down all the conditions to be fulfilled for testing in real-world conditions.

are intended to be used by public authorities, for which operators should comply with the requirements of the AI Act by 2 August 2030.[19]

Fourth, the AI Act's risk-based approach establishes different rules and obligations depending on the level of risk of AI systems. In practice, some practices will be prohibited (see Article 5), some AI systems will be considered high-risk and their operators therefore subjected to new obligations (see Article 6), and transparency requirements will apply to select AI systems (see Article 50). The systems that fall outside this scope will not be subjected to the same requirements, with a risk that AI operators could adopt "ethics washing" (Equinet 2025) and "de-risking practices" (Xenidis 2025) to avoid these requirements. However, this risk-based approach should be considered in light of the obligation of AI operators to respect fundamental rights and anti-discrimination law.

19. AI Act, Recital 177.



2. Prohibitions

2.1. Introduction to prohibited AI practices

2.1.1. Context and relevance

Article 5 lays down the list of AI systems prohibited under the AI Act, because "they contradict Union values of respect for human dignity, freedom, *equality*, democracy and the rule of law and fundamental rights enshrined in the Charter, *including the right to non-discrimination*, to data protection and to privacy and the rights of the child".[20] AI practices which are not considered prohibited under the AI Act can be so under other Union law.[21]

Such prohibitions have been in place since 2 February 2025. On 6 February 2025, the European Commission published guidelines on such prohibited practices, as per Article 96(1)(b) of the AI Act.[22] While they can give guidance on which practices

20. AI Act, Recital 28 *[emphasis added]*.
21. AI Act, Art. 5 (8).
22. European Commission (2025), "Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)", available at https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act, accessed 11 November 2025. Henceforth, "AI Act Prohibition guidelines".

should be prohibited or not, the guidelines have been criticised for remaining ambiguous.[23] The risk of ambiguity is for AI operators to engage in "de-risking strategies", namely, in case of doubt, to consider that a certain practice is not prohibited. In addition, such guidelines are non-binding, and only case law will allow for more clarity on prohibitions.

Market surveillance authorities (MSAs) report annually to the European Commission ("the Commission") on the use of prohibited practices that occurred during that year and the measures taken.[24] The Commission assesses "the need for amendment of the list of prohibited AI practices" once a year[25] and submits the findings to the European Parliament and the Council.[26]

The AI Office, established within the European Commission, is expected to develop "an objective and participative methodology for the evaluation of risk levels based on the criteria outlined in the relevant Articles and the inclusion of new systems" in Article 5.[27]

Connection with other regulation

The Council of Europe Framework Convention also provides for the possibility of a party to the convention to set up moratoriums or bans "where it considers such uses incompatible with the respect for human rights, the functioning of democracy or the rule of law."[28]

2.1.2. Role of equality bodies and other NHRS in addressing prohibited AI applications

This section presents the role that equality bodies and NHRS could play across all prohibited AI applications. Subsequent sections emphasise actions that equality bodies and NHRS can undertake which are specific to certain prohibitions.

Across all prohibitions, equality bodies and NHRS can:

- monitor prohibited applications, by consolidating examples of cases that have been or should be assessed under Article 5. These examples will help illustrate the importance of current prohibited uses and the potential need to expand to other applications due to their risks for fundamental rights, especially equality and non-discrimination. Such examples can be collected by collaborating with civil society organisations and academics who have studied these systems, analysing complaints received by equality bodies and

23. See e.g. Autoriteit Persoonsgegevens (2025), "Summary and next steps call for input on prohibition on AI systems for emotion recognition in the areas of workplace or education institutions", available at www.autoriteitpersoonsgegevens.nl/en/documents/summary-and-next-steps-call-for-input-on-prohibition-on-ai-systems-for-emotion-recognition-in-the-areas-of-workplace-or-education-institutions (2025), accessed 11 November 2025.
24. AI Act, Art. 74 (2).
25. AI Act, Art. 112 (1).
26. While the AI Act provides for the European Commission to assess the need to amend the list of prohibited practices, it does not allow the Commission to update the list within the AI Act. Such an update would require a separate legislative procedure.
27. AI Act, Art. 112 (11) (b).
28. Council of Europe Framework Convention, Art. 16 (4).

NHRS, and tracking litigation, including private litigation. Partnerships can also be considered with the EU Fundamental Rights Agency.

- contribute to the yearly assessments of the Commission under Article 112. This may take the form of sharing with the Commission the evidence on prohibited applications and dangerous AI systems currently not prohibited under the AI Act.
- contribute to the participatory methodology of assessment of risk levels of the AI Office.
- promote the enforcement of the prohibitions by market surveillance authorities, including by using the examples consolidated through monitoring.
- provide expertise on equality and non-discrimination to market surveillance authorities, who will be required to assess prohibitions due to harms to fundamental rights.
- receive complaints from the public, which could include deployments by private actors.

2.2. AI systems that manipulate, deceive or exploit vulnerabilities of people

2.2.1. Context and relevance

The AI Act prohibits harmful AI systems that manipulate, deceive or exploit vulnerabilities of people under Article 5 (1) (a) and (b). This prohibition covers many fundamental rights that are at risk: human dignity, autonomy of individuals, disability rights, non-discrimination due to age (rights of the child, rights of the elderly) or socio-economic situation.

Public sector organisations are not highly likely to intentionally deploy manipulative AI systems. But they could, accidentally, for example via the chatbots they deploy.

Examples

Chatbots are increasingly used in the public sector, including to give the public information about public services. In 2024, a chatbot deployed by the city of New York provided incorrect information about labour law.[29] Such tools are also likely to be used in the banking and insurance sectors.

29. Offenhartz J. (2024), "NYC's AI chatbot was caught telling businesses to break the law. The city isn't taking it down", *AP News*, available at https://apnews.com/article/new-york-city-chatbot-misinformation-6ebc71db5b770b9969c906a7ee4fae21, accessed 10 November 2025.

A chatbot could be prohibited under Art. 5 (1) (a) and/or (b):

- If such a chatbot deceives people by providing misleading information that results in a person taking a decision that results in harm such as encouraging the person to commit suicide,[30] then it could be prohibited under Art. 5 (1) (a).
- If, however, a chatbot exploits a person's socio-economic status and does not provide information (or provides incorrect information) about certain essential services such as access to means-tested welfare benefits, which results in financial difficulties, then it could be prohibited under Art. 5 (1) (b), because the AI system exploits the socio-economic situation of the person (see below). Depending on the circumstances, the latter might also be within the scope of Art. 5 (1) (a).

The two prohibitions are considered together because Art. 5 (1) (b) can be treated as *lex specialis* when there is an overlap with Art. 5 (1) (a).[31]

Assessing prohibitions under Article 5 (1) (a) and (b)

Assessing whether an AI system is prohibited under Art. 5 (1) (a) requires a five-step assessment fulfilling all of the following steps.

1. Has the AI system been placed on the market, put into service, or is it being used?[32]
2. Does the AI system deploy "subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques" or a combination of these?
3. Is the AI system deployed with "the objective, or the effect of materially distorting the behaviour of a person or a group"?
4. Has the AI system, by distorting the behaviour, "caused a person or group to take a decision that they would not have otherwise taken"?
   a. Has there been a significant impairment of the autonomy of the person/group (beyond merely being influenced through lawful persuasion)?
5. Has this decision of a person or group caused "or is [it] reasonably likely to cause that person, another person or group of persons significant harm"?
   a. How were they harmed? Physical, psychological, financial.
   b. Was the harm significant[33]? Severity based on combination of harms, cumulative effects of harms, scale of harm, reversibility of harm and duration of harm.[34]

30. Walker, L. (2023), "Belgian man dies by suicide following exchanges with chatbot", *Brussels Times*, available at www.brusselstimes.com/430098/belgian-man-commits-suicide-following-exchanges-with-chatgpt, accessed 10 November 2025.
31. AI Act Prohibition guidelines.
32. AI Act, Art. 3 (9)-(11). For the Commission's interpretation of "placed in the market, put into service, or being used", see the "Blue Guide" on implementation of EU product rules 2022, 2022/C247/01, Section 2.
33. Court of Justice of 7 September 2004, *Waddenvereniging and Vogelbeschermingsvereniging*, C-127/02, EU:C:2004:482 and of 11 April 2013, *Sweetman and Others*, C-258/11, EU:C:2013:220.
34. AI Act Prohibition guidelines, Paragraph 92.

Assessing whether an AI system is prohibited under Art. 5 (1) (b) requires a four-step assessment fulfilling all of the following steps:

1. Has the AI system been placed in the market, put into service, or is it being used?
2. Does the AI system exploit "any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation"?
   a. Age: children and elderly;
   b. Disability: includes physical, mental, intellectual and sensory impairments that hinder full participation of individuals in society;[35]
   c. Social or economic situation: includes persons living in extreme poverty, ethnic or religious minorities.[36]
3. Is the AI system deployed with the "objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group"?
4. Has the AI system, by distorting the behaviour, caused "or is reasonably likely to cause that person or another person significant harm"?

In relation to Art. 5 (1) (a), some important concepts are not self-evident. Terms such as "subliminal techniques beyond a person's consciousness", "purposefully manipulative techniques" and "deceptive techniques" are not defined in the AI Act.

- Subliminal techniques beyond a person's consciousness may involve stimuli that are not consciously perceived by people but are still processed by the brain and could influence their behaviour. Such stimuli could be audio or visual, or alter the perception of time.[37] Subliminal techniques could include "machine-brain interfaces or virtual reality".[38] In the context of "audiovisual commercial communications",[39] the Audiovisual Media Services Directive (AVMSD) already bans subliminal techniques.[40] In such a context, the prohibition in the AI Act, which applies only when an AI system is involved, is a special case of the prohibition in the AVMSD. Subliminal techniques could be seen as an example of manipulative techniques.
- Purposefully manipulative techniques could be used to "persuade persons to engage in unwanted behaviours," exploiting their biases or their emotional state

35. Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).
36. AI Act, Recital 29: "In addition, AI systems may also otherwise exploit the vulnerabilities of a person or a specific group of persons due to their age, disability within the meaning of Directive (EU) 2019/882 of the European Parliament and of the Council, or a specific social or economic situation that is likely to make those persons more vulnerable to exploitation such as *persons living in extreme poverty, ethnic or religious minorities" (emphasis added)*.
37. AI Act Prohibition guidelines, paragraphs 64-66.
38. AI Act, Recital 29.
39. Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (OJ L 95, 15.4.2010, p. 1); AVMSD, Art. 1 (h).
40. AVMSD, Art. 9 (1) (b).

"to deceive them by nudging them into decisions in a way that subverts and impairs their autonomy, decision making and free choices."[41] Such manipulation could include exploitation of personal data to direct personalised messages, for example targeted advertisements.

- Deceptive techniques present false and misleading information. Deception can take the form of audiovisual content such as "deepfakes" and deceptive chatbots. When assessing whether a technique is deceptive, the transparency measures in Article 50 are relevant because they may prevent deception by informing people that they are interacting with an AI system. However, despite transparency measures, the same techniques may still be manipulative.

The prohibition applies when an AI system is deployed with "the objective, or the effect of materially distorting the behaviour of a person or a group." This implies that the *intent* to materially distort behaviour is not necessary but the *effect* suffices. The European Commission, in its guidelines, states that even the likelihood[42] of the effect, for instance due to the presentation of the information,[43] without proof of the effect after harm has materialised, is sufficient. According to the Commission, the effect, or the likelihood of the effect, might fall on

1. the average consumer,[44] including the recognition that their decision-making capacity may be impaired by constraints, such as cognitive biases;[45] and
2. individuals or groups who might have been specifically targeted, or discriminated against.

Nevertheless, it is necessary that there is a plausible likelihood of a link between the "the objective, or the effect of materially distorting" and the subliminal, purposefully manipulative or deceptive technique deployed by the AI system.

To assess the reasonable likelihood of significant harm, the different forms of physical, psychological and financial harm need to be considered.[46] In addition, the significance of the harm needs to be assessed;[47] for example, the severity based on combination of harms, cumulative effects of harms, scale of harm (e.g. chatbots deployed at national level in the public sector, makes it likely they are to be used by many people), reversibility of harm and duration of harm.[48]

41. AI Act, Recital 29.
42. Judgment of the Court of Justice of Judgment of the Court (Fifth Chamber) of 26 October 2016. *Canal Digital Danmark A/S*. EU:C:2016:800, Case C-611/14, para 73.
43. Judgment of the Court of Justice of 19 December 2013, *Trento Sviluppo and Centrale Adriatica*, C-281/12, EU:C:2013:859.
44. Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ C 526, 29.12.2021, p. 1). See also Recital 18 of Directive 2005/29/EC for the definition of an average consumer: "reasonably well-informed and reasonably observant and circumspect, taking into account social, cultural and linguistic factors".
45. *Compass Banca SpA v Autorità Garante della Concorrenza e del Mercato (AGCM)*, Case C-646/22, EU:C:2024:957.
46. AI Act, Recital 29.
47. Court of Justice of 7 September 2004, *Waddenvereniging and Vogelbeschermingsvereniging*, C-127/02, EU:C:2004:482 and of 11 April 2013, *Sweetman and Others*, C-258/11, EU:C:2013:220.
48. AI Act Prohibition guidelines, Paragraph 92.

2.2.2. Role of equality bodies and other NHRS in addressing AI systems that manipulate, deceive or exploit vulnerabilities of people

- Raise awareness of this prohibition and emphasise the harm to the person as opposed to the consumer, as the rights of the person extend beyond being a consumer, while the Commission guidelines specifically reference the "average consumer" for this prohibition (see Section 2.2 above). This can be done in the public communications of equality bodies and NHRS and in their communication with market surveillance authorities.
- Proactively ensure the "significance" of the harm takes into account fundamental rights, and especially equality and non-discrimination. EBs could assess the "significance" of the harm based on existing case laws on non-discrimination. The threshold of harm that is significant enough for the prohibition to apply would need to be assessed.
  - It will be important for EBs to collect examples. Civil Society Organisations (CSOs) can be helpful allies with this. In addition, EBs need to track private litigation.
- Ensure "exploitation" of vulnerabilities takes into account fundamental rights, and in particular equality and discrimination, by drafting guidance and providing it to the market surveillance authorities who will be in charge of assessing harms. One particular point of attention will be whether this criterion could include indirect discrimination.

2.3. Social scoring

2.3.1. Context and relevance

Article 5 (1) (c) of the AI Act prohibits unacceptable AI-enabled social scoring of people by public and private actors as this could result in "discriminatory outcomes and the exclusion of certain groups"[49] violating the right to dignity and non-discrimination.

Examples of social scoring systems

This prohibition is particularly relevant for the public sector, where classification and evaluation are widespread, including in employment and social security, fiscal matters, migration, law enforcement or justice. Classification and evaluation systems are also used in insurance and banking, such as the Schufa system used in Germany to attribute a credit score to individuals.[50]

49. AI Act, Recital 31.
50. AlgorithmWatch (2018), "SCHUFA, a black box: OpenSCHUFA results published", available at https://algorithmwatch.org/en/schufa-a-black-box-openschufa-results-published/ and C-634/21 SCHUFA Holding (Scoring) EU:C:2023:957.

For instance, the Austrian employment agency developed an algorithm, to predict chances of employment, in order to allocate support resources to job seekers. The prototype was shown to be discriminatory against women (in particular single mothers) and job seekers with a migration background.[51] In the Netherlands, a system used to predict fraud was found to have discriminated against recipients on grounds of race,[52] ethnic origin and citizenship.[53] In Poland, a system used by the employment agency was eventually abandoned because it was deemed unconstitutional.[54] ADM and AI systems are or were also used to control welfare beneficiaries in multiple countries (e.g. France,[55] the Netherlands,[56] Denmark,[57] Belgium[58]), with discriminatory outcomes and overcontrol of people in vulnerable situations. Such systems are usually built on a combination of personal and personality characteristics, data about the interactions between beneficiaries and public employment agencies and, sometimes, data from private companies (such as electricity companies).

Classification and evaluation systems can also be based on other types of data. For instance, a partly automated surveillance system in a refugee camp could be analysing data from cameras and motion sensors, to ascertain whether specific individuals (such as migrants) are at risk of trying to leave.[59]

Assessing prohibitions under Art. 5 (1) (c)

Assessing whether an AI system fits into Art 5 (1) (c) requires a five-step assessment fulfilling all of the following steps:

1. Has the AI system been placed in the market, put into service, or is it being used?

51. Allhutter D. et al. (2020), "Algorithmic profiling of job seekers in Austria: How austerity politics are made effective", *Frontiers in Big Data*, 3, available at https://doi.org/10.3389/fdata.2020.00005, accessed 11 November 2025.
52 Since all human beings belong to the same species, the Committee of Ministers of the Council of Europe rejects theories based on the existence of different "races". However, in this document, the term "race" is used in order to ensure that those persons who are generally and erroneously perceived as "belonging to another race" are not excluded from the protection provided for by the legislation and the implementation of policies.
53. De Rechtspraak (2019), "SyRI legislation in breach of European Convention on Human Rights", *De Rechtspraak*, available at www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Den-Haag/Nieuws/Paginas/SyRI-legislation-in-breach-of-European-Convention-on-Human-Rights.aspx, accessed 11 November 2025. The SyRI system was also deemed to have disproportionately interfered with end users' right to privacy because it processed personal data from various government agencies.
54. Szymielewicz K. et al. (2015), "Profiling the unemployed in Poland: social and political implications of algorithmic decision making", Fundacja Panoptykon, available at https://en.panoptykon.org/profiling-unemployed-poland-report, accessed 11 November 2025.
55. Romain et al. (2023).
56. Mehrotra D. et al. (2023), "Inside the suspicion machine", *WIRED*, available at www.wired.com/story/welfare-state-algorithms/.
57. Geiger G. (2023), "How Denmark's welfare state became a surveillance nightmare", *WIRED*, available at www.wired.com/story/algorithms-welfare-state-politics/ and Amnesty International (2024), "Denmark: AI-powered welfare system fuels mass surveillance and risks discriminating against marginalized groups – report", available at www.amnesty.org/en/latest/news/2024/11/denmark-ai-powered-welfare-system-fuels-mass-surveillance-and-risks-discriminating-against-marginalized-groups-report/.
58. Degrave E. (2020), "The use of secret algorithms to combat social fraud in Belgium", *European Review of Digital Administration & Law* 1-2: 167-78.
59. Example given in AI Act Prohibition guidelines, paragraph 155.

2. Is "the evaluation or classification of natural persons or groups of persons" the intended purpose or the use of this AI system?
3. Has the evaluation or classification taken place "over a certain period of time"?
   a. One-time grading is not prohibited; however, the prohibition would apply if the data that are analysed one-time span a period of time.[60]
4. Is the evaluation or classification based on
   a. social behaviour of natural persons or groups of persons or
   b. "known, inferred or predicted personal or personality characteristics"?[61]
5. Does the evaluation or classification result in a social score leading to "detrimental or unfavourable treatment of certain natural persons or groups of persons" in:
   a. "social contexts that are unrelated to the contexts in which the data was originally generated or collected"; and/or
   b. an unjustified or disproportionate manner to their social behaviour or its gravity?[62]

Classification is broader than evaluation, and can be "based on known characteristics such as their age, sex, and height [that] does not necessarily lead to profiling".[63] Evaluation is more closely related to "profiling", which means[64]

> gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to analyse and/or make predictions about, for example, their:
> - ability to perform a task;
> - interests; or
> - likely behaviour.

For example, the credit scoring system used in Germany, Schufa, that generates a "probability score" to estimate a person's ability to make payments has been ruled as "profiling" by the Court of Justice of the European Union (CJEU).[65]

60. AI Act Prohibition guidelines, paragraph 155. The paragraph builds on the example of a system used in a refugee camp, where the analysed data span a period of time.
61. AI Act Prohibition guidelines, paragraph 158: "'Personal characteristics' may include a variety of information relating to a person, for example sex, sexual orientation or sexual characteristics, gender, gender identity, race, ethnicity, family situation, address, income, household members, profession, employment or other legal status, performance at work, economic situation, financial liquidity, health, personal preferences, interests, reliability, behaviour, location or movement, level of debt, type of car etc."
62. The Childcare Benefits scandal in the Netherlands is an example where both the conditions in Art. 5 (1) (c) of the AI Act are satisfied. See de Nationale ombudsman, "Belastingdienst treft 232 gezinnen met onevenredig harde actie", 27 November 2019 [in Dutch]. See also ibid."Geen powerplay maar fair play. Onevenredig harde aanpak van 232 gezinnen met kinderopvangtoeslag", 9 August 2017, p. 32.
63. Article 29 Working Party, Guidelines on Automated individual decision making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, 6.2.2018, p. 7. Also see GDPR, Art. 4 (4).
64. Ibid.
65. Judgment of the Court of Justice of 7 December 2023, SCHUFA Holding (Scoring), C-634/21, EU:C:2023:957, paragraph 47.

A scoring practice can result in unfavourable treatment even if no specific harm is caused, for example singling out an individual for additional inspections, while detrimental treatment results in a harm. Both unfavourable and detrimental treatment may already be prohibited under EU non-discrimination law that protects certain protected groups based, for example, on age, ethnic and racial origin, sex and religion. But the scope of the prohibition in the AI Act is broader and applies to treatment beyond EU non-discrimination law.[66]

If the score results in "detrimental or unfavourable treatment" then this prohibition applies even if the score is produced by an organisation (a private creditworthiness company) other than the organisation (public authority) using it.[67] This prohibition is also not limited to the evaluation or classification performed solely by an AI system. The scope of the prohibition includes scoring practices that may involve human assessments as long as the output from the AI system plays "a sufficiently important role in producing the social score".[68] For example, a public authority using an AI system for scoring and combining that score with human assessment of additional facts would be prohibited if the result is detrimental or unfavourable treatment.

