EUROPEAN ASSESSMENT METHODOLOGY ON ALGORITHMIC DISCRIMINATION

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

Louise Hooper
Ylja Remmits
Ioanna Papageorgiou

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 ASSESSMENT METHODOLOGY ON ALGORITHMIC DISCRIMINATION

Louise Hooper
Ylja Remmits
Ioanna Papageorgiou

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

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.

All other correspondence concerning this document should be addressed to the AI Co-ordinator of the Anti-discrimination and Inclusion Department of the Council of Europe, F-67075 Strasbourg Cedex, E-mail: anti-discrimination@coe.int

Cover: Publications and Visual Identity Division, Council of Europe
Layout: Luminess
Photos: Shutterstock, Unsplash and Better Images of AI

Contents

Abbreviations

ADR	Alternative dispute resolution
ADM	Automated decision making
AI	Artificial intelligence
CJEU	Court of Justice of the European Union
CSO	Civil society organisation
DPA	Data protection authority
DPIA	Data protection impact assessment
DSAR	Data subject access request
EB	Equality body
EDPB	European Data Protection Board
FRIA	Fundamental rights impact assessment
GDPR	General Data Protection Regulation
HRIA	Human rights impact assessment
LED	Law-enforcement directive
MSA	Market surveillance authority

Terminology

For the purposes of this methodology, the following relevant terminology choices have been made or the terms shall have the meanings set out below.

AI system: a machine-based system that is designed to operate with varying levels of autonomy; that may exhibit adaptiveness after deployment; and that can infer, from the input it receives and for explicit or implicit objectives, how to generate output such as predictions, content, recommendations or decisions that can influence physical or virtual environments (AI Act, Article 3(1)).

Algorithmic system: a term used in this methodology to cover both AI systems and non-AI systems, including ADM systems. It also includes AI systems that are not used in decision-making processes.

Automated decision-making system (ADM): the term covers a wide range of automated systems, which are used in the context of or for the purpose of decision making. They could be AI based, but could also be based on other technologies, even as simple as basic if-then rules. They range from fully automated systems that do not involve any human input to semi-automated or decision-support systems, which include both machine-driven and human input and are very widely used in practice.

Caseworker: a person from an equality body performing the assessment at any step of this methodology in the course of their work investigating cases of discrimination.[1]

Complainant(s): the person or group of persons alleging or experiencing (unlawful) discrimination. For coherence with the wording of the GDPR and the AI Act, the terms "data subject(s)" and "affected person(s)" correspond to "complainant(s)" when referring to the relevant provisions of those regulations, respectively.

Confusion matrix: a table used to evaluate how well an algorithmic system is performing by comparing its predictions against the actual, real-world results. The rows in the confusion matrix table denote the actual real-world results, while the columns denote the system's predictions. The table shows how many of the predictions were correct or incorrect.

Expert: a person with specialised knowledge or technical expertise consulted or involved by the equality body to support the caseworker at any stage of this methodology. The expert provides specialist input but is not the main caseworker.

High-risk AI system: or "high-risk AI", this is used to refer to an AI system as exhaustively defined in Article 6 of the AI Act.

Input data: any information, signals or raw data provided to the algorithmic system, based on which the system comes to its output. For example, an AI-based cancer screening app that is intended to detect suspicious moles may use age, gender

1. While this methodology is primarily aimed at EBs, it may also be relevant to national human rights institutions (NHRIs) and ombudsperson institutions or other stakeholders. Where this methodology is applied by NHRIs and ombudspersons, the term "caseworker" could also refer to caseworkers at those institutes.

and a picture of the mole as input data. In an LLM (large language model) system like ChatGPT, the input is the text of the chat interaction and potentially the text of prior chat interactions too.

Market surveillance authority: the national authority or authorities carrying out activities and taking measures under Regulation (EU) 2019/1020 (market surveillance and compliance of products).

Non-discrimination: the term "non-discrimination" is used over "equality" or related terms.

Non-discrimination directives: the term refers to the EU directives listed at Appendix G.

Notified body: this is a conformity assessment body that performs third-party conformity assessments, including testing, certification and inspection. For example, the notified body assesses the conformity of high-risk AI systems in accordance with the conformity assessment procedures set out in the EU AI Act.

Non-high-risk AI system: an AI system that is not included in the exhaustive definition of high-risk AI under the AI Act. Note that this only means these systems are not categorised as high-risk under the AI Act, not that these AI systems are risk free.