2.3.2. Role of equality bodies and NHRS in addressing prohibitions related to social scoring

- Monitor and assess the range of scoring practices going beyond EU non-discrimination law that result in unfavourable and detrimental treatment. EBs will need to develop additional expertise to effectively monitor them.

2.4. Risk assessment of committing a criminal offence

2.4.1. Context and relevance

Article 5 (1) (d) of the AI Act prohibits individual criminal offence risk assessment and prediction "based solely on the profiling of a natural person or on assessing their personality traits and characteristics."[69] This prohibition attempts to limit the harms to the right to human dignity, non-discrimination, the right to fair trial, the right to be presumed innocent, the right to defence, effective remedy, privacy and data protection.[70]

Assessing whether an AI system fits into Art 5 (1) (d) requires a three-step assessment fulfilling all of the following steps:

1. Has the AI system been placed in the market, put into service, or is it being used?

66. AI Act Prohibition guidelines, paragraph 165.
67. Judgment of the Court of Justice of 7 December 2023, *SCHUFA Holding (Scoring)*, C-634/21, EU:C:2023:957, paragraphs 42-51, 60-61.
68. AI Act Prohibition guidelines, paragraph 161.
69. AI Act, Art. 5 (1) (d).
70. AI Act, Recital 48.

2. Is the intended purpose of the AI system "making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence"?

3. Is the assessment or prediction based solely on

   a. profiling,[71] and/or

   b. assessing their personality traits and characteristics such as nationality, place of birth, place of residence, number of children, level of debt, type of car, etc.[72]

For instance, an AI system used by a law enforcement authority to predict criminal behaviour for crimes such as terrorism solely based on individuals' age, nationality, address, type of car and marital status, would be prohibited.[73]

Examples that are not prohibited include:

- Risk assessment of a group (instead of an individual);[74]
- Any other predictive policing approaches that are not solely based on profiling or assessing personality traits and characteristics;
- AI systems used to support human assessment based on objective and verifiable facts directly linked to a criminal activity;[75]
- Location based predictive policing;[76]
- AI systems making individual predictions that are allowed under national and EU law related to an administrative offence (and not a criminal offence), even if "information might be gathered for possible involvement of the natural persons in criminal offences".[77]

This prohibition is limited in scope, and is not a prohibition of predictive policing in its entirety. When the prohibition does apply, it is broader in terms of when and to whom it applies. The AI Act complements the Directive (EU) 2016/343 to protect the right to be presumed innocent until proven guilty before a formal criminal

71. Profiling that results in indirect or direct discrimination is already prohibited under LED, Art. 11 (3). See also Article 29 Working Party, Guidelines on Automated individual decision making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, 6.2.2018, p. 7; EU Fundamental Rights Agency, *Preventing unlawful profiling today and in the future: a guide*, Handbook, 2018, p. 138.
72. AI Act, Recital 42.
73. AI Act Prohibition guidelines, Paragraph 202.
74. AI Act Prohibition guidelines, Paragraph 196. Note that if a group profile is used to assess and predict the risk of a specific individual committing a similar offence this constitutes profiling and may therefore fall within the prohibition.
75. AI Act Prohibition guidelines, Paragraph 214.
76. AI Act Prohibition guidelines, Paragraphs 212-13. This means that patrols could be heavily deployed in areas decided by predictive algorithms "based on historical data and perpetuate discrimination and inequities in law enforcement". See also "Cop out: automation in the criminal legal system", Georgetown Law Centre on Privacy & Technology, available at: https://copout.tech/, accessed 10 November 2025.
77. AI Act Prohibition guidelines, paragraph 217. See also Footnote 143 in the AI Act Prohibition guidelines on the criteria to assess whether an offence is criminal or not.

investigation is launched.[78] Directive (EU) 2016/343 applies only when a person is suspected or accused of having committed a criminal offence.

It is important to note that this prohibition is not limited to law enforcement authorities, or entities acting on their behalf. Any entity that has a legal obligation to "assess or predict the risk of a natural person committing a criminal offence" is within scope. A tax authority that builds profiles of individuals based on nationality or other characteristics using AI systems is within the scope of this prohibition.[79] A banking institution, a private entity, that is entrusted by law to screen customers for a criminal offence such as money laundering would also be within the scope of this prohibition if it uses AI systems and does not comply with Regulation (EU) 2024/1624.[80]

It is also important to highlight that application of "group profiling"[81] to individuals is within the scope of this prohibition. Group profiling involves building a profile of a specific group, which can involve categories such as terrorists, gangsters etc. Such profiles may be used to assess and predict the risk of other persons committing similar crimes. This is prohibited.

2.4.2. Role of equality bodies and NHRS in addressing prohibitions related to risk assessment of committing a criminal offence

- Explore the full range of the prohibition, by conducting or commissioning studies on applications within the scope of this prohibition that are beyond law enforcement use of risk assessment for individual crime prevention (e.g. tax authorities or institutions in charge of money laundering).
- Contribute to the enforcement of the prohibition by training and sensitising the relevant competent authorities for those applications, who may not be a competent authority under the AI Act, to address the discrimination harms.

2.5. Scraping to build or expand facial recognition databases

2.5.1. Context and relevance

Article 5 (1) (e) of the AI Act prohibits providers and deployers from developing and expanding "facial recognition databases through the untargeted scraping of facial images from the internet or closed-circuit television (CCTV)[82] and harms the right to

78. Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings.
79. The prohibition does not apply when a tax authority is assessing the risk of a legal entity such as a company.
80. Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Article 20 and 76 (5) (b).
81. EU Fundamental Rights Agency (2018), *Preventing unlawful profiling today and in the future: a guide*, Handbook, p. 21.
82. AI Act, Recital 43.

human dignity, non-discrimination, privacy and data protection[83]. The prohibition applies regardless of the storage structure of the database. A facial recognition database does not need to be centralised in one location or under the control of only one legal entity. It can be decentralised. The prohibition also applies if the database is temporary or for a brief moment in time.

Untargeted scraping of facial images, however, is already unlawful under EU data protection law.[84] Enforcement, especially extraterritorial, has been the problem. For example, the facial recognition application commercialised by United States company Clearview AI, which relied on untargeted scraping of facial images on social media, was said to be used by several law enforcement authorities throughout Europe.[85]

Assessing whether an AI system fits into Art. 5 (1) (e) requires a four-step assessment fulfilling all of the following steps:

1. Has the AI system been placed in the market, put into service, or is it being used?
2. Does this AI system perform "untargeted scraping" (see below)?
3. Are "facial images" sourced from the "internet or CCTV footage"?
4. Is the AI system used to "create or expand facial recognition databases"?

The AI Act does not prohibit all scraping. Neither does it prohibit building of databases of data other than facial images. Such activities, especially those involving biometric data,[86] are already restricted under EU data protection law.[87]

Whether a company crawling a website respects technical opt-out mechanisms[88] does not affect the question whether the scraping is untargeted or not. Targeted scraping of "images or video containing human faces only of specific individuals or a predefined group of persons" is not prohibited.[89] However, if such targeted scraping is performed for multiple individuals or groups over a span of time, then such scraping would be equivalent to untargeted scraping, and thereby prohibited.[90]

---

83. AI Act Prohibition guidelines, Paragraph 226.
84. De Autoriteit Persoonsgegevens (2024), "Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition", available at www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition, accessed 10 November 2025.
85. European Data Protection Board (10 June 2020), Letter to Members of the European Parliament, available at www.edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf, accessed 10 November 2025.
86. Note that the definition of "biometric data" in the AI Act differs from the GDPR, and the LED. AI Act, Art. 3 (34) defines "biometric data" as :
"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". GDPR, Art. 4 (14) and LED, Art. 3 (13) define "biometric data" as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;"
87. EDPB (2024), Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 December 2024, paragraphs 104-106.
88. Koster M. et al. (2022), "Robots Exclusion Protocol", RFC 9309, DOI 10.17487/RFC9309, available at www.rfc-editor.org/info/rfc9309, accessed 10 November 2025.
89. AI Act Prohibition guidelines, paragraph 229.
90. AI Act Prohibition guidelines, paragraph 230.

Furthermore, publicly available data, even if a person has published their facial image on a social media website, is protected under EU data protection law. "[T]he mere fact that personal data is publicly accessible does not imply that 'the data subject has manifestly made such data public'."[91]

2.5.2. Role of equality bodies and NHRS in addressing prohibitions related to scraping to build or expand facial recognition databases

- Support the enforcement of this prohibition, especially against companies which are based outside the EU but scrape facial images of people in the EU, via continuous engagement with MSAs and Data Protection Authorities (DPAs).

2.6. Emotion recognition

2.6.1. Context and relevance

Despite the "highly undesired discriminatory and dignity consequences, manipulative effects"[92] and the lack of scientific evidence that emotion recognition[93] works,[94] Article 5 (1) (f) of the AI Act only prohibits emotion recognition in workplaces and educational institutions. All other uses of emotion recognition are treated as high-risk,[95] but are not prohibited.

Examples

Emotion recognition comprehends "different technologies and processing operations to detect, collect, analyse, categorise, react, interact and learn emotions from persons."[96] Such technologies can be used in employment during the recruitment process or to monitor the emotions of employees, in healthcare, for suicide prevention, or by law enforcement as "lie detectors" at border control.[97]

91. EDPB (2024), "Report of the work undertaken by the ChatGPT Taskforce", adopted on 23 May 2024, paragraph 18.
92. Codagnone C. et al. (2022), *Identification and assessment of existing and draft EU legislation in the digital field*, Study for the special committee on Artificial Intelligence in a Digital Age (AIDA), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, p. 62.
93. AI Act, Art. 3 (39): "'emotion recognition system' means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data."
94. Barrett L. F. et al. (2019), "Emotional expressions reconsidered: challenges to inferring emotion from human facial movements", *Psychological Science in the Public Interest*, 20(1), 1-68, available at https://doi.org/10.1177/1529100619832930, accessed 10 November 2025.
95. AI Act, Annex III (1) (c).
96. AI Act Prohibitions Guidelines, paragraph 240.
97. Boffey D. (2018), "EU border 'lie detector' system criticised as pseudoscience", *The Guardian*, available at www.theguardian.com/world/2018/nov/02/eu-border-lie-detection-system-criticised-as-pseudoscience, accessed 10 November 2025.

Assessing whether an AI system fits into Art. 5 (1) (f) requires a three-step assessment fulfilling all of the following steps:

1. Has the AI system been placed in the market, put into service, or is it being used?
2. Does the AI system identify or infer emotions or is it capable of inferring emotions or intentions of persons based on biometric data?
3. Is the AI system deployed in "workplace and education institutions"?

It is important to note that the notion of emotion recognition is restricted in the AI Act:

> The notion refers to emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement. It *does not include physical states*, such as pain or fatigue, including, for example, systems used in detecting the state of fatigue of professional pilots or drivers for the purpose of preventing accidents. This *also does not include the mere detection of readily apparent expressions, gestures or movements, unless* they are used for identifying or inferring emotions. Those expressions can be basic facial expressions, such as a frown or a smile, or gestures such as the movement of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whispering.[98]

The above paragraph does not mean that these are lawful practices. Emotion recognition involves processing biometric data, which without a valid legal basis would be unlawful under EU data protection law.[99]

While the notion of a workplace includes the recruitment process and protects employees as well as self-employed people, according to the European Commission's guidelines, it does not include other people. For example, "[u]sing webcams and voice recognition systems by the call centre to track their customers' emotions, such as anger or impatience, is not prohibited" and "by a supermarket … to track its employees' emotions" is prohibited but that of customers is not.[100]

The notion of educational institutions applies to all levels of education institution, public or private "accredited or sanctioned by the relevant national education authorities or equivalent authorities". The use of emotion recognition at educational institutions, including during admission process and tests is included; but the prohibition does not apply to courses, including online, that are offered by entities that are not considered an educational institution.[101]

Even in workplaces and educational institutions, emotion recognition is allowed for medical or safety reasons if it is strictly necessary and proportionate. Emotion recognition systems used for medical reasons would have to comply with Regulation (EU) 2017/745 (Medical Device Regulation), Union and national law on employment and working conditions, including health and safety at work, which may restrict their use. In other words, a Conformité Européenne (CE) marking[102] for an emotion recognition

98. AI Act, Recital 18 *(emphasis added)*.
99. GDPR, Art. 6 (lawfulness of processing) and 9 (special categories of data) in particular.
100. AI Act Prohibition guidelines, paragraph 254.
101. AI Act Prohibition guidelines, paragraph 257.
102. European Commission (n.d.), *CE Marking*, available at https://single-market-economy.ec.europa.eu/single-market/ce-marking_en, accessed 10 November 2025.

system under the Medical Device Regulation is necessary but not sufficient for the use of that system in workplaces and educational institutions under the AI Act.

Furthermore, any such use requires a "prior written and motivated expert opinion relating to the specific use case … [whose] necessity should be assessed on an objective basis in relation to the medical and safety purpose, and not refer to the employer's or educational institution's 'needs'. This assessment should inquire whether less intrusive alternative means exist which would achieve the same purpose."[103]

Non-prohibited emotion recognition systems are regulated as high-risk under Annex III (1) (c). Examples could include,[104] if and only if there is a valid legal basis,

- Statistics authorities using emotion recognition in voting booths to find out about people's attitude towards democracy (e.g. anger, satisfaction)
- A company using a chatbot that uses emotion recognition to react appropriately to very dissatisfied customers;
- A law enforcement authority using an emotion recognition system during interrogation of a suspect.

Note in all cases this refers to using biometric data to infer or identify emotion.

2.6.2. Role of equality bodies and NHRS in addressing prohibitions related to emotion recognition

- Gather evidence of discrimination harms and risks due to emotion recognition in areas other than workplaces and educational institutions. In particular, equality bodies and NHRS can monitor the emotion recognition systems considered high-risk under Annex III (1) (c) of the AI Act that will be registered in the database of high-risk AI systems (see Article 49).
- Gather evidence of the reasons given by AI operators to argue that the use of emotion recognition for medical and safety reasons is necessary and proportionate to ensure conformity with the law.
- Protect customers, clients and other people interacting with the people at their workplace as this is not prohibited by 5 (1) (f).

2.7. Biometric categorisation

2.7.1. Context and relevance

Article 5 (1) (g) of the AI Act prohibits categorising natural persons *individually* "based on their biometric data to deduce or infer their race, political opinions, trade union

103. AI Act Prohibition guidelines, paragraph 259.
104. Wendehorst C. and Duller. Y (2021), *Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces*, Study for the European Parliament's Committee on Legal Affairs and Petitions Committee, European Parliament, p. 66.

membership, religious or philosophical beliefs, sex life or sexual orientation"[105] as such categorisation harms the right to human dignity, non-discrimination, privacy and data protection. Note that biometric categorisation as explained below is different from (remote) biometric identification where persons are identified (see 2.8).

In contrast to the term "biometric categorisation system" the term "biometric categorisation" is not defined in the AI Act but can be understood as

> the process of establishing whether the biometric data of an individual belongs to a group with some predefined characteristic in order to take a specific action. In this case, *it is not important to identify or verify the individual* but to assign him/her automatically to a certain category. For instance an advertising display may show different adverts depending on the individual that is looking at it based on the age or gender.[106] *[emphasis added]*

Examples

Other examples of biometric categorisation include the use of software to automatically categorise people by a race or a gender, or an AI system that analyses a person's social media pictures to assume their political orientation and send them targeted messages, or to assume their sexual orientation to send them targeted advertising.

Biometric categorisation is a form of profiling.[107] Article 22 (1) of the GDPR and Article 11 (3) of Law Enforcement Directive (LED) already prohibit indirect or direct discrimination based on profiling.

Assessing whether an AI system fits into Article 5 (1) (g) requires a five-step assessment of the following:

1. Has the AI system been placed in the market, put into service, or is it being used?
2. Is the AI system based on "biometric data"?
3. Is the AI system a "biometric categorisation system" as defined in Art. 3 (40)?
4. Are individuals categorised through this "biometric categorisation system"?
   a. Is the primary purpose of the AI system "assigning natural persons to specific categories on the basis of their biometric data"?
5. Is the AI system used to "deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation"?

105. AI Act, Art. 5 (1) (g).
106. Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, 27 April 2012, p. 6.
107. Article 29 Working Party, Guidelines on Automated individual decision making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, 6.2.2018, p. 7. Also see GDPR, Art. 4 (4).

Out of scope of the prohibition, but considered high-risk under Annex III (1) (b), are:

- "[L]abelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorising of biometric data in the area of law enforcement."[108]
- Biometric categorisation that is "ancillary to another commercial service and strictly necessary for objective technical reasons."[109]

Note that such uses may still be prohibited under the GDPR and LED if either the purpose of the processing is not lawful or the interference to the fundamental rights of people due to the processing of biometric data is not necessary and proportional.

2.7.2. Role of equality bodies and NHRS in addressing prohibitions related to biometric categorisation

- Accumulate evidence of discrimination harms due to biometric categorisation and share with MSAs and the European Commission to contribute to the yearly assessment of Article 5 and Annex III, according to Article 112, via concrete examples. In particular, equality bodies and NHRS can collaborate with civil society organisations and market surveillance authorities to pay particular attention to high-risk uses in the area of law enforcement, which will be recorded in the non-public version of the database of high-risk AI systems (see Article 49).

2.8. Remote biometric identification

2.8.1. Context and relevance

The AI Act addresses remote biometric identification (RBI) systems[110] through a combination of articles. Under Annex III (1) (a), all RBI systems[111] that are allowed under national or Union law are considered high-risk AI systems. As RBI systems process biometric data, which "under all circumstances constitutes a serious interference [with the rights guaranteed in the EU Charter]",[112] a legal basis is required to allow such an interference. Facial recognition and voice recognition technologies are two common examples of RBI systems. The use of biometric identification for purposes other than law enforcement is already generally prohibited.[113]

108. AI Act, Art. 5 (1) (g).
109. AI Act, Art. 3 (40).
110. AI Act, Art. 3 (41): "'remote biometric identification system' means an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database". See also AI Act, Art. 3 (35) and AI Act Prohibition guidelines, paragraph 306.
111. Such systems could include remote facial recognition systems, remote voice recognition systems, gait recognition systems, etc.
112. EDPB (2022), Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, p. 5.
113. AI Act, Recital 39. See also GDPR, Art. 9 (1) and EUDPR, Art. 10 (1).

For law enforcement purposes a "mere transposition into domestic law of the general clause in Article 10 LED"[114] is not sufficient to establish a legal basis. The AI Act does not provide a legal basis for such interference either.[115] Thus, processing of biometric data, including through RBI systems for law enforcement, is prohibited in EU countries unless a specific legal basis has been established. At least two countries, the Netherlands[116] and Italy[117] have not yet established such a legal basis.

Real-time RBI systems

The AI Act makes the distinction between real-time RBI systems and post RBI systems.[118] The latter is defined as any RBI system that is not real-time. The use of real-time RBI systems can "evoke a feeling of constant surveillance and *indirectly dissuade the exercise of the freedom of assembly and other fundamental rights*" and can result in discrimination with regard to age, ethnicity, race, sex or disabilities.[119]

To address this concern, Article 5 (1) (h) prohibits real-time RBI in publicly accessible spaces for law enforcement *purposes*. This means that the prohibition applies not only when law enforcement authorities[120] use real-time RBI; it also applies if any other entity such as a public transport company or a sports club uses it for law enforcement purposes, as will be the case if a law enforcement authority delegated the deployment to them.[121] With regard to this prohibition, the AI Act applies as *lex specialis* to Article 10 LED.[122]

Assessing whether an AI system fits into Art. 5 (1) (h) requires a five-step assessment fulfilling all of the following steps:

1. Is the AI system an RBI system according to Article 3 (41)?
2. Is the RBI system being used?
   - this implies that the prohibition only applies to deployers (and not providers as in the case of other prohibitions)

114. EDPB (2022), Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, p. 5.
115. AI Act, Recital 38.
116. Galič M. and Stevens L. (2023), "Regulating police use of facial recognition technology in the Netherlands: The complex interplay between criminal procedural law and data protection law", *New Journal of European Criminal Law* 14(4), 459-78, available at https://doi.org/10.1177/20322844231212834, accessed 10 November 2025.
117. "Garante per la protezione dei dati personali" (2021), *Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy*, available at www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575842, accessed 10 November 2025.
118. AI Act, Art. 3 (42) and (43). Art. 3 (42) states "'real-time remote biometric identification system' means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay, comprising not only instant identification, but also limited short delays in order to avoid circumvention".
119. AI Act, Recital 32. *(emphasis added)*
120. AI Act, Art. 3 (45).
121. AI Act, Art. 3 (46): "law enforcement" means activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security;
122. AI Act, Recital 38.

3. Is the RBI system being used in "publicly accessible spaces"?
4. Is the RBI system "real-time"?
5. Is the real-time RBI system being used for law enforcement purposes?

This prohibition, however, is *not* absolute. The use of real-time RBI systems for law enforcement purposes *could* be allowed if it is strictly necessary for the following cases:

1. the targeted search for victims of three specific serious crimes[123] and missing persons;
2. the prevention of imminent threats to life or physical safety or a genuine threat of terrorist attacks; and/or
3. localisation or identification of suspects and offenders of certain criminal offences.[124]

The AI Act does not provide the legal basis for such use. In these exceptional cases, real-time RBI for law enforcement purposes can be used only if

- A national law is adopted that provides a legal basis for real-time RBI and authorises one or more of the three cases;
- A fundamental rights impact assessment (FRIA) according to Article 27 to assess necessity and proportionality has been performed by the law enforcement authority (LEA);[125]
- For each use, if an LEA (or an entity on their behalf) wants to use real-time RBI, the LEA needs to:[126]
  - get an authorisation from a judicial or an independent administrative authority whose decision is binding in the specific EU country (except in the case of emergency when post-hoc approval is required);
  - notify the market surveillance authority (MSA) and the data protection authority (DPA);
  - add the use information to the non-public EU database according to Article 49 (4).
- DPA and MSA should submit an annual report to the European Commission noting the frequency, etc. of the use of real-time RBI in their country. They can choose to send a joint report.[127]
- Based on the reports from DPAs and MSAs of EU countries, the European Commission should publish annual reports.[128]

123. The three serious crimes are abduction, trafficking in human beings and sexual exploitation of human beings.
124. AI Act, Art. (5) (1) (h) (iii): The criminal offences are within scope if they satisfy both conditions: (1) they are listed in AI Act, Annex II, and (2) they are "punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years."
125. AI Act, Art. 5 (2).
126. AI Act, Art. 5 (2)-(5).
127. AI Act, Art. 5 (6).
128. AI Act, Art. 5 (7).

If a national law is established to provide a legal basis, then the rules for high-risk AI systems will apply to such use for law enforcement purposes.

If a national law does not establish a legal basis for the use of real-time RBI, which first requires a legal basis for processing biometric data, then there is a blanket prohibition, effective from 2 February 2025, on the use of real-time RBI in public spaces for law enforcement purposes. Member states do not have a deadline to adopt such a national law. As of the date of this report, no EU country has adopted any such national law. EU countries can support blanket prohibition by not adopting a national law in this regard.

In summary, real-time RBI systems are prohibited unless they are allowed for law enforcement purposes through a national law that allows their use for specific objectives, with checks on their proportionality and necessity because such use interferes with a range of fundamental rights including non-discrimination.

Key case in the European Court of Human Rights:
***Glukhin v. Russia* – Application No. 11519/20 (2023)**

During routine monitoring of the internet the police discovered photographs and a video of the applicant holding a solo demonstration in the Moscow underground published on a public Telegram channel. According to the applicant, the police used facial recognition technology to identify him from screenshots of the channel, collected video-recordings from CCTV surveillance cameras installed in stations of the Moscow underground through which he had transited and, several days later, used live facial technology to locate and arrest him while he was travelling in the underground.

The various screenshots were used in evidence in administrative-offence proceedings against the applicant, who was convicted.

The European Court of Human Rights found a violation of articles 10 and 8.

The use of facial recognition technology in administrative proceedings in order to identify, locate and arrest a peaceful protestor was capable of having a chilling effect on rights to freedom of expression and assembly (Article 10). In implementing facial recognition technology there is a need for:

- detailed rules governing the scope and application of measures,
- strong safeguards against the risk of abuse and arbitrariness.

The Court held that this increased when live facial recognition technology was used and while not ruling out the use of such technology at all, the Court found that in Glukhin's case the use of the technology to find, locate and arrest him did not correspond to a "pressing social need" and could not be regarded as "necessary in a democratic society".

Court factsheet on cases on new technologies

Post RBI systems

RBI systems that are not prohibited, either in the AI Act or any other national or Union law, are considered high-risk. By definition, these include all post RBI systems (in addition to the allowed real-time RBI systems) that are allowed under national or Union law.

All the rules for high-risk AI systems apply to these post RBI systems. Law enforcement use of post RBI systems includes an *additional obligation* for the deployers.

The deployers of post RBI systems "for the targeted search of [i.e. to locate] a person suspected or convicted of having committed a criminal offence"[129] are required to obtain authorisation from a judicial or an independent administrative authority whose decision is binding in the specific EU country. Such authorisation should be obtained before each use of the system, at the very least 48 hours before. Each such use should "be limited to what is strictly necessary for the investigation of a specific criminal offence."[130]

2.8.2. Role of equality bodies and other NHRS in addressing prohibitions related to remote biometric identification

- Encourage governments to maintain blanket prohibition on the use of real-time RBI systems for law enforcement purposes.

129. AI Act, Art. 26 (10).
130. AI Act, Art. 26 (10).



3. High-risk AI systems

3.1. Classification of high-risk AI systems

3.1.1. Context and relevance

Article 6 lays down the rules to classify high-risk AI systems that are within the scope of the AI Act. Of particular relevance to EBs are the applications listed in Annex III, which cover:

- biometrics;[131]
- critical infrastructure (digital infrastructure, road traffic, supply of water, gas, electricity);[132]
- education and vocational training;[133]
- employment, workers' management and access to self-employment;[134]

131. AI Act, Annex III (1) and Recital 54.
132. AI Act, Annex III (2) and Recital 55.
133. AI Act, Annex III (3) and Recital 56.
134. AI Act, Annex III (4) and Recital 57.

- access to and enjoyment of essential private services and essential public services and benefits (e.g. social security, credit scoring, insurance, health care, emergency services);[135]
- law enforcement;[136]
- migration, asylum and border control management;[137]
- administration of justice and democratic processes.[138]

The Recitals in the AI Act pertaining to these areas stress that the notion of risk is not limited to technological characteristics but is closely tied to the societal context and warn of the potential for reinforcing structural inequalities.

Compared to other AI systems, high-risk AI systems are subjected to more documentation, quality assurance and transparency obligations, which are all safeguards against discrimination.

However, providers of AI systems in these areas can opt out of being considered high-risk if they consider that their specific case does not pose a "significant risk" (see below). In doing so, providers choosing to opt out of the regime will not have to comply with high-risk obligations.

Opting out is based on self-assessment by providers, who are not obliged to publish this assessment (see below). This poses the risk that certain unregulated high-risk AI systems will be wrongly deployed as non-high-risk.

The rules on high-risk AI systems for AI systems pertaining to areas listed in Annex III will enter into force in August 2026. The AI Office is expected to produce guidelines for the classification of AI systems as high-risk by 2 February 2026.[139] The guidelines should include "practical examples of use-cases of AI systems that are high-risk and not high-risk."[140] As per Article 6 (6)-(8) on classification rules for high-risk AI systems, delegated acts can add, delete or modify the conditions of Article 6 (3), but "shall not decrease the overall level of protection of health, safety and fundamental rights".[141]

Significant risk and opt-out conditions

Although the term "significant risk" is not defined in the AI Act, it can be interpreted as adversely impacting fundamental rights including "right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, the right to non-discrimination, the right to education, consumer protection, workers" rights, the rights of persons with disabilities, *gender equality*, intellectual property rights, the right to an effective remedy and to a fair trial, the right of defence and the presumption of innocence, and the right to good administration,"[142] the rights of children and the right to a high

135. AI Act, Annex III (5) and Recital 58.
136. AI Act, Annex III (6) and Recital 59.
137. AI Act, Annex III (7) and Recital 60.
138. AI Act, Annex III (8) and Recital 61.
139. AI Act, Art. 6 (5).
140. Ibid.
141. AI Act, Art. 6 (8).
142. AI Act, Recital 48. *(emphasis added)*

level of environmental protection.[143] The assessment may consider the severity of the harm and the probability of the occurrence.

In particular, "significant risk" needs to be assessed when considering the four conditions, any one of which the providers of AI systems could rely on to opt out:[144]

a. the AI system is intended to perform a narrow procedural task (for example, an AI system that classifies incoming documents into categories);

b. the AI system is intended to improve the result of a previously completed human activity (for example, an AI system intended to improve the language used in previously drafted documents);

c. the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review (for example, an AI system that "given a certain grading pattern of a teacher, can be used to check ex post whether the teacher may have deviated from the grading pattern so as to flag potential inconsistencies or anomalies"); or

d. the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use-cases listed in Annex III (for example, AI systems used for translation of initial documents).

"Profiling"[145] as defined in EU data protection law is already considered a "significant risk". AI systems falling under Annex III and performing profiling are always considered high-risk.[146]

Consequences of opting out of the high-risk AI system regime

1. If providers of AI systems self-choose to opt out, they are obliged to:
   - document their assessment to opt out before placing the AI system on the market or putting it into service;
   - register their system in the EU database based on Article 49 (2) and Article 71 with the information required by Annex VIII Section B. The information required is less detailed than that required by Annex VIII Section A (in accordance with Article 49(1)) for systems considered high-risk. However, the information includes the "condition or conditions under Article 6 (3) based on which the AI system is considered to be not-high-risk";[147]
2. Providers of AI systems are not required to publish their self-assessment. However, they are requested to provide the documentation of the assessment upon request from the national competent authorities.[148]

143. EU Charter, Art. 37.
144. AI Act, Art. 6 (3) and Recital 53. These conditions do not prevent an AI system being prohibited.
145. GDPR, Art. 4(4) and Law Enforcement Directive, Art. 3 (4).
146. AI Act, Art. 6 (3) third subparagraph.
147. Annex VIII, Section B (6).
148. AI Act, Art. 6 (4). Equality bodies are not considered national competent authorities under Article 6(4) of the AI Act. However, equality bodies have the possibility to access the same information with the powers under AI Act, Art. 77. Furthermore, Standards Directives Art. 8 gives them investigative powers and a right of access to information to fulfil their mandate.

3. MSAs may carry out evaluation of the AI systems to assess whether the AI systems are high-risk, and require the provider to take corrective actions.[149] The MSA can fine the provider for misclassifying the AI system as non-high-risk to circumvent the AI Act.[150] (See Article 77.)

Issues with de-risking practices

The combination of self-assessment for opting out, the lack of definition of the term "significant risk" and the opting-out conditions laid out in Article 6(3) pose the risk that providers will engage in "de-risking practices" – that is, opting out of the high-risk regime despite their systems posing significant risk, thus escaping the obligations set for high-risk AI systems.

The current lack of a comprehensive list of practical examples exacerbates this risk. For instance, AI systems used to parse resumés,[151] which could impact who gets interviewed, could go unregulated if considered to be a narrow procedural task or a preliminary task. The same goes for an AI system used to translate documents in the context of asylum claims. Such systems can underperform for certain languages, leading to misunderstandings and detrimental effects on asylum seekers.[152] Thus, equality bodies and NHRS will be instrumental in ensuring that high-risk AI systems do not bypass the regulation. They should shape the upcoming guidelines and delegated acts.

3.1.2. Role of equality bodies and NHRS regarding the classification of high-risk AI systems

- Assess the information provided in the self-assessments by providers who opt out of the high-risk regime, to ascertain whether the information provided allows for a proper analysis of impacts on equality and non-discrimination.
- Compile a list of AI systems whose providers have opted out of the high-risk regime under Article 6(3), but pose significant risk. Such examples can be gathered from the EU database of high-risk AI systems,[153] complaints received by the EBs and information obtained through collaboration with CSOs (see 5.3. Co-operation mechanisms).
- Publish this list and directly communicate it to MSAs, DPAs and the European Commission to increase awareness and contribute to the European Commission's guidelines.
- Develop guidance on how AI systems can pose significant risk to equality and discrimination. This guidance can be developed on the basis of the aforementioned list of examples.

149. AI Act, Art. 80 (1)-(2).
150. AI Act, Art. 80 (7).
151. HrFlow.ai, available at https://hrflow.ai/parsing/, accessed 12 November 2025.
152. Bhuiyan J. (2023), "Lost in AI translation: growing reliance on language apps jeopardizes some asylum applications", *The Guardian*, available at www.theguardian.com/us-news/2023/sep/07/asylum-seekers-ai-translation-apps, accessed 10 November 2025.
153. It is unclear if the EBs will have access to the non-public part of the database.

- EBs should co-operate with MSAs and assist them when they evaluate whether an AI system that has been opted out of the high-risk regime poses significant risk of harm to fundamental rights.

3.2. Amending the list of high-risk use-cases

3.2.1. Context and significance

Article 7 gives to the European Commission the power to adopt delegated acts to

1. add or modify use-cases of high-risk AI systems listed in Annex III,[154] and
2. remove high-risk AI systems listed in Annex III.[155]

To understand the difference between these two possibilities, viewing an example from Annex III may help:[156]

> Employment, workers' management and access to self-employment:
>
> (a) AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates;
>
> (b) AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.

In this example, an AI system is considered high-risk in the area of "Employment, workers' management and access to self-employment" for two use-cases in sub-paragraphs (a) and (b).

Add or modify high-risk use-cases

In a delegated act, the Commission can modify any of the use-cases in sub-paragraphs (a) and (b), or add new use-cases by adding sub-paragraph (c), (d), etc. to the AI systems that pose "an adverse impact on fundamental rights, and that risk is equivalent to, or greater than, the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III."[157] However, the Commission cannot add a new area in addition to the eight areas listed as high-risk AI systems in Annex III.

Remove high-risk use-cases

In a delegated act, if the Commission considers that use of AI systems in the area of "Employment, workers' management and access to self-employment" no longer poses

154. AI Act, Art. 7 (1) first sub-paragraph.
155. AI Act, Art. 7 (3) first sub-paragraph.
156. AI Act, Annex III (4).
157. AI Act, Art. 7 (1) (b).

any significant risks nor decreases the protection of fundamental rights, health or safety,[158] then the AI systems used in this area and all use-cases can be removed from Annex III.

For adding or modifying use-cases, and removing high-risk AI systems from Annex III, the Commission needs to consider many criteria. These include[159]

- "the nature and amount of special categories of personal data [that] are processed";
- "the possibility for a human to override a decision or recommendations [from an AI system] that may lead to potential harm";
- current evidence or "significant concerns in relation to the likelihood" of an AI system having had an adverse impact on fundamental rights demonstrated "by reports or documented allegations submitted to national competent authorities or by other reports";
- potential adverse impact on fundamental rights "in particular in terms of its intensity and its ability to affect multiple persons or to disproportionately affect a particular group of persons";
- extent of dependence: "persons who are potentially harmed or suffer an adverse impact are dependent on the outcome produced with an AI system" due to lack of practical viability or legal reasons that make it "not reasonably possible to opt-out from that outcome";
- imbalance of power: "the persons who are potentially harmed or suffer an adverse impact are in a vulnerable position in relation to the deployer of an AI system, in particular due to status, authority, knowledge, economic or social circumstances, or age";
- corrigibility or reversibility of an outcome produced by an AI system where "outcomes having an adverse impact on health, safety or fundamental rights, shall not be considered to be easily corrigible or reversible"; and
- whether existing Union law (not national law) provides "effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages" and "effective measures to prevent or substantially minimise those risks."

These criteria clearly show that fundamental rights, including non-discrimination, are at the core of any amendment to Annex III.

3.2.2. Role of equality bodies and NHRS regarding amending the list of high-risk use-cases

- Document and publish reports highlighting the adverse impact of AI systems on fundamental rights. Such reports should distinguish between
  1. AI systems already considered high-risk in Annex III, and
  2. Use-cases not yet listed in Annex III including those exempted under Article 6(3).

158. AI Act, Art. 7 (3) (a) and (b).
159. AI Act, Art. 7 (2).

The evidence for (1) emphasises the importance of maintaining the areas of high-risk AI systems in Annex III and not removing them. The evidence for (2) emphasises the need to modify or add use-cases in Annex III. For (2), EBs should prioritise AI systems deployed in use-cases where there is power imbalance between deployers such as public authorities and the affected persons, where people do not have an option not to use (for example, migration management or the social security system in a country) and where the outcome of decisions that harm fundamental rights cannot be easily reversed. Such reports can be based on evidence gathered by civil society organisations, in particular on systems that are not yet listed in Annex III. Civil society organisations can also be helpful in identifying priority areas for research and investigation.

- Send these reports to the national competent authorities in the member states, to raise awareness, as well as the European Commission so that they are considered when the Commission plans to draft and adopt delegated acts.
- Conduct or commission research that highlights the shortcomings of Union law "to prevent or substantially minimise"[160] discrimination risks due to uses of AI systems and to provide effective redress mechanisms for affected persons in relation to the risks posed by an AI system, which is one of the criteria that the Commission needs to consider. Such research could be done collaboratively across different equality bodies, via potential co-ordination by The European Network of Equality Bodies (Equinet).

3.3. Risk management system requirements

3.3.1. Context and relevance

The AI Act in Article 9 requires providers of high-risk AI systems to establish, implement, document and maintain a risk management system "throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating."[161] This should include

- "the identification and analysis of the known and the reasonably foreseeable risks"[162] to fundamental rights, especially the "adverse impact on persons under the age of 18 and, as appropriate, other vulnerable groups,"[163] and including evaluation of risks arising post-deployment.[164]
- "the adoption of appropriate and targeted risk management measures designed to address the risks identified"[165] such that "overall residual risk of the high-risk AI systems is judged to be acceptable."[166] These measures include:

160. AI Act, Art. 7 (2) (k) (ii).
161. AI Act, Art. 9 (1).
162. AI Act, Art. 9 (2) (a).
163. AI Act, Art. 9 (9).
164. AI Act, Art. 9 (2) (c).
165. AI Act, Art. 9 (2) (d).
166. AI Act, Art. 9 (5) first sub-paragraph.

- "elimination or reduction of risks identified and evaluated … in as far as technically feasible through adequate design and development of the high-risk AI system",[167]
- "implementation of adequate mitigation and control measures addressing risks that cannot be eliminated",[168]
- transparency and information towards deployers.[169]

It is important to highlight that Article 9 is only concerned with risks "which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information."[170] However, Article 52(1) of the EU Charter of Fundamental Rights states that "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms" and that "[s]ubject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." Put together, it is possible that discrimination harms may not justifiably be included in the risk management systems under Article 9 if they cannot be mitigated or eliminated through technical means. However, unmitigated and persisting risks should be included in the technical documentation under Article 11 of the AI Act.[171] This is especially the case because there may not be an acceptable residual discrimination risk.

Connection with other legal frameworks

Article 16 of the Council of Europe Framework Convention also provides for the adoption and maintenance of a risk and impact management framework. To that end, the Council of Europe has developed the methodology for the risk and impact assessment of AI systems from the point of view of human rights, democracy and the rule of law (HUDERIA) "[to] ensure a uniform approach towards identification, analysis and evaluation of risk and assessment of impact of [AI systems] in relation to the enjoyment of human rights, the functioning of democracy and the observance of rule of law".[172] It proposes a "graduated and differentiated approach to measures for risk and impact identification, assessment, prevention and mitigation that takes into account the severity and probability of the occurrence of the adverse impacts on human rights, democracy and the rule of law as well as relevant contextual factors", through a context-based risk analysis, a stakeholder engagement process, a

167. AI Act, Art. 9 (5) (a).
168. AI Act, Art. 9 (5) (b).
169. AI Act, Art. 9 (5) (c).
170. AI Act, Art. 9 (3).
171. AI Act, Art. 11 and Annex IV paras 2 (g) and (3).
172. Council of Europe Committee on Artificial Intelligence (2022), *Outline of Huderia risk and impact assessment methodology*, Strasbourg, available at https://rm.coe.int/cai-bu-2022-03-outline-of-huderia-risk-and-impact-assessment-methodolo/1680a81e14, accessed 10 November 2025; and Council of Europe Committee on Artificial Intelligence (2024), "Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (Huderia methodology)", Council of Europe, Strasbourg, available at https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f, accessed 10 November 2025.

risk and impact assessment and a mitigation plan; and it demands iterative review. However, it is neither a legally binding instrument nor a source of interpretive guidance in relation to the Framework Convention, and compliance with HUDERIA is not mandatory to satisfy the obligations of the Convention.

3.3.2. Role of equality bodies and NHRS regarding risk management systems requirements

- Collaborate with legal scholars to clarify whether discrimination harms are within the scope of Article 9 considering the references to acceptable residual risk and risks that can be addressed through technical means. Such collaboration will be useful until there is a legally binding interpretation from the CJEU.
- Produce interim guidance on the necessity of including the risk of discrimination in the Article 9 risk assessment. This guidance could include the requirement to explain the identification of the risk, the evaluation of the risk and the adoption of appropriate risk management measures.
- Interim guidance should clarify that, even if the identified discrimination risks in the high-risk AI system cannot be mitigated, they should be included in the technical documentation.

3.4. Data governance requirements

3.4.1. Context and relevance

Data are an integral component in the development of AI systems. Article 10 lays down data governance obligations for providers of high-risk AI systems. Providers could design their own approach, including technical implementation, to fulfil these obligations. Regardless of the approach taken, the fulfilment of these obligations is necessary but not sufficient to limit the risk to non-discrimination due to AI systems. This is because data are only one of the sources of bias and discrimination in AI systems. AI systems can be discriminatory due to the algorithms as well as their evaluations.[173]

Providers of high-risk AI systems are obliged to examine and take "appropriate measures to detect, prevent and mitigate possible biases"[174] in the datasets[175] that are likely to "have a negative impact on fundamental rights or lead to discrimination prohibited under Union law."[176] To fulfil this obligation, it is essential that providers

173. Shrishak K. (2025), "Bias evaluation, AI-complex algorithms and effective data protection supervision", EDPB, available at www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-complex-algorithms-and-effective-data_en, accessed 10 November 2025.
174. AI Act, Art. 10 (2) (g).
175. AI Act, Art. 3 (29)-(33) defines training, validation and testing datasets. AI systems can be developed using these three datasets or with only one dataset, depending on the specific technique. In either case, based on Art. 10 (1) and (6), the obligations in Art. 10 (2)-(5) apply.
176. AI Act, Art. 10 (2) (f).