Output data: the result of the algorithmic system after processing the input data. For example, a predicted characteristic about an individual, a score, recommendation, decision or content like images, video or text.

Provider/deployer: the terms are used as defined in Article 3 of the AI Act. While defined with reference to AI systems, the respective roles may also apply, by analogy, to non-AI systems.

Qualifying ADM: for the purposes of this methodology, qualifying ADM is used to mean a subcategory of ADM systems that meets the criteria defined in Article 22 of the GDPR, of "solely" automated decision making (Regulation (EU) 2016/679). These systems trigger heightened transparency and information obligations under the GDPR.

Respondent: the organisation or entity investigated by the equality body for unlawful discrimination following a complaint, an *ex officio* procedure or a notification from the market surveillance authority (MSA). In the context of the GDPR and the AI Act, respondents may be termed "data controllers" and "AI providers" or "deployers", respectively, as defined in those regulations.

For the terminology related to the EU AI Act, please refer to Article 3 of the EU AI Act.

Acknowledgements

This report was prepared in the context of the project Upholding Equality and Non-Discrimination by Equality Bodies regarding the Use of Artificial Intelligence in Public Administrations, which is co-funded by the European Union via the Technical Support Instrument and 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 (YVV, Finland) and the Commission for Citizenship and Gender Equality (CIG, Portugal).

The report was authored by Louise Hooper (international consultant, Council of Europe), Ylja Remmits and Ioanna Papageorgiou (algorithm audit/international consultants, Council of Europe). The Council of Europe wishes to extend its 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, Sophie Vincent, Thelma Raes and Laetitia Parmentier (Unia, Belgium); Tiina Valonen and Ville Rantala (YVV, Finland); Carla Peixe, Lúcia Pestana and Alexandra Andrade (CIG, Portugal); Massimiliano Santini (Reform and Investment Task Force, Secretariat-General, European Commission); and Menno Ettema, Sara Haapalainen, Ayca Dibekoğlu and Delfine Gaillard (Anti-Discrimination and Inclusion Department, Council of Europe).

Special thanks to Raphaële Xenidis, Kris Shrishak, Brent Mittelstadt, Chris Russell, Ydo Bergstra and Jurriaan Parie for review contributions, and to Laurens Naudts and Plixavra Vogiatzoglou for their expert input. The report also benefited from the discussions with and contributions by national experts from equality bodies and civil society organisations who participated in a multi-country seminar and workshop in Brussels on 15 April 2026. All these perspectives enriched the analytical and operational sections of these guidelines.

Executive summary

Algorithmic systems can reinforce and create discrimination because they are often designed to differentiate among individuals: classifying, ranking or targeting them. In combination with historical inequalities and human biases embedded in the data, rules and design choices of algorithmic systems, discriminatory patterns may be reproduced and scaled unless they are proactively identified and mitigated.

This methodology provides a step-by-step guidance to equality bodies (EBs) and other human rights organisations in Europe to assess discrimination cases related to artificial intelligence (AI) or algorithmic systems. It is meant for the caseworkers, advisers and lawyers of these entities investigating discrimination claims that involve or are suspected to involve AI or automated decision making (ADM). It aims to serve as a reference list of issues and sources to consider at each step of an assessment. The methodology is divided into four iterative stages:

Step 1: identification of AI or algorithmic cases

Step 2: information gathering on the AI or algorithmic system to identify discrimination

Step 3: methodology for assessing received information

Step 4: remedies

These stages rely on the European regulatory framework on AI, specifically on the EU AI Act, and anti-discrimination law, and make references to other legislation, such as data protection, example cases and jurisprudence, where relevant. The stages make distinctions between high-risk AI systems and other systems in line with the EU AI Act providing means to access technical documentation, data and testing of high-risk systems, especially by bodies named as "authorities protecting fundamental rights" under Article 77 of the EU AI Act.

The methodology does not focus on national legislation and in some countries national law may provide better enforceable means to access information or investigative powers on algorithmic discrimination. Caseworkers should keep these considerations in mind while using this tool.

To support the use of the four steps, the methodology has an extensive list of appendices that provide example template letters for requesting information, support the understanding of risks of algorithmic discrimination, for example by types of AI system or sector where a system is used, and help in assessing information, such as by providing a checklist/record sheet for step 3.