- make "relevant design choices;"[177]
- collect and use high-quality data based on well formulated assumptions;[178]
- make sure the data sets are "sufficiently representative"[179] for "the persons or groups of persons in relation to whom the high-risk AI system is intended to be used",[180] have the "the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting;"[181] and
- perform "relevant data-preparation processing operations, such as annotation, labelling, cleaning,"[182] etc.

It is important to emphasise that annotation and labelling, which are integral to the performance of many AI systems, are often outsourced to anonymous individuals not from the representative population where the AI system is deployed.[183] Thus it is not uncommon to have incorrect labels in datasets. In some cases, racial slurs and derogatory phrases are added during the labelling process.[184] This issue can also occur in general-purpose AI systems and when they are deployed for specific applications.[185] As a result, annotation and labelling can be a source of bias in data used in developing AI systems.

Although elaborating on the various technical approaches "to detect, prevent and mitigate possible biases"[186] is out of scope of this work,[187] it is important to emphasise that

- AI systems are socio-technical, and purely technical approaches do not fully address biases.[188]
- Removing sensitive variables from datasets is not sufficient because the data usually have proxies that could still contribute to bias.[189]

177. AI Act, Art. 10 (2) (a).
178. AI Act, Art. 10 (2) (d).
179. AI Act, Art. 10 (3).
180. Ibid.
181. AI Act, Art. 10 (4).
182. AI Act, Art. 10 (2) (c).
183. C. G. Northcutt et al. (2021), "Pervasive label errors in test sets destabilize machine learning benchmarks", available at https://labelerrors.com, accessed 10 November 2025.
184. Birhane A. and Prabhu V. U. (2021), "Large image datasets: A pyrrhic win for computer vision?" *WACV (2021 IEEE Winter Conference on Applications of Computer Vision)*, 1536-46; Crawford K. and Paglen T. (2021), "Excavating AI: The politics of images in machine learning training sets", *AI & SOCIETY* 36, 1105-16.
185. Even when no labelling is performed during the initial training of general purpose AI systems, some companies rely on a process called *reinforcement learning from human feedback* later in the development process that introduces bias in the system.
186. AI Act, Art. 10 (2) (g).
187. For more information on bias evaluation, see Shrishak K. (2025), "Bias evaluation, AI-complex algorithms and effective data protection supervision", EDPB.
188. Buyl M. and De Bie T. (2024), "Inherent limitations of AI fairness", *Communications of the ACM*, 67(2), 48-55, available at https://doi.org/10.1145/3624700, accessed 10 November 2025; Schwartz R. et al. (2022). "Towards a standard for identifying and managing bias in artificial intelligence" (National Institute of Standards and Technology, Special Publication 1270).
189. Dwork C. et al. (2012), "Fairness through awareness", *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, 214-26; Kamiran F. and Calders T. (2012), "Data preprocessing techniques for classification without discrimination", *Knowledge and Information Systems*, 33(1), 1-33.

Article 10 (5) of the AI Act

The GDPR generally prohibits the processing of special category personal data,[190] unless an exception applies. Article 10 (5) of the AI Act implements an exception in the GDPR where "processing is necessary for reasons of substantial public interest."[191] The substantial interest invoked in the AI Act is "the purpose of ensuring bias detection and correction."[192]

Article 10 (5) only applies to providers of AI systems, and not to deployers or any other third party. To understand the implications, consider these two example scenarios:

- A public authority as a provider and a deployer: If a public authority develops (as a provider of) an AI system in-house and deploys it to assess welfare benefits, then as a provider, it can rely on Article 10 (5).
- A public authority only as a deployer: If a company (provider) develops AI systems to be used to assess welfare benefits, and the public authority (deployer) buys this AI system and uses it, only the company can rely on Article 10 (5). The AI system developed by a company may be used to assess welfare benefits in multiple countries by different public authorities. However, the public authorities, who may have more geographical and contextual knowledge, would not be able to collect and process special category data to detect and correct bias. This means that public authorities can be incentivised to not develop high-risk AI systems in-house, as this will place greater responsibility (as a provider) on them.

Providers of AI systems can only rely on Article 10 (5) to process special category data when it is strictly necessary for bias detection and correction, and other non-special category data is ineffective.[193] The approach of the providers must be "precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."[194] This could involve documentation to show how the processing of specific special category data ensures bias detection and correction and effectively prevents discrimination.

Furthermore, the provider cannot use this special category of personal data for other purposes, must keep the data secure, not share with or allow access to other parties and delete "once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first."[195] This also means that such data will not be accessible to equality bodies or NHRS, at least, on the basis of Article 10 (5).

However, it is important to emphasise that GDPR's special categories of personal data overlap with only four of the protected characteristics in non-discrimination law: (1) disability, (2) religion or belief, (3) racial or ethnic origin and (4) sexual orientation.

190. GDPR, Art. 9 (1) and Regulation (EU) 2018/1725, Art. 10 (1).
191. GDPR, Art. 9 (2) (g) and Regulation (EU) 2018/1725, Art. 10 (2) (g).
192. AI Act, Art. 10 (5) first sub-paragraph.
193. AI Act, Art. 10 (2) (a) and (f).
194. Judgment of the Court of Justice of 8 April 2014, *Digital Rights Ireland Ltd*, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 65.
195. AI Act, Art. 10 (5) (e).

Providers and deployers are not prohibited by the GDPR from collecting information on the other characteristics, such as age and gender.

Furthermore, providers can already process special category data if the "the data subject has given explicit consent."[196] Article 10 (5) of the AI Act is useful only when the provider cannot obtain explicit consent from the data subject.

Connection with other legal frameworks

Although Article 10 (5) of the AI Act only applies to providers, equality bodies could rely on Article 21 of the Standards Directives,[197] which permits equality bodies to process special categories of personal data. For equality bodies to use this possibility, it is essential that their Member State transposes the Standards Directive in a national law implementing an exception in Article 9 (2) (g) of the GDPR, provided that this exception is not already guaranteed in national data protection or other laws. While the Standards Directive allows equality bodies to process special categories of personal data, neither the AI Act nor the Standards Directive explicitly allows equality bodies to collect such data from AI providers.

3.4.2. Role of equality bodies and NHRS regarding data governance requirements

- Be aware of the limitations of technical approaches to bias detection and correction when assessing risk to discrimination from high-risk AI systems. Compliance with the AI Act, including Article 10, may not be sufficient to address the risk of discrimination from high-risk AI systems. In such scenarios, when the EBs are consulted by an MSA exercising their powers in Article 82 (1), EBs could ask the MSA to force companies "to take all appropriate measures to ensure that the AI system … no longer presents that risk."[198]
- Ensure the transposition into national law of Article 21 of the EU Standards Directives that allows equality bodies to process special categories of personal data, if not already permitted by other national law.

3.5. Fundamental rights impact assessment (FRIA)

3.5.1. Context and relevance

Equality bodies and NHRS should consider FRIA as the entry point to their assessment of AI systems deployed by or on behalf of public administrations. FRIA should include a range of information that will highlight potential gaps and harms to rights, including non-discrimination. FRIA should be performed by the deployer, not the provider, of a high-risk AI system because it is assumed that the deployer has contextual information relevant for this assessment.

196. GDPR Art. 9 (2) (a) and Regulation (EU) 2018/1725, Art. 10 (2) (a).
197. Standards Directives, Art. 21 and Recital 48.
198. AI Act, Art. 82 (1).

FRIA should include information on how the deployer will use the high-risk AI system as intended by the provider, how long and how often the AI system will be used and how the human oversight measures have been implemented.[199] This would, ideally, require the deployer to explain in understandable words how the AI system functions, based on the documentation received from the provider, and it to link to the high-risk AI system registered in the EU database. Public authorities should not use high-risk AI systems that providers have not registered in the EU database.[200]

In addition, FRIA should describe[201]

- "the categories of natural persons and groups likely to be affected";
- "the specific risks of harm" to their fundamental rights, including non-discrimination, considering information supplied by the provider;
- the measures "including the arrangements for internal governance and complaint mechanisms" that the deployer intends to take if these risks materialise.

Where personal data are processed, FRIA complements data protection impact assessments (DPIA), conducted under EU data protection law.[202] Deployers can be expected to combine FRIA with DPIA.

Recital 96 of the AI Act states that "deployers of high-risk AI system, in particular when AI systems are used in the public sector, *could* involve relevant stakeholders, including the representatives of groups of persons likely to be affected by the AI system, independent experts, and civil society organisations in conducting such impact assessments and designing measures to be taken in the case of materialisation of the risks" *(emphasis added)*.

Connection with other legal frameworks

Data protection law provides for conducting impact assessments of AI systems. EU data protection law provides for DPIAs.[203] The Council of Europe Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (the Convention 108+) provides for a general obligation to examine the likely impact of data processing on individuals' rights and fundamental freedoms before their use.[204]

The provisions on fundamental rights impact assessments in the AI Act can be linked to the risk assessment obligations laid down in the Council of Europe Framework Convention and HUDERIA methodology. The Council of Europe Framework Convention requires parties to "adopt or maintain measures for the identification, assessment, prevention and mitigation of risks posed by artificial intelligence systems by considering actual and potential impacts to human rights, democracy and the rule

199. AI Act, Art. 27 (1) (a) and (e).
200. AI Act, Art. 26 (8). This applies to European Union institutions, bodies, offices or agencies as well.
201. AI Act, Art. 27 (1) (c), (d), and (f).
202. AI Act, Art. 27 (4). Also see GDPR, Article 35 and LED, Art. 27. GDPR Art. 35 states that a DPIA should be performed when the processing of personal data is "likely to result in a high risk to the rights and freedoms of natural persons," in particular when involving "automated processing, including profiling."
203. GDPR, Art. 35 and LED, Art. 27.
204. Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Art. 10 (2).

of law."[205] Article 16 (2) (f) of the Convention requires "risks, actual and potential impacts, and the risk management approach" to be documented. Furthermore, such risk assessment measures should "consider, where appropriate, the perspectives of relevant stakeholders, in particular persons whose rights may be impacted"[206] and should "apply iteratively throughout the activities within the lifecycle of the artificial intelligence system".[207]

Limitations of FRIAs

Limited scope: Despite the potential for FRIA to be important, the obligation to perform FRIA before deployment applies only to a subset of deployers of high-risk AI systems:

1. For all high-risk AI systems except in the area of critical infrastructure,[208] the obligation applies to deployers that are
   - bodies governed by public law, or
   - private entities providing public services.[209]
2. For high-risk AI systems for two use-cases – evaluating creditworthiness or establishing credit score of natural persons,[210] and risk assessment and pricing of life and health insurance[211] – this obligation applies to all deployers.

In practice, this means that systems used in the employment sector by private entities (who, here, would be deployers) are exempt from the FRIA obligation.

Additionally, the deployer may not perform FRIA because the provider has opted out of being considered high-risk. It is also possible that the "deployer may, in similar cases, rely on previously conducted fundamental rights impact assessments or existing impact assessments carried out by [the] provider."[212] However, this should not be interpreted as relieving deployers from their obligation to conduct FRIA; It only means that they can build on previously conducted FRIA instead of starting from scratch.

Lack of public information

Public authorities or persons acting on their behalf deploying high-risk AI systems should "register themselves, select the system and register its use in the EU database"[213] and include a summary of the FRIA findings.[214]

---

205. Council of Europe Framework Convention, Art. 16 (1).
206. Council of Europe Framework Convention, Art. 16 (2) (c).
207. Council of Europe Framework Convention, Art. 16 (2) (d).
208. AI Act, Annex III (2).
209. AI Act, Art. 27 (1) first sub-paragraph.
210. AI Act, Annex III (5) (b).
211. AI Act, Annex III (5) (c).
212. AI Act, Art. 27 (2). The provider can also be a deployer of the AI system that it has developed. In such a case, the provider may have carried out FRIA.
213. AI Act, Art. 49 (3).
214. Annex VIII Section C (4).

However, "in the areas of law enforcement, migration, asylum and border control management"[215]

- the EU database will be non-public, with access limited to the European Commission and data protection authorities ;[216]
- FRIA findings will not be included in the EU database.[217]

In addition, even though all deployers in the use-cases of evaluating creditworthiness or establishing credit scores of natural persons,[218] and risk assessment and pricing of life and health insurance,[219] have the obligation to conduct a FRIA (see below), only "deployers that are public authorities, Union institutions, bodies, offices or agencies or persons acting on their behalf"[220] have an obligation to register the use of an AI system into the database. Thus, private companies that deploy AI systems for these use-cases do not need to register. Consequently, the summary of their FRIA will not be made available.

Lack of efficacy to assess risks to non-discrimination

Although deployers should notify the results of the FRIA to the MSA, the assessment itself could be a box-ticking exercise without meaningful impact assessment because the deployer could fill out a "template for a questionnaire" to be developed by the AI Office.[221] One of the risks is that FRIAs will not provide sufficiently precise information to assess how discrimination has been prevented and/or mitigated, which grounds of discrimination have been tested for, and how any legally protected groups have been defined during risk assessment procedures.

3.5.2. Role of equality bodies and NHRS regarding the fundamental rights impact assessment (FRIA) requirements

- **Use the FRIA summaries in the EU database as a starting point to investigate AI systems.** EBs should map the use of high-risk AI systems based on the EU database and assess the summary of the FRIA. Then, EBs could request access to the FRIA results from the MSA. Based on this information, EBs can make an initial assessment regarding breaches of non-discrimination law and whether a full-scale investigation should be pursued, which would require assessing post-deployment (which FRIA does not offer).

215. AI Act, Art. 49 (4) first subparagraph.
216. AI Act, Art. 74 (8) states that the national authority should be the competent authority under the GDPR or the LED, or "any other authority designated pursuant to the same conditions laid down in Articles 41 to 44" of the LED.
217. AI Act, Art. 49 (4) (c).
218. AI Act, Annex III (5) (b).
219. AI Act, Annex III (5) (c).
220. AI Act, Art. 49 (3).
221. AI Act, Art. 27 (3) and (5).

- **Contribute to the template for the FRIA questionnaire.** The AI Office is required to develop a template for the FRIA questionnaire. It will be important for this template to ask appropriate, specific questions on different dimensions of equality and non-discrimination so that the information submitted and the analysis provide adequate assessment and safeguards, rather than becoming a "box ticking" exercise. There is no deadline for the AI Office to produce the template. Equality bodies and NHRS could proactively contribute to such implementation by drafting specific guidance. Such guidance could be developed based on the HUDERIA methodology developed by the Council of Europe.
- **Develop guidance on:**
  - what meaningful summaries of FRIAs entail; and
  - who should conduct FRIAs. Equality bodies and NHRS should emphasise the importance and necessity of fundamental rights expertise in organisations conducting fundamental rights impact assessments.
- **Publish case studies** to highlight "the specific risks of harm" due to discrimination, which should be assessed as part of FRIA. Such studies should focus on specific examples addressing questions around the severity and the scale of the harm. Such a study could be done in collaboration with a willing public authority.

3.6. EU database for high-risk AI systems listed in Annex III

3.6.1. Context and significance

Article 71(1) of the AI Act requires the Commission, "in collaboration with the Member States, [to] set up and maintain an EU database containing information." This database should include information on:

1. High-risk AI systems listed in Annex III;
2. AI systems which have been self-assessed by providers as not high-risk pursuant to Article 6(3).

The information contained in the database should be "easily navigable and machine-readable" as well as, for the public section of the database, "accessible and publicly available in a user-friendly manner".[222] A broad interpretation of accessibility would mean that the information should be not only accessible to readers with disabilities but, following Recital 72 (which discusses requirements for instructions for use prepared by AI providers for AI deployers), also meaningful, comprehensible and understandable to different audiences.[223]

222. AI Act, Art. 71 (4).
223. Equinet 2025 underlines that the recital is about transparency requirements of AI providers to AI deployers (AI Act, Art. 13), and "thus this definition may not apply in this context". However, it points out that it is "the only explanation of what "accessible" means in relation to documentation in the AI Act."

An opportunity for transparency

The registration obligations and the EU database of high-risk AI systems will be particularly useful for equality bodies and NHRS to obtain an overview of AI systems used by public bodies, which is currently lacking (Xenidis 2025). Many stakeholders agree that such databases are a necessary albeit insufficient step to ensure AI systems respect fundamental rights, and especially the right to non-discrimination.[224]

The EU database will be useful for equality bodies and NHRS to monitor the putting on the market or into service of AI systems, for civil society organisations and journalists working on these issues, and for potentially affected people to draw links between their situation and the potential use of AI systems.[225]

Types of systems to be registered

AI systems should be registered in the EU database in the following four cases:

Entity subject to the registration obligation	*Overview of information to be registered*[226]
1. By providers of high-risk AI systems (or, where applicable, the authorised representative) pertaining to areas listed in Annex III, with the exception of high-risk AI systems referred to in point 2 of Annex III ("critical infrastructure") that will be registered at national level,[227] before placing the system on the market or putting it into service.[228]	Name, address and contact details of the provider; Purpose of the system and its components; Basic and concise technical information; Status of the system (e.g. if the system is in use or has been discontinued); The electronic instructions for use communicated by the provider to the deployers in accordance with Article 13(2) (including the "characteristics, capabilities, and limitations of the system, such as its level of accuracy", and human oversight measures[229]).

224. IA Ciudadana (2025), "Making algorithm registers work for meaningful transparency", available at https://iaciudadana.org/2025/03/13/making-algorithm-registers-work-for-meaningful-transparency/; Ada Lovelace Institute (2020), "Meaningful transparency and (in)visible algorithms: Can transparency bring accountability to public-sector algorithmic decision-making (ADM) systems?", available at www.adalovelaceinstitute.org/blog/meaningful-transparency-and-invisible-algorithms/; also C. Cath and F. Jansen (2022), "Dutch comfort: the limits of AI governance through municipal registers", *Techné Research in Philosophy and Technology*, 26(3), pp. 395-412, available at https://doi.org/10.5840/techne202323172, all accessed 10 November 2025.
225. IA Ciudadana (2025), "Making algorithm registers work for meaningful transparency", available at https://iaciudadana.org/2025/03/13/making-algorithm-registers-work-for-meaningful-transparency/.
226 AI Act, Annex VIII and IX, which include a comprehensive list.
227. AI Act, Art. 49 (5).
228. AI Act, Art. 49 (1).
229. AI Act, Art. 13 (2).

2. By providers of AI systems (or, where applicable, their authorised representative) **which they have concluded are not high-risk** despite pertaining to areas listed in Annex III (under Article 6 (3)), before placing the system on the market or putting it into service.[230]	Similar information as for high-risk AI systems, with reduced requirements. For instance, "electronic instructions for use" are not to be registered. The information also includes a short summary of the grounds on which the AI system is considered to be not-high-risk in application of the procedure under Article 6(3);
3. By deployers of high-risk AI systems pertaining to areas listed in Annex III (with the exception of high-risk AI systems in the area of critical infrastructure) **that are "public authorities**, Union institutions, bodies, offices or agencies or persons acting on their behalf", before putting the system into service or using it.[231]	Name, address and contact details of the deployer; The URL of the entry of the AI system in the EU database by the provider; A summary of the findings of the Fundamental Rights Impact Assessment that has to be conducted as per Article 27; A summary of the DPIA carried out pursuant to relevant data protection regulation.
4. By providers of high-risk AI systems referred to in Annex III conducting **testing in real world conditions** outside AI regulatory sandboxes.[232]	The name and contact details of the provider or prospective provider and of the deployers involved in the testing in real world conditions; A brief description of the AI system, its intended purpose and other information necessary for the identification of the system; A summary of the main characteristics of the plan for testing in real world conditions; Information on the suspension or termination of the testing in real world conditions.

230. AI Act, Art. 49 (2).
231. AI Act, Art. 49 (3). See also AI Act, Annex III (1), (6) and (7).
232. AI Act, Art. 60 (4) (c).

Deployers of AI systems not concerned by obligations *"should be entitled"* to register their system in the database voluntarily, which includes deployers that are private entities.[233]

Public authorities as deployers must check whether the provider has registered the high-risk system in the database. If the system is not registered, they shall not use it and inform the provider or distributor.[234]

A public and a non-public version of the database

The database will contain two sections: a public section, and a "secure, non-public" version.[235] The non-public version of the database will contain information on:

- High-risk AI systems used in biometrics, law enforcement, and migration, asylum and border control management;[236]
- High-risk AI systems that are tested in real world conditions under Article 60 (unless the provider has consented to making this information publicly accessible).[237]

Timeline of setup and implementation

- The Commission is responsible for setting up the functional specifications of the database, in consultation with "relevant experts", and updating the functional specifications of the database will be done by the Commission, in consultation with the AI Board.[238]
- At the time of writing, the database has not yet been set up by the European Commission.
- Registration into the database will become mandatory on 2 August 2026. However, registration before 2 August 2026 is also encouraged, on a voluntary basis.[239]

Connection with other legal frameworks

Registration obligations in the AI Act can be linked to Article 8 of the Council of Europe Framework Convention, which provides that parties shall adopt or maintain measures to ensure "adequate transparency and oversight requirements", and to Article 9, which pertains to measures "to ensure accountability and responsibility for adverse impacts on human rights, democracy and the rule of law". Article 14 of the Framework Convention also requires parties to put in place "measures to ensure that relevant information regarding artificial intelligence systems which have the potential to significantly affect human rights and their relevant usage is documented, provided to bodies authorised to access that information and, where appropriate and applicable, made available or communicated to affected persons."

233. AI Act, Recital 131 *(emphasis added)*.
234. AI Act, Art. 26 (8).
235. AI Act, Art. 49 (4) and AI Act, Art. 71 (4).
236. AI Act, Art. 49 (4).
237. AI Act, Art. 60 (4) (c).
238. AI Act, Art. 71 (1).
239. AI Act, Recital 179.

The explanatory report to the Framework Convention recognises that: "Parties are required to strike a proper balance between [transparency] and various competing interests,"[240] including "privacy, confidentiality (including, for instance, trade secrets), national security, protection of the rights of third parties, public order, judicial independence". However, the term "adequate" suggests that a minimum level of transparency, in particular towards the general public, should be considered, even for AI systems for which certain information has to be kept private.

Challenges

The database presents several limitations that may hinder its usefulness at identifying and mitigating discrimination in AI systems.

- **Some information will be in the non-public section of the database:**
  - Information on AI systems used in biometrics, law enforcement, and migration, border control and asylum;
  - Information on AI systems tested in real world conditions.

- **Some information will not be recorded in the database at all:**
  - The scope of the database is limited to high-risk AI systems. This could leave out applications such as chatbots used by public servants or directly interacting with citizens.
  - Providers and deployers of high-risk AI systems in biometrics, law enforcement, and migration, asylum and border control have to register less information about their AI systems. For instance, providers are not required to register the electronic instructions for use provided to the deployers. Deployers do not have to register a summary of their FRIAs.
  - When providers of AI systems do not consider them high-risk as per Article 6 (3), their deployers do not have to register their putting into service or testing in the database.
  - Only deployers who are "public authorities, Union institutions, bodies, offices or agencies or persons acting on their behalf"[241] are required to register. However, deployers of some high-risk AI systems may be private entities, such as insurance companies; such deployers are not required to register their AI system in the EU database. This means some information, such as the summary of FRIA, will not be available about these high-risk AI systems.
  - Even for high-risk AI systems registered in the public-facing version of the database, the information to be registered is not guaranteed to be sufficient to assess discrimination. For instance, deployers are required to submit only a summary of FRIAs, and not the complete FRIAs.

240. Council of Europe (2024), Explanatory report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, paragraph 62.
241. AI Act, Art. 49 (3).

- Registration in the database will only be mandatory from 2 August 2026. This means that AI systems put in service before that date will not be obligated to be recorded, barring "significant change".[242]

Access by equality bodies and NHRS to information in the non-public section of the database

AI systems used in law enforcement, and migration, asylum and border control management have had discriminatory effects on people (see Section 7.1: Thematic focus on law enforcement, migration, asylum, and border control), and access to the documentation contained in the non-public version of the database is necessary for equality bodies and NHRS to effectively fulfil their mandate. Without such access, EBs and NHRS will be unable to have an overview of high-risk AI systems used in these areas. However, the extent to which EBs and NHRS can access the information in the non-public version of the database is unclear.

Article 71 (4) states that "the information registered in accordance with Article 60 [of high-risk AI systems outside regulatory sandboxes] shall be accessible only to market surveillance authorities and the Commission, unless the prospective provider or provider has given consent for also making the information accessible to the public." Article 49 (4) on registration also provides that "only the Commission and national authorities referred to in Article 74 (8) shall have access" to information pertaining to high-risk AI systems used in biometrics, law enforcement, and migration, asylum and border control management.

Article 77(1) provides that "national public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights, including the right to non-discrimination, in relation to the use of high-risk AI systems referred to in Annex III shall have the power to request and access any documentation created or maintained under this Regulation in accessible language and format when access to that documentation is necessary for effectively fulfilling their mandates within the limits of their jurisdiction" (see Article 77).

If legal bases for information sharing between equality bodies/NHRS, market surveillance authorities and other Article 77 bodies is established (see 5.3. Co-operation mechanisms), then it would be possible for EBs and NHRS to access information obtained by market surveillance authorities under Article 71 (4) and 49 (4).

3.6.2. Role of equality bodies and NHRS regarding the EU database for high-risk AI systems listed in Annex III

During the setup of the database

- Participate as relevant experts[243] (possibly via Equinet or other means) in the setup of the database, including to ensure the database fulfils the accessibility requirement.

242. AI Act, Recital 177.
243. AI Act, Art. 71 (1).

Once the database is in place

- Advocate for the database to be filled voluntarily by government agencies when they are deployers of AI systems which are not considered high-risk, and deployers of high-risk AI systems who are private entities (especially in the insurance and banking sectors).
- Develop a co-ordination template with the national competent authorities which will have access to the non-public version of the database.
- Advocate for national laws implementing the AI Act to clearly state that EBs and NHRS should have access to the information submitted to the national authorities and to the non-public EU database.
- Monitor AI systems registered in the database to identify high-risk AI systems which should be investigated further due to their risks of discrimination, either by EBs or by market surveillance authorities (possibly in collaboration with other stakeholders such as civil society organisations).
- Monitor registered AI systems that were not considered high-risk under Article 6(3) and use the summary of self-assessments to identify whether they should be considered high-risk. If so, report to the MSA and request they carry out an evaluation under the Article 80 procedure for dealing with AI systems classified by the provider as non-high-risk.
- Monitor AI systems pertaining to credit scoring and insurance registered by providers, to ask deployers for information not present in the database such as FRIAs.
- Use the public version of the database as an awareness-raising tool about how AI systems are used in the public sector.
- Monitor how the database is used by civil society organisations, journalists, individuals and other relevant institutions, and suggest updates to the Commission and the AI Board. In particular, monitor if the information contained in the summaries of FRIAs is sufficient to assess risks to non-discrimination.



4. Transparency of AI systems requirements

4.1. Context and significance

Article 50 lays down transparency obligations for providers and deployers of AI systems, that should be communicated clearly to natural persons "at the latest at the time of the first interaction or exposure"[244] and conforming to accessibility requirements.

Deployers should inform natural persons when

- deploying an emotion recognition system[245] or a biometric categorisation system;[246]
- deploying an AI system that generates deep fake;[247]

244. AI Act, Art. 50 (5).
245. AI Act, Art. 3 (39).
246. AI Act, Art. 3 (40).
247. AI Act, Art. 3 (60): "'deep fake' means AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful".

- deploying "an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest."[248]

Providers should design and develop the AI systems that interact with natural persons such that natural persons are made aware of this interaction, and do not assume that they are interacting with a human. This obligation applies "unless this is obvious … [to a] reasonably well-informed, observant and circumspect [natural person], taking into account the circumstances and the context of use."[249]

For AI generated content, providers of AI systems should provide "effective, interoperable, robust and reliable"[250] technical solutions that provide machine-readable marking to detect that the content has been artificially generated or manipulated. However, this obligation is conditional on the technical feasibility, the state of the art and the types of content generated. This obligation extends to providers of general-purpose AI systems.[251]

The EU AI Office based within the European Commission may also "encourage and facilitate the drawing up of codes of practice at Union level"[252] on detecting and labelling artificially generated or manipulated content and may adopt implementing acts to adopt these codes of practice. On 4 September 2025, a consultation was launched to begin the process to develop guidelines and codes of practice.[253] If the eventual codes of practice are inadequate, the Commission may adopt implementing acts that provide common rules.

Three important points to keep in mind:

1. Article 50 applies to all AI systems, regardless of whether they are high-risk or not;[254]
2. compliance with Article 50 does not make the use or the output of an AI system lawful,[255] for example, some AI systems are prohibited under Article 5;
3. Article 50 obligations do "not apply to AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences."[256]

Connection with other legal frameworks

Transparency and oversight are among the principles laid down by the Council of Europe Framework Convention.[257] Article 15 (2) of the Framework Convention provides

248. AI Act, Art. 50 (4), second sub-paragraph clarifies that deployers do not need to inform the public of artificially generated content if the "content has undergone a process of human review or editorial control and where a natural or legal person holds editorial responsibility for the publication of the content."
249. AI Act, Art. 50 (1).
250. AI Act, Art. 50 (2).
251. AI Act, Art. 3 (66).
252. AI Act, Art. 50 (7).
253. "Commission launches consultation to develop guidelines and Code of Practice on transparent AI systems", 4 September 2025, available at https://digital-strategy.ec.europa.eu/en/news/commission-launches-consultation-develop-guidelines-and-code-practice-transparent-ai-systems, accessed 11 November 2025.
254. AI Act, Art. 50 (6) and Recital 132.
255. AI Act, Recital 137.
256. AI Act, Art. 50 (1).
257. Council of Europe Framework Convention, Art. 8.

that "[e]ach Party shall seek to ensure that, as appropriate for the context, persons interacting with artificial intelligence systems are notified that they are interacting with such systems rather than with a human."

4.1.1. Role of equality bodies and NHRS regarding transparency of AI systems requirements

This article can be considered through the lens of prohibited uses listed in Article 5:

- Consider Article 50 in conjunction with Article 5 (1) (a) and (b) and advocate for the prohibition in those articles where the transparency obligation in this article is insufficient to prevent harms to fundamental rights; this should include the situation where the technical solutions and state-of-the-art labelling of AI generated and manipulated content are not "effective, interoperable, robust and reliable".[258]
- Consider Article 50 in conjunction with Article 5 (1) (f), which prohibits emotion recognition systems in workplaces and educational institutions, and Article 5 (1) (g), which prohibits biometric categorisation systems "that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation".[259] Article 50 does not make prohibited AI systems lawful.
- Prevent "de-risking" strategies, by conducting or commissioning a legal study to identify the various situations and conditions when Article 50 transparency obligations might be used to get around Article 5 prohibitions. This study should be published to inform providers and deployers that they should not attempt to circumvent the prohibitions. This study could be done in co-ordination with different equality bodies and/or NHRS.

258 AI Act, Art. 50 (2).
259 AI Act, Art. 5 (1) (g).



5. Enforcement

5.1. Powers of bodies protecting fundamental rights

5.1.1. Context and significance

Article 77 offers EBs new powers to assess discrimination through AI systems, through a right to access documentation, a right to testing and a right to collaboration from MSAs and AI operators. However, EBs are not automatically considered relevant bodies under Article 77.

Cumulative conditions for an EB to be an authority under Article 77

1. They should be considered as "[n]ational public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights, including the right to non-discrimination."[260]
2. Their Member State should have explicitly identified the EB or other fundamental rights body, include them in a list to notify the Commission and other Member

260. AI Act, Art. 77 (1).

States, and should have made the list public by 2 November 2024. Member States "shall keep the list up to date,"[261] which indicates that EBs or other fundamental rights bodies not listed by Member States at the first notification deadline can still be added. EBs and other bodies could also be removed from the list.

In this section and the rest of the document, when we refer to EBs, we are specifically referring to EBs who are identified as Article 77 bodies under the AI Act in their Member State.

Equality bodies' role in the Council of Europe Framework Convention

Equality bodies and human rights structures are explicitly mentioned by the Council of Europe Framework Convention as competent to be part of the oversight measures to ensure compliance with the obligations in the Convention.[262] The Framework Convention also provides that such mechanisms "exercise their duties independently and impartially and that they have the necessary powers, expertise and resources to effectively fulfil their tasks of overseeing compliance with the obligations in this Convention."[263] This is a notable difference between the Council of Europe Framework Convention and the AI Act: under the AI Act, the market surveillance authorities are tasked with monitoring and enforcement, while the equality bodies and NHRS are identified as Article 77 bodies, but are not part of the oversight measures. Under the Council of Europe Framework Convention, equality bodies and NHRS could be designated as part of the supervision and enforcement authorities.

Powers of the EBs under Article 77

► Right to request and access documentation

EBs and NHRS "in relation to the use of high-risk AI systems referred to in Annex III shall have the power to request and access any documentation created or maintained under this Regulation in accessible language and format".[264] EBs and NHRS should interpret and test the use of this article to request any documentation under the AI Act that is necessary for effectively fulfilling their mandates. EBs and NHRS should inform MSAs of their country when they make a request for documentation. This documentation could be used to identify discrimination harms to individuals or groups, e.g. the AI system performing poorly for black women and resulting in cutting off welfare benefits to them, even when the AI system performs well for black people overall.[265]

261. AI Act, Art. 77 (2).
262. Council of Europe (2024), Explanatory report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, paragraph 63.
263. Council of Europe Framework Convention, Art. 26.
264. AI Act, Art. 77 (1).
265. For an extended analysis of (1) what documentation EBs could have access to and (2) how to understand the basic parameters of this technical documentation gathered on the basis of implemented technical standards, see Equinet 2025.

▸ Right to testing

If the documentation is insufficient "to ascertain whether an infringement of obligations under Union law protecting fundamental rights has occurred,"[266] EBs and NHRS can ask MSAs "to organise testing of the high-risk AI system through technical means … within a reasonable time".[267] Such insufficiencies could consist in providers failing to report the results of multiple fairness metrics, or narrowly defining impacting groups, thus making it impossible to assess specific types of discrimination, in particular intersectional discrimination (Equinet 2025). EBs and NHRS should be closely involved with MSAs during the testing.

▸ Right to collaboration with MSAs and AI operators

- When MSAs are notified by providers of high-risk AI systems of any serious incident[268] that violates Union law intended to protect fundamental rights such as non-discrimination,[269] MSAs should inform the EBs and NHRS.[270]
- MSA should evaluate "AI systems presenting a risk"[271] to fundamental rights including risk to vulnerable groups.
  - MSAs are required to "inform and fully cooperate"[272] with EBs and NHRS when carrying out the evaluation.
  - The relevant operators of AI systems are also required to co-operate with MSAs and EBs and NHRS.[273]
  - MSAs, based on their evaluation, can require AI operators to take corrective action, withdraw the AI system from the market or recall it.[274]
- EBs and NHRS should co-operate with MSAs and assist them when they evaluate whether an AI system that has been opted out of the high-risk regime poses significant risk of harm to fundamental rights.
- MSAs should evaluate if "an AI system classified by the provider as non-high-risk pursuant to Article 6(3) is indeed high-risk"[275] due to a risk to fundamental rights. EBs can assist MSAs with this evaluation.
- The MSA has a requirement to consult EBs and NHRS even when a high-risk AI system is compliant with the AI Act, but still presents a risk to fundamental rights.[276]

266. AI Act, Art. 77 (3).
267. Ibid.
268. AI Act, Art. 73 (1).
269. AI Act, Art. 3 (49): A serious incident is "an incident or malfunctioning of an AI system that directly or indirectly leads to … (c) the infringement of obligations under Union law intended to protect fundamental rights".
270. AI Act, Art. 73 (7).
271. AI Act, Art. 79 (1) and Regulation (EU) 2019/1020, Art. 3 (19).
272. AI Act, Art. 79 (2).
273. Ibid.
274. Note Regulation (EU) 2019/1020, Art. 18: AI operators have a right to be heard before such a measure is taken.
275. AI Act, Art. 80 (1).
276. AI Act, Art. 82 (1).

EBs and NHRS can thus contribute to the investigations of MSAs and potentially suggest relevant corrective actions, including withdrawal of the AI system from the market, since they could be involved in assisting MSAs finding whether a potentially discriminatory AI system is not compliant with the obligations in the AI Act.

These powers, when used, can be effective in assessing and remedying discrimination in AI systems.

Furthermore, it is important to highlight that the AI Act is "without prejudice to the competences, tasks, powers and independence of relevant national public authorities or bodies which supervise the application of Union law protecting fundamental rights, including equality bodies."[277] In other words, investigations assessing compliance with the AI Act do not affect investigations assessing compliance with equality laws.[278] Similarly, affected persons have the right to lodge a complaint under Article 85 of the AI Act as well as under equality laws.

5.1.2. Role of equality bodies and NHRS regarding Article 77 of the AI Act

- Advocate to become Article 77 bodies.
- As Article 77 bodies, through their right to request and access documentation:
  - Develop robust arguments supporting their right to access information, building on the work of Equinet (see Equinet 2025). Otherwise, EBs and NHRS are likely to be challenged by companies and public authorities in their attempts to prevent access.
  - Develop test cases, based on the available information, to establish if the information is relevant to carry out their mandate.
  - Use the documentation received to investigate discrimination harms.
  - Check for ethics washing and assess how groups have been defined by AI operators when testing for bias.
- As Article 77 bodies, in the context of testing:
  - Ensure that they have sufficient resources to be able to co-operate effectively with MSAs, who will be leading the testing. This can entail having in-house technical expertise, non-technical staff trained to collaborate with technical experts, or building partnerships with external partners (for more detail, see 5.3. Co-operation mechanisms).
  - Develop templates for co-operation with MSAs.
- As Article 77 bodies, in the context of enforcement actions by MSAs:
  - Raise awareness about the risks of AI systems to discrimination by, for example, publishing their decisions.

277. AI Act, Recital 157.
278. See also AI Act Recital 45: the AI Act does not affect prohibitions under Union non-discrimination law.

- Track and publicise actions related to their role as Article 77 bodies, to raise general awareness of their role and illustrate their necessity to promote equality and non-discrimination in AI systems.

▶ Issue guidance and advocate for fundamental rights to be taken into account by the European Commission:

- The European Commission "shall establish a simplified technical documentation form targeted at the needs of small and microenterprises."[279] The harm to the rights of the people is not correlated with the size of the companies developing high-risk AI systems. EBs and NHRS should emphasise that essential information in the documentation is not to be left out.
- The European Commission is empowered to adopt delegated acts in accordance with Article 97 (exercise of delegation) to amend Annex IV (technical documentation of high-risk AI systems).
- Contribute to the guidance of the European Commission on serious incident reporting. The European Commission is expected to develop guidance on serious incident reporting by 2 August 2025.[280] This guidance is likely to include co-ordination and protocols for the transfer of information from MSAs to EBs and NHRS. EBs through Equinet or other bodies should consider influencing this guidance.
- See also recommendations listed under these guidelines related to classification, amending list of high-risk and prohibited AI systems, fundamental rights impact assessments, etc.

5.2. Remedies

5.2.1. Context and relevance

The AI Act offers natural and legal persons the right to complain to an MSA and, for the individual, a right to explanation. However, neither of these rights are in and of themselves effective rights.

Right to complain

An affected person can complain to an MSA (Article 85). The complaint "shall be taken into account for the purpose of conducting market surveillance activities"[281] and handled according to "procedures for following up on complaints."[282] However, there is no general obligation on the MSA to act on a complaint of an affected person. The complainant does not have a legal standing in the process even when the complaint is "taken into account for the purpose of conducting market surveillance

279. AI Act, Art. 11 (1) second subparagraph.
280. AI Act, Art 73 (7).
281. AI Act, Art. 85.
282. Regulation (EU) 2019/1020, Art. 11 (7) (a).

activities."[283] Thus, the right to complaint in the AI Act can, at best, be treated as a partial right. This right, however, is without prejudice to other existing remedies in other national and Union laws.[284]

Whenever the fundamental rights of a person are harmed through an AI system, they should instead consider complaining to a fundamental rights body, for example an equality body in the case of discrimination. When personal data are involved, an affected person may also have the option to complain to the relevant data protection authority.[285]

Right to an explanation

The AI Act also provides any affected person the right to explanation (Article 86) when the deployer makes a decision "on the basis of the output from a high-risk AI system listed in Annex III … which produces legal effects or similarly significantly affects that person in a way that they consider to have an *adverse impact on* their health, safety or *fundamental rights*."[286] The explanation should include "clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken."[287]

When does the right to explanation under the AI Act apply?

However, the right to explanation in the AI Act only applies if the same right "is not otherwise provided for under Union law."[288] When personal data are processed by high-risk AI systems, the right to information in Article 15 (1) (h) in the GDPR that includes "meaningful information about the logic involved"[289] will apply.

Furthermore, it is important to emphasise that there is a general prohibition under Article 22 (1) of the GDPR for a "decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." This means that high-risk AI systems using personal data that produce "legal effects or similarly significantly affects" can only be used when specific exceptions under Article 22 (2) of the GDPR apply, namely when such use:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

283. AI Act, Art. 85. An affected party could also consider other avenues for redress such as Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC. See also AI Act, Art. 110.
284. AI Act, Recital 170.
285. GDPR, Art. 77-79.
286. AI Act, Art. 86 (1). *(Emphasis added.)*
287. AI Act, Art. 86 (1).
288. AI Act, Art. 86 (3).
289. GDPR, Art. 15 (1) (h): "(1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: … (h) the existence of automated decision making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

Moreover, the word "solely" has been interpreted in the Schufa case to include automated processing that may only be a part of the decision but still plays a "determining role."[290]

Thus, Article 86 of the AI Act can be useful in two situations:

1. When personal data are not involved in the high-risk AI system (otherwise Article 15 (1) (h) of the GDPR would apply); and
2. When personal data are involved and automated processing using the high-risk AI system does not play a "determining role" in the decision (See CJEU Schufa decision above).

What is a meaningful explanation?

The AI Act requires "clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken."[291] The judgment in *CK v Dun & Bradstreet* could be helpful. It clarified that "meaningful information about the logic involved"[292] in the GDPR means "a concise, transparent, intelligible and easily accessible form, the procedure and principles actually applied in order to use, by automated means, the personal data concerning that person with a view to obtaining a specific result."[293] Such an explanation is "not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm."[294]

Trade secret protection

The AI Act states that the "right to obtain an explanation should not apply to the use of AI systems for which exceptions or restrictions follow from Union or national law."[295] One such exception could be the protection of trade secrets.[296] As in *CK v Dun & Bradstreet,* the right to explanation would need to be balanced with the protection of intellectual property including trade secrets. In that case, the court judged that the balancing of rights needs to be performed by the regulator or a relevant court, and not by the company.[297] In the case of the AI Act, a similar analogous argument can be made.