For ease of using this methodology, a basic understanding of AI and algorithmic bias and discrimination and related terminology is helpful, while the tool also provides a terminology list. Other publications produced under the project Upholding Equality and Non-Discrimination by Equality Bodies regarding the Use of Artificial Intelligence in Public Administrations complement this methodology and may support building this basic understanding.

- Legal protection against algorithmic discrimination in Europe: current frameworks and remaining gaps, December 2025 (also available in French, Dutch, Portuguese, Finnish, Swedish).
- European policy guidelines on AI and algorithm-driven discrimination for equality bodies and other national human rights structures, December 2025 (also available in French, Dutch, Portuguese, Finnish, Swedish).

Introduction

New regulatory frameworks on AI, such as the EU AI Act,[2] the EU directives on standards for equality bodies (hereinafter "the standards directives")[3] and the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (hereafter the "Council of Europe Framework Convention on AI"), provide new tools and powers for equality bodies and human rights organisations to investigate algorithmic discrimination.

These tools come with some limitations and challenges. For example, some discriminatory algorithmic systems may not be categorised as AI under the EU AI Act.[4] Furthermore, many areas of the law relating to AI and discrimination are not yet clear. Finally, for many readers and caseworkers, this will be a new and relatively complex area of law.

Despite these challenges, this four-step methodology aims to support and provide a structure to systematically analyse the discriminatory impact of a decision or treatment that has potentially been made by or with an algorithmic system. Readers should not view each step of the methodology as something that must be completed. Rather, the steps provide a reference manual containing a variety of tools for identifying systems, gathering and assessing evidence and deciding what action to take. By following the steps in the methodology and seeking (technical) expert assistance where necessary, it should be possible to have in place the elements for establishing the presumption of discrimination and seeking remedies in algorithmic discrimination cases.

EBs should approach discrimination claims in relation to AI and ADM like any other case of discrimination but should also recognise that a lack of transparency or uncertainty about how an algorithmic system works may be considered when deciding whether there is a risk of discrimination or whether a prima facie case has been established. This is because of a growing recognition that there is an unequal power and information balance between companies making AI systems, those

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) Nos. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence 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 and 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.
4. Certain examples of algorithmic discrimination are based on simple rule-based systems that are not qualified as AI, such as the Dutch examples of discriminatory algorithms in the childcare benefits scandal (Amnesty International 2021) and fraud risk scoring by the Dutch Education Executive Agency (Rechtbank Overijssel 2024).

responsible for deploying them and those on whom the systems are deployed.[5] In those circumstances the burden of proof may shift to the respondent to show that the algorithmic system did not discriminate or contribute to discrimination in an unlawful way. For affected persons to have effective access to justice, a higher degree of transparency will be required.

The Digital Omnibus on AI,[6] a legislative package amending and streamlining the AI Act and other laws, was adopted by the European Parliament. Where relevant, reference is made to these amendments.

Key elements of the new legal framework

The standards directives

The standards directives, to be transposed by 19 June 2026 (Article 24 of the standards directives), lay down minimum requirements for the functioning of equality bodies to improve their effectiveness and guarantee their independence. These powers should be read alongside the existing powers in the EU non-discrimination directives.

Directive 2024/1500, Recital 21, and Directive 2024/1499, Recital 22, record in respect of allocation of financial resources that:

> 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.[7]

EU AI Act, Article 77: powers of authorities protecting fundamental rights and co-operation with market surveillance authorities

New powers are given to equality bodies and national human rights institutions (NHRIs) meeting the requirements of Article 77 of the AI Act[8] in respect of high-risk

5. This is discussed in detail in sub-section 3.8.
6. Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). Available at: https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng, accessed 24 July 2026.
7. Article 26 of the Framework Convention on AI also requires that EBs are effective, impartial and independent, sufficiently resourced and have adequate powers and expertise.
8. Article 77(1) of the AI Act, including the Omnibus amendments: "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, shall have the power to request and access any information or documentation created or maintained from the relevant market surveillance authority pursuant to this Regulation in accessible language and machine-readable format by electronic means where access to that information or documentation is necessary for effectively fulfilling their mandates within the limits of their jurisdiction. This Article is without prejudice to the competences, tasks, powers and independence of the relevant national public authorities or bodies under their mandates."