---

290. Judgment of the Court of Justice of 7 December 2023, *SCHUFA Holding (Scoring)*, C-634/21, EU:C:2023:957, paragraph 50.
291. AI Act, Art. 86 (1).
292. GDPR, Article 15 (1) (h).
293. Judgment of the Court (First Chamber) of 27 February 2025. *CK v Dun & Bradstreet Austria GmbH and Magistrat der Stadt Wien*, C-203/22, ECLI:EU:C:2025:117, paragraph 66.
294. Ibid., paragraph 60.
295. AI Act, Recital 171.
296. Directive 2016/943, Article 2 (1).
297. Judgment of the Court (First Chamber) of 27 February 2025. *CK v Dun & Bradstreet Austria GmbH and Magistrat der Stadt Wien*, C-203/22, ECLI:EU:C:2025:117, paragraph 76.

5.2.2. Role of equality bodies and NHRS regarding remedies

- Inform citizens of their rights. As part of their duty to assist victims of discrimination (as outlined in the Standards Directives), EBs should inform individuals of their right to an explanation and right to lodge a complaint with the market surveillance authority under the AI Act and with the data protection authority under EU data protection law. This entails training the staff to recognise instances where the right to explanation applies.
- Individuals should be informed that this right is in addition to and not instead of pursuing existing legal action.

5.3. Co-operation mechanisms

5.3.1. Context and relevance

For EBs and NHRS to be effective and use their powers under the AI Act, they have to co-operate with the MSAs in their country as well as other Article 77 bodies, including data protection authorities. In addition, consultation with civil society organisations will benefit the work of EBs.

5.3.2. Role of equality bodies and NHRS regarding co-operation with different stakeholders

Co-operation between Article 77 bodies

EBs and NHRS should convince their Member State that a clear legal basis for the sharing of information between Article 77 bodies is established, if it has not been already. The AI Act provides for the sharing of information between MSAs and EBs/NHRS.[298] However, in certain situations, EBs and NHRS will need to also co-operate with other Article 77 bodies in their country, for which a separate legal basis for information sharing would be required.

Co-operation with MSAs

EBs and NHRS should establish a close working relationship with MSAs as soon as they are established. The exact structure of governance in each Member State may vary. It is possible that some countries will choose one regulator as market surveillance authorities while others will choose a range of regulators. Both the Netherlands and Ireland have indicated a preference for multiple regulators in a hub-and-spoke model with a lead regulator supporting other regulators. France has set up a co-ordinated governance scheme: the General Directorate for Competition Policy, Consumer Affairs and Fraud Control [*Direction générale de la concurrence, de la consommation et de la répression des fraudes*] is responsible for operational co-ordination, and liaises with the General Directorate of Enterprises for strategic co-ordination.

298. AI Act, Art. 73 (7) and 79 (2).

Over ten other entities are then tasked with specific provisions of the AI Act, including national Data Protection Authority CNIL (*la Commission nationale de l'informatique et des libertés*) and Media Regulator Arcom (see Direction générale des Entreprises 2025). In such a setting, EBs should establish collaboration with all of the market surveillance authorities with a specific priority for the lead market surveillance authority.

Establish legal bases for information sharing

EBs and NHRS should convince their Member State Government and ensure that the Member State has established a broad legal basis for sharing of information between Article 77 bodies as well as between MSAs and Article 77 bodies.[299] The existence of such legal bases is a prerequisite to establish bilateral and multilateral co-operation agreements for information sharing. Such agreements should be broadly drafted to cover the remit of the Article 77 bodies and MSAs. These agreements should allow for additional case-specific bilateral agreements where needed.[300]

Establish equality-specific taskforces

EBs and NHRS along with MSAs should establish task forces that can exchange their expertise with each other on specific topics. Initially, such a task force can work towards establishing common understanding across organisations. An example taskforce could be "best practices in identifying discrimination harms through AI systems". This can be helpful for EBs in developing guidance for MSAs on identifying discrimination harms so that EBs can be notified.

Establish clear automatic triggers that oblige the MSA to co-operate with equality bodies and NHRS

It is important that the MSAs are made acutely aware about the expertise, e.g. on non-discrimination and equality, of the EBs and NHRS. The MSAs should be automatically triggered to inform EBs when a serious incident that infringes non-discrimination has been reported under Article 73 (7). When MSAs are unsure whether there is a risk of discrimination, they should consult EBs immediately, for instance in scenarios related to Article 79 and 80 of the AI Act, so that the EB can provide their expertise. It is better to receive false flags instead of missing out on infringements that the MSAs have overlooked due to lack of expertise.

Notification of non-compliance from other EU countries

Where MSAs identify non-compliance that is not restricted to their national territory, they are required to "inform the Commission and the other Member States without undue delay of the results of the evaluation and of the actions which it has required the operator to take"[301] and further notify along with details if

299. De Autoriteit Persoonsgegevens (2024), *Final recommendation on supervision of AI: sector and centrally coordinated*, paragraph 37, available at www.autoriteitpersoonsgegevens.nl/en/current/final-recommendation-on-supervision-of-ai-sector-and-centrally-coordinated, accessed 11 November 2025.
300. Ibid.
301. AI Act, Art. 79 (3).

the operator fails to comply with the required actions.[302] EBs and NHRS should emphasise to MSAs and the EU AI Board that the EBs and NHRS in other member states should be informed and notified when the evaluation of non-compliance involves risks to fundamental rights such as non-discrimination.

Access to documents

EBs and NHRS can request documents from providers of high-risk AI systems.[303] EBs could also access the documentation from the MSAs if an MSA has already accessed the same from the provider. This could accelerate the process of access for EBs and NHRS. In both cases, it is important to highlight that companies cannot prevent the MSAs from sharing the documentation with EBs and NHRS under the guise of trade secret protection. Especially in the case where EBs and NHRS request the documentation through the MSA, the recent judgment indicates that the company cannot decide whether the documentation can be shared or not.[304] That decision is for the regulator or Court.

Involvement in testing

When EBs and NHRS find the documentation provided by the providers insufficient to ascertain whether an infringement of Union law protecting fundamental rights has occurred, then they may request the MSA "to organise testing of the high-risk AI system through technical means … within a reasonable time."[305] The AI Act states that the MSAs should organise the tests. This leaves room for the tests to be performed by a third party vendor or expert. The testing should be conducted with "the close involvement"[306] of EBs and/or NHRS.

It is important for EBs and NHRS to establish:

- Who will perform the test?
- What is being tested?
- The exact nature of "reasonable time". This should be established as early as possible and not when a case arises;
- The exact mutual understanding between EBs/NHRS and MSAs of "close involvement". Does it involve a point of contact directly involved in testing? Does it involve EBs/NHRS consulted on the steps of the tests a priori?
- Develop a protocol for interagency working?

Examples and good practices

Inspiration can be drawn from past co-operations between equality bodies, NHRS and data protection authorities. In the United Kingdom, the Equality and Human Rights Commission worked with the Information Commissioner's Office as part of the Fairness and Innovation Challenge, on test cases in higher education, finance, healthcare and recruitment, in order to find new ways to address statistical, human and structural bias and discrimination in AI systems. The Challenge was funded by the United Kingdom's Ministry of

302. AI Act, Art. 79 (5)-(6).
303. AI Act, Art. 77 (1).
304. Judgment of the Court (First Chamber) of 27 February 2025. *CK v Dun & Bradstreet Austria GmbH and Magistrat der Stadt Wien*, C-203/22, ECLI:EU:C:2025:117, p. 76.
305. AI Act, Art. 77 (3).
306. Ibid.

Science.[307] In Norway, the equality body has co-operated with the data protection authority as part of a regulatory sandbox on artificial intelligence.[308]

In France, co-operation between the EB Defender of Rights and the DPA CNIL is facilitated by several mechanisms: both institutions have a memorandum of understanding agreement, and the Defender of Rights has also an advisory role to the board of CNIL. Because of this structural link, the Defender of Rights is informed of all the projects submitted to plenary meetings of the board of CNIL.[309]

Co-operation with other public agencies

Co-operation should also be considered as a way to pool specific resources. For instance, France has set up a data science taskforce called *PEReN* (Le Pôle d'expertise de la régulation numérique), made up of around 20 data scientists, hosted by the Ministry of the Economy, but available to all central agencies and regulators. This enables the French EB Defender of Rights to have access to state-of-the-art technical knowledge and skills. Importantly, in case of such co-operation, clear collaboration mechanisms have to be put in place to ensure the needs of EBs will be filled and to set up safeguards for EB independence.

Co-operation with civil society and other external stakeholders

Establish an advisory forum in each member state, consisting of members of civil society, grass roots organisations and academics who together combine experience on the ground with expertise in equality and non-discrimination law, but also in digital rights. This advisory forum can flag harmful uses of AI that equality bodies in their member states can prioritise investigating. The forum should meet regularly and exchange insights with equality bodies.

Continue and deepen existing engagement with civil society organisations

Equinet and equality bodies in some member states (for example, Belgian EB Unia) have regularly engaged with civil society organisations by inviting them to events and discussions. Such engagements offer the opportunity to exchange information that can benefit both sides. There is room to deepen these engagements with respect to AI by establishing connections between civil society organisations and equality bodies in other member states. However, this would likely require more human resources. A pathway would be to extend formal co-operation structures that exist in other regulatory contexts.

Improve complainant handling

Establish a clear and straightforward complaint-handling process for discrimination harms from AI systems.[310] Share the equality bodies/NHRS process to receive

307. Gov.uk (2024), Press release: "AI Fairness Innovation Challenge winners announced", available at www.gov.uk/government/news/ai-fairness-innovation-challenge-winners-announced, accessed 11 November 2025.
308. See www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/, accessed 11 November 2025.
309. Information based on the interview with the Defender of Rights.
310. See also Equinet (2023), Minimal guidelines on improving complaints data collection by equality bodies, available at https://equineteurope.org/wp-content/uploads/2024/01/Minimal-Guidelines-on-Improving-Complaints-Data-Collection-by-Equality-Bodies-1.pdf, accessed 11 November 2025.

complaints under its mandate and the rights of the complainant throughout the process. Raise awareness with civil society about the process and examples of case studies that clarify the kinds of complaints equality bodies and NHRS can handle within their remit. It can be helpful to also highlight cases which are within the remit of regulators under the AI Act and/or the GDPR, and the rights of the complainants under those laws. Encourage civil society organisations to share this information with people being harmed through AI systems so that potential complainants are empowered.

External experts can also bring technical expertise

The project AI Equality by Design enabled professors to give academic advice on cases of AI and discrimination[311]. It may be necessary to seek funding from government, through academic research initiatives, litigation funding or elsewhere to obtain expert evidence or advice.

311. Equinet (2025), Embedding equality safeguards into technical standards for the EU AIA and empowering equality defenders: Equinet's participation in the project "Equality by Design, Deliberation and Oversight", available at https://equineteurope.org/latest-developments-in-ai-equality/, accessed 11 November 2025.

PART II



6. Standards directives

6.1. General context

On 7 May 2024, two new directives were adopted to guarantee the effectiveness and independence of equality bodies and thus strengthen "the application of the principle of equal treatment".[312] They follow standard-setting efforts by Equinet,[313] the European Commission against Racism and Intolerance (ECRI)[314] and the European Commission.[315]

They establish harmonised, minimum standards:

- Directive 2024/1500 in the field of equal treatment and equal opportunities between women and men in matters of employment and occupation;
- Directive 2024/1499 in the field of equal treatment between persons irrespective of their racial or ethnic origin, equal treatment in matters of employment and occupation between persons irrespective of their religion or belief, disability,

312. Standards Directives, Art. 1.
313. Equinet (2016), *Developing Standards for Equality Bodies: An Equinet Working Paper*.
314. ECRI, General Policy Recommendation No. 2 (revised): *Equality Bodies to Combat Racism and Intolerance at National Level*, December 2017.
315. Commission Recommendation (EU) 2018/951 of 22 June 2018 on standards for equality bodies.

age or sexual orientation, equal treatment between women and men in matters of social security and in the access to and supply of goods and services.

The Standards Directives[316] can help EBs prevent and uncover discrimination in AI systems and they explicitly mention artificial intelligence and automated systems in their recitals:

> Devoting attention to the opportunities and risks presented by the use of automated systems, including artificial intelligence, is key. In particular, equality bodies should be equipped with appropriate human and technical resources. Those resources should, in particular, enable equality bodies to use automated systems for their work on the one hand and to assess such systems as regards their compliance with non-discrimination rules on the other hand. Where the equality body is part of a multi-mandate body, the resources necessary to carry out its equality mandate should be ensured.[317]

The Standards Directives must be transposed into national law by June 2026.

6.2. Changes to mandate and resourcing

6.2.1. An extension of the scope of the mandate

The Standards Directives extend the scope of the mandate of equality bodies. In particular, states that have not yet done so should extend the mandate of equality bodies to the grounds and the areas of life covered by the Gender Social Security Directive (79/7/EEC) and the Framework Employment Directive (2000/78/EC), giving them more competencies to cover the grounds of religion or belief, age, disability and sexual orientation in the area of employment, and sex and gender in the area of social security.[318] This is important because automated decision-making (ADM) systems in the area of social security have often been shown to be biased against women, as observed in Austria, France and Sweden.[319]

It is important to note that the scope of the Standards Directives is still limited to the grounds and areas of life covered by EU non-discrimination law.[320] However, the Standards Directives set minimum requirements, and the scope of the mandate of EBs can be broader at the national level.

In addition, the Standards Directives explicitly refer to the concept of intersectional discrimination in the context of the promotional and preventative activities of EBs. The Standards Directives provide that, in that context, EBs "can take into consideration

316. Equinet (2024) and the MOOC developed by the Council of Europe provide a comprehensive overview of the regulation.
317. Directive 2024/1500, Recital 21; and Directive 2024/1499, Recital 22.
318. Directive 2024/1499, Art. 1(2). In practice, the scope of many equality bodies already extends beyond the minimum requirements of EU discrimination law. See Equinet 2024: 24.
319. Allhutter D. et al. (2020), "Algorithmic profiling of job seekers in Austria: How austerity politics are made effective", *Frontiers in Big Data*, 3, available at https://doi.org/10.3389/fdata.2020.00005, accessed 11 November 2025; Romain et al. (2023); Amnesty International (2024), "Sweden: Authorities must discontinue discriminatory AI systems used by welfare agency", available at www.amnesty.org/en/latest/news/2024/11/sweden-authorities-must-discontinue-discriminatory-ai-systems-used-by-welfare-agency/, accessed 11 November 2025.
320. Directives 2024/1499 and 2024/1500, Recital 15.

specific situations of disadvantage resulting from intersectional discrimination".[321] Recitals of the directives also stress that "[i]n promoting equal treatment, preventing discrimination, collecting data on discrimination and assisting victims in accordance with this directive, it is important that equality bodies pay particular attention to intersectional discrimination."[322]

As AI systems, and specifically predictive analytics, are likely to give rise to intersectional forms of discrimination, it will be especially important for EBs to leverage these new powers, starting with promotional and preventative activities (Xenidis 2020).

6.2.2. An obligation to provide sufficient resources

Article 4 provides that states must "ensure that each equality body is provided with the human, technical and financial resources necessary to perform all its tasks and to exercise all its competences effectively." Aforementioned recitals explicitly link the issue of resources to tackling AI and ADM systems,[323] which may require new and additional technical and human resources.

What does this mean in practice?

► Human resources

Equality bodies must have "qualified staff … to carry out each of their tasks effectively",[324] "hire enough people with various and complementing sets of skills to perform all its duties and functions effectively and efficiently" and "offer competitive salaries and working conditions".[325] In the context of tackling AI and ADM systems, this means:

- Hiring technologists, including data scientists, and offering them competitive salaries, to build equality bodies' internal technical expertise. Alternatively, ensuring (via hiring or upskilling) that equality bodies are equipped internally to select and liaise with external technical experts, for example, researchers or experts within MSAs or other Article 77 bodies;
- Ensuring (via hiring or upskilling) that a sufficient number of legal and policy experts within equality bodies are knowledgeable about how ADM/AI systems work (with at least a basic understanding of technical issues) and about laws related to AI and ADM systems, in particular the AI Act; and
- Training the staff in charge of taking complaints on how to spot potential use of ADM/AI in complaints to equality bodies, and having adequate personnel able to examine complaints and ask follow-up questions if relevant.

The Netherlands Institute for Human Rights, after successfully conducting an *ex officio* investigation into possible systemic discrimination regarding the operation of the

321. Directives 2024/1499 and 2024/1500, Art. 5 (2).
322. Directive 2024/1499, Recital 16; 2024/1500, Recital 15, see also Directive (EU) 2023/970 (Equal Pay), Recital 15.
323. Directive 2024/1499, Recital 22; Directive 2024/1500, Recital 21.
324. Directive 2024/1499, Recital 21; Directive 2024/1500, Recital 20.
325. Equinet (2023), Measuring Standards for Equality Bodies: Indicators for Self-Assessment, Resources, Indicators 2.2.1.1 and 2.2.1.2.

childcare benefits system, plans to institutionalise a framework to handle technology-based data cases. In light of the amount of resources required for such a case, the Institute deems that ideally this handling should be done via training staff lawyers and hiring data scientists (Ilieva 2024: 73).

Many of the recommendations related to training and upskilling are in line with Article 20 of the Council of Europe Framework Convention, which pertains to digital literacy and skills, for "all segments of the population, including specific expert skills for those responsible for the identification, assessment, prevention and mitigation of risks posed by artificial intelligence systems."

▸ Technical resources

Technical resources can be considered the "third limb" of resourcing, beyond equality bodies' staff and funding (Equinet 2024). This includes premises, infrastructure and sufficient resources to meet their IT needs, including, among others, data collection systems and online consulting tools.[326] More specifically, in the context of tackling AI and ADM systems, this can mean:

- Ensuring that the complaint-handling IT system allows staff to easily flag and spot complaints where there is a suspicion that AI and ADM systems may have been used. Patterns between different complaints that could point to AI and ADM systems should be identifiable. This would help solve one of the practical hindrances of identifying discrimination stemming from AI and ADM systems, as raised by Unia: "the workload in complaint handling means that complaints filed in the technical system may not always make it easy to detect that multiple complaints about the same organisation have come in. Another area for improvement in the technical system is that, while it has a field to register whether an AI or ADM system was involved in the case, this field is buried deep in the forms that users must fill in to file a complaint and is therefore easily overlooked." (Xenidis 2025)
- Having appropriately secure IT infrastructure to run data analyses in the context of investigating AI and ADM systems. Considering the sensitive nature of complaints and the personal data of people, the use of Cloud services provided by technology companies from the USA cannot be considered secure IT infrastructure.[327]

With regards to the amount of resources required, Equinet stresses that "equality bodies themselves are the entity best placed to determine what resources are necessary to 'carry out each of their tasks effectively, within a reasonable time' based on their assessment of the problems which they are working to address and the activities and measures which they need to undertake" (Equinet 2024). Discussions on tools could also be tackled at a collective level for instance via Equinet, which has

326. Equinet (2023), Measuring Standards for Equality Bodies: Indicators for Self-Assessment.
327. See Cloud Act and Foreign Surveillance Intelligence Act in the USA. See also the recent reporting that Microsoft may have cancelled the email account of the International Criminal Court's chief prosector in reaction to an executive order from US President Trump. Molly Quell (2025), *Trump's sanctions on ICC prosecutor have halted tribunal's work*, available at https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3, accessed 11 November 2025.

a platform for such discussions through the multi-annual Standards Project, which involves annual meetings of interested members to discuss all aspects related to the resources, independence and powers of EBs.

The Standards Directives indicate that equality bodies can use AI and ADM tools to carry out their mandate. While this can enable equality bodies to be more efficient (for instance, by detecting patterns between different complaints), these tools should be carefully procured, carefully evaluated and carefully deployed with instructions for their use.

6.2.3. Role of equality bodies regarding their mandate and resourcing, in the context of ADM and AI systems

Regarding their mandate, and in particular the concept of intersectional discrimination

- Leverage the references to intersectionality to tackle the often-intersectional discriminations potentially embedded in ADM and AI systems, when conducting research and communication.
- Advocate to extend the mandate of equality bodies to cover grounds beyond EU discrimination law.
- Advocate for a broader application of intersectionality, as currently the directives confine "intersection work" to prevention and promotion activities.

Regarding resourcing

- Evaluate the human and technical resources required to tackle AI/ADM systems.
- Advocate for such human and technical resources to be made available, including in the context of the transposition of the Standards Directives.
- Identify the kinds of technical tools that will be useful and collaborate at an international level on procuring or developing them. For example, in the context of complaint-handling software, prioritise open-source software that can be used by different EBs and be modified if necessary, based on specific needs. Another example could be the development of tools for investigations that can be used by multiple EBs instead of each developing the same from scratch.[328]

6.3. Changes to powers

The Standards Directives set harmonised, minimum standards in terms of what powers equality bodies have, and give them new tools to address algorithmic discrimination, on two fronts:

- Powers to promote equal treatment and prevent discrimination,

328. Similar initiatives can be observed in areas such as data protection. See EDPB website auditing tool, available at www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/edpb-website-auditing-tool_en, accessed 11 November 2025.

- Powers to investigate and redress.

Section 6.3. looks at what the directives' provisions mean in the context of AI and ADM systems.

The powers laid down by the Standards Directives are linked to obligations introduced by the Council of Europe Framework Convention to set up or maintain remedies,[329] safeguards[330] and oversight mechanisms.[331] These obligations include "continuous monitoring of current developing capabilities and auditing, public consultations and engagement, risk and impact management frameworks and human rights impact assessment frameworks, technical standards, as well as education and awareness programmes."[332]

6.3.1. Promotion of equal treatment and prevention of discrimination

The Standards Directives introducing the "promotion of equal treatment" as a competence of EBs "requires States to enable Equality Bodies to move from the reactive, remedial approach to discrimination towards a proactive, preventative and promotional approach" (Equinet 2024). This shift is critical in the context of automated decision making and AI systems, where lack of awareness and lack of information are two challenges encountered in preventing and mediating discrimination.

Awareness-raising

Article 5 (1) of the Standards Directives introduces a new general power of awareness-raising for equality bodies. In the context of AI and ADM systems, this means raising awareness around the risks of discrimination by AI and ADM systems, around existing non-discrimination rights and around potential recourse and redress routes, including the existence of equality bodies. This awareness-raising should be accessible,[333] and particular attention should be paid to people in vulnerable situations who are often the target of AI and ADM systems. This awareness-raising sits alongside the requirements of the MSA to pay particular attention to AI systems presenting a risk to vulnerable groups and to inform the EB where a risk to fundamental rights is identified.[334]

329. Council of Europe Framework Convention, Art. 14.
330. Council of Europe Framework Convention, Art. 15.
331. Council of Europe Framework Convention, Art. 9.
332. Council of Europe (2024), Explanatory report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, paragraph 63.
333. Standards Directives, Art. 12.
334. AI Act, Art. 79 (2).

Proactive prevention

Article 5 (2) of the Standards Directives marks another shift from the Equality Directives[335] by empowering equality bodies to take a proactive role in preventing discrimination. Actions to do so include, but are not limited to, "promoting positive action and gender mainstreaming among public and private entities, providing them with relevant training, advice and support, engaging in public debate, communicating with relevant stakeholders, including the social partners, and promoting the exchange of good practices".[336]

Read together with Article 4 of the Standards Directives on resources, this means that equality bodies should have sufficient resources to conduct such activities.

Consultation

Article 15 of the Standards Directives requires states to consult with equality bodies in the development and implementation of laws, policies, procedures and programmes related to the rights and obligations derived from the Equality Directives. This article could be interpreted narrowly, as restricted to equality law and policy. However, the intention of the consultation as set out in recitals is to enable equality bodies to contribute to "equality mainstreaming".[337] As such, equality bodies should be involved in digital law and policies, including AI Act implementation or national legislation on specific uses of AI and ADM systems.

This provision also echoes Article 19 of the Council of Europe Framework Convention, which provides for public and multistakeholder consultations to be conducted around "important questions raised in relation to artificial intelligence systems".

335. In this report, "Equality Directives" refers to key directives enacted under EU law: Council Directive of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin (Directive 2000/43/EC); Council Directive of 27 November 2000 establishing a general framework for equal treatment in employment and occupation (Directive 2000/78/EC); Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) (Directive 2006/54/EC); Council Directive of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services (Directive 2004/113/EC); Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010 on the application of the principle of equal treatment between men and women engaged in an activity in a self-employed capacity and repealing Council Directive 86/613/EEC (Directive 2010/41/EU); Directive (EU) 2023/970 of the European Parliament and of the Council of 10 May 2023 to strengthen the application of the principle of equal pay for equal work or work of equal value between men and women through pay transparency and enforcement mechanisms (Directive 2023/970/EU); Council Directive of 19 December 1978 on the progressive implementation of the principle of equal treatment for men and women in matters of social security (Directive 79/7/EEC).
336. Standards Directives, Art 5 (2).
337. See Equinet (2024) for a similar analysis of the provision.

Collection of data, access to equality data and production of reports

Article 16 of the Standards Directives gives equality bodies the power to collect data (with an emphasis on it being disaggregated),[338] conduct surveys,[339] access statistics collected by others[340] and make recommendations on what equality data to collect.[341] This power is explicitly tied to the reporting obligations of equality bodies, which include reports on "the state of equal treatment … in the State".[342] The recitals also give more details about the purposes of data collection, which include "quantifying discrimination" and "evaluating the implementation of equality legislation" as well as "contributing to evidence-based policymaking."

These powers can be applied to the field of AI/ADM systems, especially to reach a better understanding of the state of deployment of AI/ADM systems by public agencies.

Data protection legislation should not be viewed as an obstacle to equality data collection (EU Agency for Fundamental Rights 2021). The GDPR allows for the collection and processing of special categories of personal data under certain conditions, including for statistical or research purposes, in Article 9 (2) (a), (g) and (j). The Subgroup on Equality Data of the European Commission's High Level Group on Non-discrimination, Equality and Diversity has adopted different sets of guidelines and published guidance notes on the collection and use of equality data. In March 2025, the subgroup published a document on "Collecting and using equality data in full compliance with EU General Data Protection Regulation and national data protection rules", highlighting best practices from several member states of the European Union and experiences shared by the Fundamental Rights Agency and Subgroup members (Subgroup on Equality Data 2025; see also Ilieva 2024).

6.3.2. Role of equality bodies regarding the promotion of equal treatment and the prevention of discrimination

Awareness raising

- Raise awareness about the new rights of affected people: as part of their awareness-raising powers, equality bodies should raise awareness about the rights of affected people pertaining to AI systems such as the right to lodge a complaint, and the right to explanation under the AI Act and EU data protection law.
- Raise awareness of risks to fundamental rights, using existing evidence on AI systems at national and European level.
- Engage with the media and journalists to encourage new investigations and increased reporting on these issues.

338. Standards Directives, Art. 16 (1).
339. Standards Directives, Art. 16 (2).
340. Standards Directives, Art. 16 (3).
341. Standards Directives, Art. 16 (4).
342. Standards Directives, Art. 17 (c).

- Collaborate with existing initiatives on awareness-raising: awareness-raising for the general public can entail going where the public already is. For instance, ongoing European project AlgoLit,[343] which works on algorithmic mediation, aims to work with mediators and social workers to raise awareness about issues around AI and ADM systems in the public sector. Equality bodies could look to partner with such initiatives to make sure discrimination risks are discussed enough in such programmes, and to promote the role of equality bodies in using non-discrimination rights. This is especially important because training pertaining to challenges around artificial intelligence often takes an "ethics-based" approach rather than one based on fundamental rights (Xenidis 2025).
- Monitor strategies by providers and deployers of AI systems, including "de-risking" (Xenidis 2025) and "ethics washing" (Equinet 2025) strategies used by providers and deployers of AI/ADM systems (e.g. self-exempting from the high-risk regime or not considering certain systems are prohibited under Article 5).

Proactive prevention

- Deliver training to private and public deployers of AI/ADM systems (including public government agencies), as well as legislative and judiciary institutions. For instance, the Council of Europe offer a course "AI and anti-discrimination" in several national contexts, in co-operation with equality bodies (such as the Finnish Non-Discrimination Ombudsman in Finland, Defender of Rights in France, Commission for Citizenship and Gender Equality in Portugal, and Unia in Belgium).
- Promote inclusion and equality for science, technology, engineering and mathematics (STEM) disciplines.

Collection of data, access to equality data and production of reports

- Identify AI/ADM discrimination and implementation of the AI Act as a priority area for public reporting.
- Write reports based on national reviews of the use of AI/ADM systems in a particular field, focusing on areas considered high-risk under Annex III of the AI Act. These desktop reviews can leverage the information available in the EU database of high-risk AI systems, but go beyond and include an analysis of systems not considered high-risk or systems not featured in the public database (such as law enforcement, migration and border controls), in order to demonstrate the importance of not being limited to high-risk AI systems. These reports can also be conducted across several countries, to identify common patterns and trends.
- Conduct surveys on public perceptions around AI and ADM systems and understanding of discrimination risks. Ideally, this could be done across several countries to compare contexts and responses. In Sweden, the Equality

  Ombudsman was given an assignment by the Swedish Government to improve the knowledge of risks of discrimination in the use of artificial intelligence and other types of automated decision making in professional contexts

343. FARI (2025), "ALGO-LIT (Erasmus+ Project)", available at www.fari.brussels/research-and-innovation/project/algo-lit, accessed 11 November 2025.

(Ministry of Employment, Government decision 07/06/2022, A2022/00877), which resulted in a report published in November 2023. The report assessed the level of knowledge among employers regarding their use of artificial intelligence, and showed that employers were not aware they were already using AI and other types of automated decision making.[344]

- Work closely with statistics agencies to ensure disaggregated data are being collected and are available to use to technically analyse biases in AI/ADM systems.

6.3.3. Access to justice and remedy

The Standards Directives answer the challenge of current disparities between equality bodies in how they promote access to justice, by giving explicit powers to equality bodies to act in support of victims and to facilitate access to justice. These powers entail assistance to victims,[345] alternative dispute resolution,[346] conducting inquiries,[347] issuing opinions and decisions,[348] and pursuing litigation.[349] This section dives into specific provisions.

Assistance to victims and ability to receive complaints

Article 6 of the Standards Directives provides that "Equality bodies must inform victims about: the legal framework, including advice targeted to their specific situation; the services offered by the equality body and related procedural aspects; available remedies, including the possibility to pursue the case before the courts; the confidentiality rules applicable and the protection of personal data; and the possibility of obtaining psychological or other support from other bodies or organisations."

In the context of AI/ADM systems, this entails informing victims about their rights under the AI Act and under EU data protection law.

Inquiries

Article 8 of the Standards Directives empowers equality bodies to conduct inquiries either following a complaint or *suo moto* (of their own motion, to investigate potential violations of the right to equal treatment). As underlined by ECRI, "these inquiry activities are important in uncovering and establishing the evidence of discrimination or intolerance that ultimately enables these experiences to be redressed".[350] This latter mode is especially important in the context of AI/ADM systems, which are persistently opaque and unknown.

344. Diskriminerings ombudsmannen (2023), "AI och risker för disrkiminering I arbetslivet", available at: www.do.se/rattsfall-beslut-lagar-stodmaterial/publikationer/2023/ai-och-risker-for-diskriminering-i-arbetslivet [in Swedish], accessed 11 November 2025.
345. Standards Directives, Art. 6.
346. Standards Directives, Art. 7.
347. Standards Directives, Art. 8.
348. Standards Directives, Art. 9.
349. Standards Directives, Art. 10.
350. ECRI, General Policy Recommendation No. 2r.

Article 8 (2) of the Standards Directives gives equality bodies effective access to information and documents and is relevant with respect to the AI Act, for two reasons:

- For equality bodies that are not (yet) Article 77 Bodies, this provision could be explored as a way to access information and documents covered by confidentiality rules, including technical documentation or full versions of fundamental rights impact assessments.
- The right to access information and documents is often hindered by the difficulty of accessing understandable information. Because the AI Act provides that information created under the Act has to be accessible, equality bodies can leverage this and focus on requesting access information and documents produced in the context of the Act, and thus ensure they obtain information that will be understandable and useful (provided the accessibility requirement is clarified and respected).

Article 8 (3) of the Standards Directives allows equality bodies to entrust another competent body, in accordance with national law and practice, with the powers referred to above. This article opens up the possibility of co-operation but not to supplant equality bodies, as the wording of the article suggests that this power will be exerted by another body "in addition to" and not "instead of".[351] This provision can be explored as a way to develop formal co-operation with other bodies.

Opinions and decisions

Article 9 of the Standards Directives also gives levers to further public understanding and knowledge of AI/ADM systems in the public sector. It provides that "where appropriate, both non-binding opinions and binding decisions shall include specific measures to remedy any breach of the principle of equal treatment found and to prevent further occurrences", and that equality bodies "shall publish at least a summary of those of their opinions and decisions which they consider to be of particular relevance".

Litigation

Article 10 of the Standards Directives gives equality bodies the non-transferrable power to act in court proceedings, which should include "at least one of the following: the right to initiate court proceedings on behalf of one or several victims; the right to participate in court proceedings in support of one or several victims; or the right to initiate court proceedings in its own name, in order to defend the public interest".

Litigation around AI and ADM systems is still scarce, and initiatives or support from equality bodies in this area are needed.

351. See Equinet (2024) p. 84 for a similar analysis of the provision.

6.3.4. Role of equality bodies regarding access to justice and remedy

Assistance to victims and ability to receive complaints

- Ensure that equality bodies' staff who are responsible for assistance to victims are up to date on AI regulation, to adequately inform victims of their rights.
- Co-ordinate with market surveillance authorities (MSAs) to ensure that victims who file complaints with MSAs are encouraged to file complaints with EBs.

Inquiries

- Conduct *suo moto* inquiries on specific AI/ADM systems.
- Explore the national transposition of Article 8 of the Standards Directives as a way to access information produced under the AI Act.

Opinions and decisions

- In opinions and decisions, propose measures aimed at spreading knowledge about the systems. For instance, the Court of Bologna, in ruling no. 2949/2020 of 31 December 2020, after sentencing Deliveroo to pay 50 000 euros in favour of the plaintiff, ordered the publication of the text of the sentence in a national newspaper with the aim of guaranteeing maximum visibility.[352]
- Systematically publish opinions and decisions pertaining to AI/ADM systems, in order to make knowledge around their uses and risks public.

Litigation

- Act in court proceedings on cases pertaining to AI/ADM systems.

352. Fernandez Sánchez S. F. (2021), "Frank, el algoritmo consciente de Deliveroo. Comentario a la Sentencia del Tribunal de Bolonia 2949/2020, de 31 de diciembre", *Revista De Trabajo Y Seguridad Social CEF*, pp. 179-93, available at https://doi.org/10.51302/rtss.2021.2374 [in Spanish], accessed 11 November 2025.






7. Thematic focus

This section covers use of AI in five thematic areas based on most common sectors covered by equality bodies and NHRS' work: law enforcement, migration, asylum, and border control; education; employment, and social security and employment support services. Each thematic focus area addresses examples of AI use and lists relevant EU AI Act articles to consider for that sector.

7.1. Thematic focus: Law enforcement, migration, asylum and border control

7.1.1. Context

Uses of AI systems in law enforcement, migration, asylum and border control

AI and ADM are used in a range of contexts in the areas of law enforcement, migration, asylum and border control.

In law enforcement, previous research has highlighted uses ranging from mapping crime patterns based on past crime data, detecting illicit objects from satellite images,

detecting online hate speech,[353] deciding on temporary releases in prisons[354] or assessing risks with regard to gender-based violence.[355]

Image recognition and biometrics are also widely used. In Finland, the police can use image recognition to identify non-biometric features, e.g. clothes, car plates (Xenidis 2025). France made use of remote video surveillance during the Paris 2024 Summer Olympic and Paralympic Games.[356] The facial recognition application commercialised by US company Clearview AI, which relied on untargeted scraping of facial images on social media, was said to be used by several law enforcement authorities throughout Europe (Veld et al. 2020).

Research shows that face recognition technologies can exhibit problematic discriminatory biases.[357] Even when AI and ADM systems themselves are not reported to be biased, their deployment is criticised for disproportionately targeting and surveilling minorities and performing ethnic profiling. This can happen when over-surveillance of locations or populations feeds back into predictive tools and reinforces mass surveillance or risk-scoring of these communities. It can also happen when those systems are used in different ways depending on the person's skin colour, for example police officers interpreting the results of a system differently depending on the skin colour of the suspect.

AI and ADM systems are also used in migration, asylum and border control, in different areas (Dumbrava 2025, Jones et al. 2023, McGregor 2023). In 2023, a report under the Algorithmic Fairness for Asylum Seekers and Refugees (AFAR) project mapped the use of AI technologies in migration and asylum fields in Europe, and identified the following uses: forecasting of future immigration and displacement; risk assessments and triaging; processing of visas, travel authorisations and citizenship applications; document verification for identity verification and fraud detection; speech recognition (to establish asylum applicants' country of origin or in assessment of language proficiency in citizenship applications); electronic monitoring (such

353. See European Union Agency for Fundamental Rights (2022), *Bias in Algorithms: Artificial Intelligence and Discrimination,* Luxembourg: Publications Office of the European Union, pp. 28-49.
354. García T. et al. (2025), "Spanish prisons use a 30-year-old algorithm to decide on temporary releases", *Civio*, available at https://civio.es/justicia/2025/03/12/spanish-prisons-use-a-30-year-old-algorithm-to-decide-on-temporary-releases/, accessed 11 November 2025.
355. Public Sector Tech Watch (2025), "Viogen 5.0: discovering Spain's risk assessment system of gender-based violence", available at https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/viogen-50-discovering-spains-risk-assessment-system-gender-based-violence, accessed 11 November 2025.
356. Ministère de l'Intérieur (2025), *Expérimentation, en temps réel, de caméras « augmentées »*, available at www.interieur.gouv.fr/actualites/actualites-du-ministere/experimentation-en-temps-reel-de-cameras-augmentees, accessed 11 November 2025.
357. The CSO Liberty attacked a face recognition application used by South Wales Police, *inter alia* for discrimination on grounds of sex and/or race because it produced a higher rate of positive matches for female faces and/or for black and minority ethnic faces. See the subsequent decision of the Court of Appeal of England and Wales in *R (Bridges) v. Chief Constable of South Wales Police* ([2020] EWCA Civ 1058) highlighting that the South Wales Police "Equality Impact Assessment was obviously inadequate and was based on an error of law (failing to recognise the risk of indirect discrimination)" and that its "subsequent approach to assessing possible indirect discrimination arising from the use of AFR is flawed". See Xenidis 2025.

as ankle tags); distribution of welfare benefits; matching tools (for instance, in the allocation of reception centres); and mobile phone data extraction for verification of identity and narratives (Ozkul 2023).

Such uses pose risks to fundamental rights, partly due to the inaccuracies, biases and stereotypes that can be embedded in the tools, the impacts on fairness and due process, and issues of privacy and data protection (Dumbrava 2025, McGregor 2023). In 2020, following a legal challenge by Foxglove and the Joint Council for the Welfare of Immigrants, the United Kingdom's Home Office stopped using a streaming algorithm used in visa applications, that assigned a "red" traffic-light risk score to applicants from specific nationalities (BBC 2020). A case study by Equinet on the United Kingdom's use of an ADM system to determine eligibility for the Settled Status set up to regularise the immigration status of EU, European Economic Area (EEA), Swiss nationals and their families living in the UK after Brexit highlighted several concerns with the system, namely opacity, uncertainty about human discretion and the lack of interrogation of specific databases, leading to detrimental effects for women (Allen and Masters 2020). In April 2024, the Greek Data Protection Authority imposed a €175 000 fine on the Ministry of Migration and Asylum for GDPR violations in the development and implementation of the Centaur and Hyperion programmes in reception and accommodation facilities for asylum seekers; Centaur was a partly automated surveillance system to predict and flag "threats" using, *inter alia*, CCTV and drones, and Hyperion was an entry/exit control system (Hellenic Data Protection Authority 2024).

A wide range of exemptions

One characteristic of the AI Act is that it grants AI systems used in law enforcement, migration, asylum and border control a wide range of exemptions. For instance, certain AI systems prohibited for certain uses are only considered high-risk in the context of law enforcement, such as the prohibition on biometric categorisation.[358] In addition, they are subjected to lesser registration and publicity obligations than other high-risk AI systems (see Article 49), leading to ongoing concerns regarding transparency.

Equality body teams focused on law enforcement should have a particular look at the following provisions of the AI Act.

7.1.2. Prohibited AI systems

Article 5: Prohibited AI systems

- Article 5 (1) (c) on social scoring pertaining to classification and evaluation systems. For instance, evaluation and classification could happen in the context of incarceration or refugee camps, on the basis of video surveillance images. Such practices could be considered social scoring under certain circumstances.
- Article 5 (1) (d) on risk assessment of committing a criminal offence in certain circumstances, which covers some uses of predictive policing.
- Article 5 (1) (e) on scraping to build or expand facial recognition databases.
- Article 5 (1) (h) on remote biometric identification for law enforcement purposes.

358. AI Act, Art. 5 (1) (g) and Annex III (1) (b).

Several prohibitions do not encompass uses in law enforcement, which are however considered high-risk under Annex III:

- Article 5 (1) (g): the prohibition on biometric categorisation does not include uses in law enforcement, which are however considered high-risk under Annex III (1) (b).
- Article 5 (1) (f) on emotion recognition does not apply to uses in law enforcement, migration, and border control. However, it is considered high-risk under Annex III (1) (c). For instance, emotion recognition can be used as part of "lie detectors" during the interrogation of suspects.

7.1.3. High-risk AI systems under Annex III

- Annex III (1) on biometrics:
  - Remote biometric identification systems except those whose sole purpose "is to confirm that a specific natural person is the person he or she claims to be";[359]
  - For biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics;[360]
  - For emotion recognition;[361]
- Annex III (1) (6) on uses "by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities". Such uses encompass:
  - Assessing "the risk of a natural person becoming the victim of criminal offences". One such example could be the aforementioned VioGen system used in Spain in the context of gender-based violence;[362]
  - "Polygraphs or similar tools";[363]
  - "To evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences";[364]
  - Offence or re-offence risk assessments which are "not solely on the basis of the profiling of natural persons" (reminder: risk assessments based solely on the basis of profiling are prohibited under Article 5 (1) (d)), or "to assess personality traits and characteristics or past criminal behaviour of natural persons or groups";[365]
  - "For the profiling of natural persons … in the course of the detection, investigation or prosecution of criminal offences".[366]
- Annex III (1) (7) on migration, asylum and border control management:
  - "Polygraphs or similar tools";[367]

359. AI Act, Annex III (1) (a).
360. AI Act, Annex III (1) (b).
361. AI Act, Annex III (1) (c).
362. AI Act, Annex III (6) (a).
363. AI Act, Annex III (6) (b).
364. AI Act, Annex III (6) (c).
365. AI Act, Annex III (6) (d).
366. AI Act, Annex III (6) (e).
367. AI Act, Annex III (7) (a).