AI systems to ensure they can fulfil their mandate.[9] The current proposals in the Digital Omnibus on AI seek to clarify that these powers are without prejudice to the existing powers and independence of these bodies.[10]

The list of authorities protecting fundamental rights should have been notified to the European Commission by 2 November 2024 and member states "shall keep the list [of authorities] up to date".[11] The Commission recognises that the list of "Article 77" bodies is updated continuously in light of the ongoing implementation of the AI Act.[12] EBs not listed by member states by the first notification deadline can still be added. EBs could also be removed from the list.

Relevant authorities are empowered under Article 77(1) to request and access any document created or maintained under the AI Act in accessible language and format if it is necessary for effectively fulfilling their mandates within the limits of their jurisdiction. This should mean that requests can be made in respect of documentation created or maintained by other national competent authorities, including market surveillance authorities and notified bodies, and providers, deployers or other actors in the life cycle of an AI system. The Digital Omnibus clarify that requests to access information and documentation should be made to the market surveillance authorities who "shall grant access to such information and documentation, including by requesting such information and documentation from the provider or the deployer, where necessary and without undue delay"[13] and that involved authorities or bodies "shall cooperate closely and provide each other with mutual assistance necessary for fulfilling respective mandates".[14] This co-operation and assistance shall include the exchange of information where necessary for the effective supervision or enforcement of the AI Act and other Union legislation, which would include the non-discrimination directives (see Appendix G).

If documentation is insufficient to ascertain whether an infringement of obligations under Union law protecting fundamental rights has occurred, the equality body may make a reasoned request to the market surveillance authority, to organise testing of the high-risk AI system through technical means (EU AI Act, Article 77(3); see step 4).

Any information or documentation obtained must be treated in accordance with the confidentiality requirements of Article 78. Article 78(2) makes clear that the Article 77 authority should request only data that are strictly necessary for the assessment of

9. Not all equality bodies fall under the definition provided in Article 77 although many will do. The term "Article 77 authority" is used throughout to mean any EB or NHRI that meets the definition provided by Article 77 of the AI Act.
10. Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). Available at: https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng, accessed 24 July 2026.
11. AI Act, Article 77(2).
12. https://digital-strategy.ec.europa.eu/en/policies/fundamental-rights-protection-authorities-ai-act, accessed 5 June 2026.
13. Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). Available at: https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng, accessed 24 July 2026.
14. Ibid.

the risk posed by AI systems and for the exercise of their powers in accordance with the regulation and Union law. Any request under the AI Act should therefore be clear and narrow to avoid being refused.

Where data are requested and obtained, the equality body shall ensure that adequate and effective cybersecurity measures are in place to protect the security and confidentiality of the information and data obtained, and shall delete such data as soon as they are no longer needed for the purpose for which it was obtained, in accordance with applicable Union or national law.

Similarly, Council of Europe standards, such as the Framework Convention on AI and Recommendation CM/Rec(2026)1 on equality and artificial intelligence, set out the steps to take by member states and other stakeholders to promote equality and prevent and combat discrimination in all activities within the life cycle of AI systems.

Confidentiality

Confidentiality requirements are set out in Article 78(1) of the AI Act for the Commission, market surveillance authorities and notified bodies (Article 70) and any other natural or legal person involved in the application of the AI Act, to respect the confidentiality of information and data obtained in such a manner as to protect:

- the intellectual property rights and confidential business information or trade secrets of a natural or legal person, including source code (Directive (EU) 2016/943, Article 5). Relevant to equality bodies, Article 5 of Directive 2016/943 provides an exception for the purpose of revealing misconduct, wrongdoing or illegal activity, provided that the respondent (the EB or potentially the MSA) acted for the purpose of protecting the general public interest (Article 5 (b)) or protecting a legitimate interest recognised by Union or national law (Article 5(d)). Protecting fundamental rights and preventing or addressing discrimination are both, at least arguably, covered under this exception;
- the effective implementation of the regulation, in particular for the purposes of inspections, investigations or audits;
- public and national security interests;
- the conduct of criminal or administrative proceedings;
- information classified pursuant to Union or national law.

It is currently unclear how these may be relied on to impact the ability of the EB to obtain information from relevant parties; however, where disclosure is refused citing confidentiality the EB may have recourse to either a competent authority under the EU AI Act or the DPA under the GDPR. It is likely that where trade secrets are raised as a reason for non-disclosure, the competent supervisory authority or court may be required to balance the rights and interests at issue with a view to determining what should be disclosed (see *CK v. Dun & Bradstreet Austria GmbH and Magistradt der Stadt Wien* (2025), discussed in step 2.1).

Co-operation across sectors

For the new legal framework to be fully effective, it will also be necessary to seek, build, strengthen and formalise co-operation with the relevant market surveillance authorities, data-protection authorities and any other Article 77 authority, if not already in existence. This requirement to co-operate is formalised in the Digital Omnibus through an amendment inserting Article 77(1)(b).[15] To this end, it may be necessary or useful to develop interagency working protocols.[16] For examples and good practices, see the box below. The new standards directives foresee the establishment of national frameworks for conducting inquiries that enable equality bodies to carry out fact-finding, including appropriate mechanisms for co-operation between equality bodies and other relevant public authorities for that purpose (Article 8 of the standards directives).

Negotiations between EBs and their member state government for ensuring a clear legal basis for sharing of information between Article 77 bodies, including equality bodies and data-protection authorities, as well as between MSAs and Article 77 bodies – as provided for in their co-operation under Articles 73(7) and 79(2) of the AI Act – shall play a key role in this regard (Autoriteit Persoonsgegevens 2024, paragraph 37). The existence of such legal bases is a prerequisite for establishing 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 and allow for additional case-specific bilateral agreements where needed (Autoriteit Persoonsgegevens 2024, paragraph 37).

Examples and promising practices

In the United Kingdom, the Equality and Human Rights Commission worked with the Information Office as part of the fairness and innovation challenge, on test cases in higher education, finance, healthcare and recruitment, 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 Science (Department of Science, Technology and Innovation 2024).

In Norway, the equality body has co-operated with the data-protection authority as part of a regulatory sandbox on artificial intelligence (Norwegian Data Protection Authority 2023).

In France, co-operation between the Defender of Rights and the data-protection authority, Commission Nationale de l'Informatique et des Libertés (CNIL), is facilitated by several mechanisms: both institutions have a memorandum of understanding agreement, and the Defender of Rights also has an advisory role

15. Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). Available at: https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng, accessed 24 July 2026.
16. See also Article 26 of the Council of Europe Framework Convention on AI (2024), "Effective co-operation between institutions must be facilitated", and Article 14 of the standards directives requiring appropriate co-operation mechanisms.

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 (Council of Europe 2025b).

In the UK, a memorandum of understanding between the Information Commissioner's Office (the DPA) and the Equality and Human Rights Commission (the equality body) sets out principles of information sharing and co-operation, the legal bases on which information sharing may take place, practicalities relating to data control and processing and the respective roles, functions and powers of each body. See: Memorandum of Understanding

Risk categories under the AI Act

The EU AI Act adopts a regulatory framework that categorises AI systems according to an assumed level of risk they pose to fundamental rights, health, and safety (AI Act, Article 1). This approach reflects the idea that not all AI systems present the same level of concern: some pose unacceptable risks and must be prohibited entirely, others present significant risks requiring strict oversight, while others are deemed to require no AI-specific regulation at all.

The risk category determines the applicable obligations – ranging from absolute prohibition to comprehensive technical requirements to basic transparency duties. For equality bodies, this risk-based structure is directly relevant: it determines what information and documentation should exist and influences the available remedies under the AI Act.

Prohibited AI

The EU AI Act prohibits certain AI practices that pose unacceptable risks to fundamental rights, safety or democratic values (Article 5 of the AI Act). These include:

- manipulative techniques that materially distort behaviour, including the generation of non-consensual sexual and intimate content or child sexual abuse material (CSAM);
- exploitation of vulnerabilities;
- social scoring systems;
- risk assessments of natural persons to predict the committal of criminal offences based on profiling;
- real-time remote biometric identification in public spaces (with limited exceptions);
- emotion recognition in workplace/education contexts;
- biometric categorisation inferring protected characteristics;
- untargeted scraping of facial images.

See also Appendix J – Prohibited AI practices.

High-risk AI

High-risk AI systems include use cases that are deemed to pose significant risks to health, safety or fundamental rights and are used in specific areas listed in Annex III of the AI Act (Article 6). These include systems used in:

- biometrics
- critical infrastructure management
- education and vocational training
- employment and worker management
- access to essential services and benefits
- law enforcement
- migration, asylum and border control
- administration