- "Assess a risk, including a security risk, a risk of irregular migration or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State";[368]
- "The examination of applications for asylum, visa or residence permits and for associated complaints with regard to the eligibility of the natural persons applying for a status, including related assessments of the reliability of evidence;"[369]
- "Detecting, recognising or identifying natural persons, with the exception of the verification of travel documents".[370]

Reminder: all of these uses are permitted "in so far as their use is permitted under relevant Union or national law." Where uses infringe human rights and/or are discriminatory, this will require a consideration of whether the measures taken are proportionate and necessary in a democratic society. The European Court of Human Rights has previously considered that the use of new technologies in policing could not be regarded as necessary in a democratic society in the context of DNA profiling[371] and live facial recognition[372]. The Court in *S. and Marper* noted:

> The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests … The Court considers that any state claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.

For some AI systems, there is a possibility of providers self-excluding from the high-risk regime as per Article 6 (3). An example would be AI translation tools to examine applications for asylum. This tool could be considered a "preparatory task" to an assessment, and therefore fall outside the scope of high-risk AI systems. The lesser performance of these tools on certain languages[373] makes them likely to have discriminatory effects on individuals speaking certain languages.

7.1.4. Registration obligations and the EU AI Act database

High-risk AI systems used in law enforcement, migration, asylum and border control are subject to lesser registration obligations under the AI Act. In particular, their uses will be registered in the non-public version of the EU database, and the summaries of FRIAs will not be registered in the database.

It is recommended that equality bodies and NHRS prioritise setting up mechanisms to monitor such uses in an ongoing manner, through using their powers as Article 77 bodies (if applicable) or through co-operation with market surveillance authorities.

368. AI Act, Annex III (7) (b).
369. AI Act, Annex III (7) (c).
370. AI Act, Annex III (7) (d).
371. *S. and Marper v. United Kingdom*, Application Nos. 30562/04 and 30566/04 (2008), see https://hudoc.echr.coe.int/fre?i=001-90051, accessed 11 November 2025.
372. *Glukhin v. Russia*, Application No. 11519/20 (2023), see https://hudoc.echr.coe.int/eng?i=001-225655, accessed 11 November 2025.
373. Bhuiyan J. (2023), "Lost in AI translation: growing reliance on language apps jeopardizes some asylum applications", *The Guardian*, available at www.theguardian.com/us-news/2023/sep/07/asylum-seekers-ai-translation-apps, accessed 11 November 2025.

7.2. Thematic focus: Education

7.2.1. Context

AI and ADM systems can be used in various areas of education, ranging from admissions (see the Parcousup system used in France to rank candidates and match demand and supply in higher education)[374] or evaluating learning outcomes (for instance in the context of secondary school final exams, in the UK in 2020)[375] to administrative purposes, to learning in the classroom and to student monitoring. There is an increased focus on developing technologies for students with special educational needs and management systems designed to detect everything from suicide risks to terrorist sympathies. In 2023, the Dutch Institute for Human Rights ruled that a Dutch university did not discriminate against a student on the basis of race by using anti-cheating software.[376] The student argued that the software was discriminatory due to facial recognition performing less well on students with dark skin, due to technical limitations.

Other technologies are used in educational environments. In France, the data protection authority opposed the experimentation with facial recognition at the entrance of two secondary educational establishments, on the grounds that such use of facial recognition was neither proportionate nor necessary with regard to data protection law.[377] Facial recognition used in schools in Sweden was found to breach data protection rights and wider rights to privacy and integrity of the person.[378] Similarly, a requirement to provide biometrics for identification and lunch payment was found illegal in Poland on the grounds there was no legal basis for the measures.[379]

7.2.2. Prohibited uses

The following prohibited uses are of particular interest in the context of education:

- Article 5 (1) (a) and (b) on deceptive techniques,
- Article 5(1)(c) on social scoring,
- Article 5 (1) (f), which prohibits emotion recognition in education institutions,

374. AI Law Hub (2020), *French Parcoursup decision*, available at https://ai-lawhub.com/2020/04/16/french-parcoursup-decision/, accessed 11 November 2025.
375. Office for Statistics Regulation Authority (2021), *Ensuring statistical models command public confidence: Learning lessons from the approach to developing models for awarding grades in the UK in 2020*, available at https://osr.statisticsauthority.gov.uk/publication/ensuring-statistical-models-command-public-confidence/, accessed 11 November 2025
376. Racism and Technology Center (2023), "Judgement of the Dutch Institute for Human Rights shows how difficult it is to legally prove algorithmic discrimination", available at https://racismandtechnology.center/2023/10/17/judgement-of-the-dutch-institute-for-human-rights-shows-how-difficult-it-is-to-legally-prove-algorithmic-discrimination/, accessed 11 November 2025.
377. CNIL (2022), "Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position", available at www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position, accessed 11 November 2025.
378. KamR Stockholm, Case No. 5888-20, available at: https://gdprhub.eu/index.php?title=KamR_Stockholm_-_Case_No._5888-20#, accessed 11 November 2025.
379. EDPB (5 March 2020), "Fine for processing student's fingerprints imposed on a school". See https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en, accessed 11 November 2025.

- Article 5 (1) (g), which prohibits biometric categorisation "to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation".

7.2.3. High-risk AI systems

- Annex III (1) on biometrics, and, in particular:
  - Annex III (1) (a) on remote biometric identification systems;[380]
  - Annex III (1) (b) which pertains to biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics (and is a broader category than that of the practices prohibited by Article 5(1)(g)).
- Annex III (3) on education and vocational training, which covers:
  - "AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels";
  - "AI systems intended to be used to evaluate learning outcomes";
  - "AI systems intended to be used for the purpose of assessing the appropriate level of education that an individual will receive or will be able to access";
  - "AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests".

7.2.4. Transparency requirements

- Article 50 on transparency requirements is particularly relevant for the educational context, where generative AI and educational technologies are increasingly used in the classroom to directly interact with students.

7.2.5. Registration requirements

High-risk AI systems in the area of education will be registered in the public version of the database by providers and deployers. The information registered will include the summaries of FRIAs conducted by the deployers.

7.3. Thematic focus: Employment

7.3.1. Context

AI and ADM systems can be used at different stages of the recruiting and employment process, ranging from writing job advertisements and targeting who they are sent to, to the recruitment process (for instance, to process CVs, conduct interviews or match applicants with jobs) or management and performance review.[381] In 2024, 98.4% of Fortune 500 companies used AI or data-driven systems at the stage of hiring.[382]

380. AI Act, Annex III (1).
381. Simons J. (2020), Machine learning: case studies, Institute for the Future of Work, available at www.ifow.org/publications/2020/2/24/machine-learning-case-studies, accessed 11 November 2025.
382. Jobscan (2024), "2024 Applicant Tracking System (ATS) usage report: key shifts and strategies for job seekers", available at www.jobscan.co/blog/fortune-500-use-applicant-tracking-systems, accessed 11 November 2025.

Often, AI systems are used by employers under human supervision. This affirmation should be examined closely, as human oversight needs to fulfil certain conditions to be effective and is never, on its own, an appropriate safeguard for fundamental rights.[383]

7.3.2. Prohibited practices

- Article 5 (1) (f) on emotion recognition in the workplace, which could happen during the recruitment process or to monitor an employee's emotions.
- Article 5 (1) (g) on biometric categorisation "to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation", which recruiters or employers could be interested in.

7.3.3. High-risk practices

- Annex III (1) on biometrics, and, in particular:
  - Annex III (1) (a) on remote biometric identification systems;
  - Annex III (1) (b) which pertains to biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics (and is a broader category than that of the practices prohibited by Article 5(1) (g).
- Annex III (4) on areas of employment, workers' management and access to self-employment. This covers systems for:
  - "The recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates";[384]
  - "Decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, [and decisions] to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships."

It is likely that some of the systems used in these areas will not be considered high-risk by providers under Article 6(3). For example, an AI system used to assess CVs and motivation letters could be considered a "preparatory task to an assessment".

7.3.4. Transparency requirements

- Article 50 on transparency requirements is particularly relevant for the employment context, in particular at the recruitment stage, where more and more AI tools are used in the hiring process.

7.3.5. Registration and information obligations

Article 26 (7) provides for an information obligation of deployers who are employers. Before they put into service or use a high-risk AI system at the workplace, they "shall

383. Green B. (2022), "The flaws of policies requiring human oversight of government algorithms", *Computer Law & Security Review*, 45, p. 105681, available at https://doi.org/10.1016/j.clsr.2022.105681, accessed 11 November 2025.
384. AI Act, Annex III (4) (a).

inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system".[385]

Providers of AI systems pertaining to employment, workers' management and access to self-employment (Annex III (4)) have an obligation to register their systems in the EU database. However, this obligation is not present for deployers who are private entities. In addition, deployers do not have an obligation to conduct a fundamental rights impact assessment. This absence of obligations risks creating a lack of visibility of the systems in use and their impacts, including in large companies.

7.4. Thematic focus: Social security and employment support services

7.4.1. Context

Numerous public agencies use AI and ADM systems in the areas of social security and employment support services, to determine eligibility, calculate benefits, target controls in the context of detection of fraud and errors, and distribute resources to recipients. AI systems are offered to social security caseworkers and jobseeker-support professionals, and AI-based chatbots are increasingly used to interact with recipients. France's employment agency France Travail has developed several AI systems as part of its Intelligence Emploi programme, including MatchFT, a chatbot to send job offers to potential candidates and check their interest and eligibility, and ChatFT, a chatbot used by caseworkers to retrieve information from the agency's databases (info.gouv.fr 2025). The IA-NAVIGATE project, a collaboration between FARI (AI for the Common Good Institute) and the Public Employment Agency in Brussels, Actiris, surveyed the use of AI tools by jobseeker-support professionals in Brussels, and found that around 60% of them had already used AI tools for their work, mostly for writing reports, designing workshops, editing CVs and preparing for job interviews. It also revealed that over 80% of them had not received any guidelines from the entities they worked for on using AI tools (Xenidis 2025).

Some of these systems have already been found to be discriminatory. For example, in the Netherlands, a system used to predict fraud was found to have discriminated against recipients on grounds of race, ethnic origin and citizenship.[386] The Austrian employment agency developed the AMS algorithm to predict chances of employment, in order to allocate support resources to job seekers. The prototype was shown to be discriminatory against women (in particular single mothers) and job seekers with a migration background.[387] In Poland, a system used

385. AI Act, Art. 26(7).
386. De Rechtspraak (13 February 2019) "SyRI legislation in breach of European Convention on Human Rights", *De Rechtspraak*, , available at www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Den-Haag/Nieuws/Paginas/SyRI-legislation-in-breach-of-European-Convention-on-Human-Rights.aspx, accessed 11 November 2025. The SyRI system was also deemed to have disproportionately interfered with end users' right to privacy because it processed personal data from various government agencies.
387. Allhutter D et al. (2020) "Algorithmic profiling of job seekers in Austria: How austerity politics are made effective", *Frontiers in Big Data*, 3, available at https://doi.org/10.3389/fdata.2020.00005, accessed 11 November 2025.

by the employment agency was eventually abandoned because it was deemed unconstitutional.[388] ADM and AI systems are or were also used to control welfare beneficiaries in multiple countries such as France, the Netherlands, Denmark and Belgium – with discriminatory outcomes.[389]

A case has been brought in front of the French Council of State by CSOs against a risk-scoring system used by the French welfare agency to predict risks of fraud and errors and to target controls.[390] The CSOs have pointed to, *inter alia*, discrimination based on sex, family status, age and disability. The litigants asked the Council of State to refer questions to the CJEU, including in relation to indirect algorithmic discrimination.[391] The question of indirect discrimination and substantive equality is particularly prevalent in social security systems.[392]

Another key point will be to evaluate which systems fall under the definition of an AI system in the AI Act, as many systems in social security remain relatively simple technically, despite posing significant risk for fundamental rights.

7.4.2. Prohibited AI systems

- Article 5 (1) (c) on social scoring is a crucial provision to consider in the area of social security and employment support services, where many systems to control or orient beneficiaries are deployed (see above).
- Article 5 (1) (f) on emotion recognition in the workplace, which could happen during the recruitment process.

388. Szymielewicz K. et al. (2015), "Profiling the unemployed in Poland: social and political implications of algorithmic decision making", Fundacja Panoptykon, 2015, available at: https://en.panoptykon.org/profiling-unemployed-poland-report, accessed 31 March 2026.
389. Romain et al. (2023); Mehrotra D. et al. (2023), "Inside the suspicion machine", *WIRED*, available at www.wired.com/story/welfare-state-algorithms/, accessed 11 November 2025; Geiger G. (2023), "How Denmark's welfare state became a surveillance nightmare", *WIRED*, 7 March available at www.wired.com/story/algorithms-welfare-state-politics/, accessed 11 November 2025; Amnesty International (2024), "Denmark: AI-powered welfare system fuels mass surveillance and risks discriminating against marginalized groups – report", available at www.amnesty.org/en/latest/news/2024/11/denmark-ai-powered-welfare-system-fuels-mass-surveillance-and-risks-discriminating-against-marginalized-groups-report/, accessed 11 November 2025; Degrave E. (2020), "The use of secret algorithms to combat social fraud in Belgium", *European Review of Digital Administration & Law* 1-2: 167-78.
390. Amnesty International (2024), *France: CNAF State Council Complaint*, available at www.amnesty.org/fr/documents/eur21/8795/2024/en/, accessed 11 November 2025.
391. The question reads: "Does the processing of personal data, the controller of which is a public social administration entrusted with a public service mission, the purpose of which is to establish a risk score for each user of the public service in order to target checks by the administration, not constitute indirect discrimination within the meaning of Directive 2000/43/EC of 29 June 2000 and Council Directive 79/7/EEC of 19 December 1978? read in the light of Articles 20 and 21 of the Charter, insofar as the introduction of this treatment has resulted in a significant increase in checks on people under the age of 30, students, people on low incomes, inactive people, people bringing up a child alone (a group 95% of whom are women), or people receiving social assistance?", translated by Amnesty International. Amnesty International (2024), *France: CNAF State Council Complaint*, paragraph 71, available at www.amnesty.org/fr/documents/eur21/8795/2024/en/, accessed 11 November 2025.
392. Wachter S., Mittelstadt B., Russell C. (2020), "Bias preservation in machine learning: the legality of fairness metrics under EU non-discrimination law", *West Virginia Law Review*, 123(3), 735.

7.4.3. High-risk AI systems

Annex III (5), on the area of access to enjoyment of essential private services and essential public services and benefits, covers "AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services".[393]

Public agencies rely on computation systems to calculate the benefits of beneficiaries, often via rule-based systems. Here, the question will be which computation systems fall under the definition of AI systems in the AI Act.

Under Article 6 of the AI Act, providers can self-exempt from the high-risk regime, under certain conditions. Some of these conditions are likely to be used for systems used in welfare and social security. For instance, real-life uses include using natural language processing (NLP) to analyse the content of job seekers' emails,[394] which could be done "in preparation for an assessment", or using optical character recognition (OCR) to help crop, turn and clean applications,[395] which could be considered a "narrow procedural task". However, as stated elsewhere in these guidelines, these definitions remain vague and, in the absence of case law, close monitoring is needed.

7.4.4. Registration obligations

High-risk AI systems in the area of social security will be registered in the public version of the database by providers and deployers. The information registered will include the summaries of FRIAs conducted by the deployers.

393. AI Act, Annex III (5) (a).
394. European Union Fundamental Rights Agency (2020), *Getting the Future Right: Artificial Intelligence and fundamental rights*, Luxembourg: Publications Office of the European Union, p. 32.
395. Ibid., p. 33.

References

Allen R. and Masters D. (2020), *Regulating for an equal AI: A new role for equality bodies: Meeting the new challenges to equality and non-discrimination from increased digitisation and the use of Artificial Intelligence,* Equinet.

BBC (2020), "Home Office drops 'racist' algorithm from visa decisions", *BBC*, available at: www.bbc.com/news/technology-53650758, accessed 7 November 2025.

Direction générale des Entreprises (2025), Les autorités compétentes pour la mise en œuvre du règlement européen sur l'intelligence artificielle [Competent authorities for the implementation of the Artificial Intelligence Act], Ministère de l'Économie, des Finances et de la Souveraineté industrielle, available at www.entreprises.gouv.fr/priorites-et-actions/transition-numerique/soutenir-le-developpement-de-lia-au-service-de-0, accessed 7 November 2025.

Dumbrava C. (2025), "Briefing: Artificial intelligence in asylum procedures in the EU", European Parliamentary Research Service, available at www.europarl.europa.eu/RegData/etudes/BRIE/2025/775861/EPRS_BRI(2025)775861_EN.pdf, accessed 7 November 2025.

Equinet (2024), *Understanding the new EU Directives on standards for equality bodies: legal digest on standards for equality bodies*, available at https://equineteurope.org/publications/understanding-the-new-eu-directives-on-standards-for-equality-bodies-legal-digest-on-standards-for-equality-bodies/, accessed 11 November 2025.

Equinet (2025), *How to use the Artificial Intelligence Act to investigate AI bias and discrimination: A guide for equality bodies,* European Network of Equality Bodies, available at https://equineteurope.org/publications/how-to-use-the-artificial-intelligence-act-to-investigate-ai-bias-and-discrimination-a-guide-for-equality-bodies/, accessed 10 November 2025.

European Union Agency for Fundamental Rights (2021), Equality in the EU: 20 years on from the initial implementation of the Equality Directives, available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-opinion-equality-directives-01-2021_en_0.pdf, accessed 7 November 2025.

Hellenic Data Protection Authority (2024), Ministry of Migration and Asylum receives administrative fine and GDPR compliance order following an own-initiative investigation by the Hellenic Data Protection Authority, available at: www.dpa.gr/en/enimerwtiko/press-releases/ministry-migration-and-asylum-receives-administrative-fine-and-gdpr, accessed 7 November 2025.

Ilieva M. (2024), *Handbook on identifying and using equality data in legal casework*, Equinet, available at: https://equineteurope.org/publications/handbook-on-identifying-and-using-equality-data-in-legal-casework/, accessed 7 November 2025.

info.gouv.fr (2025), France Travail : comment ça marche? [How does France Travail work?], available at: www.info.gouv.fr/actualite/france-travail-comment-ca-marche, accessed 7 November 2025.

Jones C., Lanneau R., Maccanico Y. (2023), Europe's techno borders, EuroMed Rights and Statewatch, available at https://www.statewatch.org/publications/reports-and-books/europe-s-techno-borders/, accessed 7 November 2025.

McGregor L. (2023), *Digital border governance: a human rights based approach*, University of Essex and the OHCHR, available at www.ohchr.org/en/documents/tools-and-resources/digital-border-governance-human-rights-based-approach, accessed 7 November 2025.

Ozkul D. (2023), Automating immigration and asylum: the uses of new technologies in migration and asylum governance in Europe, Oxford: Refugee Studies Centre, University of Oxford, available at www.rsc.ox.ac.uk/publications/automating-immigration-and-asylum-the-uses-of-new-technologies-in-migration-and-asylum-governance-in-europe, accessed 7 November 2025.

Romain M. et al. (2023), "Is data neutral? How an algorithm decides which French households to audit for welfare fraud", *Le Monde*, available at www.lemonde.fr/en/les-decodeurs/visuel/2023/12/05/how-an-algorithm-decides-which-french-households-to-audit-for-benefit-fraud_6313254_8.html, accessed 11 November 2025.

Subgroup on Equality Data of the European Commission's High Level Group on Non-discrimination, Equality and Diversity (2025), Collecting and using equality data in full compliance with EU General Data Protection Regulation and national data protection rules, Publications Office of the European Union, available at: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/equality-data-collection_en, accessed 7 November 2025.

Veld S. (in 't) et al. (2020), Letter to Andrea Jelinek, Chair of the European Data Protection Board on the possible use of the Clearview AI application by law enforcement authorities in the EU, available at www.edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf, accessed 7 November 2025.

Xenidis R. (2020), Tuning EU equality law to algorithmic discrimination: Three pathways to resilience, *Maastricht Journal of European and Comparative Law*, available at: https://journals.sagepub.com/doi/10.1177/1023263X20982173, accessed 7 November 2025.

Xenidis R. (2025), "Legal protection against algorithmic discrimination in Europe: Current frameworks and remaining gaps", Council of Europe, Strasbourg.

Public administrations across Europe are using artificial intelligence (AI) and/or automated decision-making (ADM) systems in a wide range of policy areas, including migration, welfare, justice, education, employment, tax, law enforcement or healthcare. Such systems are also deployed in critical areas of the private sector, such as banking and insurance. Although AI and ADM systems present significant risks of discrimination, challenges remain in identifying and mitigating these risks. Thus, equality bodies and other national human rights structures have a key role in promoting fundamental rights-compliant deployment of AI/ADM systems by public sector organisations. The guidelines aim to equip equality bodies and other national human rights structures, especially in the European Union, to tackle discrimination in AI/ADM systems. They update them on their responsibilities regarding the changing regulatory environment – including the European Union's AI Act and the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law – offer recommendations and examples for applying new regulations and serve as a resource to assist and advise national stakeholders, such as policy makers and regulators on human rights, equality and non-discrimination.



PREMS 003426

ENG

The Member States of the European Union have decided to link together their know-how, resources and destinies. Together, they have built a zone of stability, democracy and sustainable development whilst maintaining cultural diversity, tolerance and individual freedoms. The European Union is committed to sharing its achievements and its values with countries and peoples beyond its borders.

www.europa.eu

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

www.coe.int

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE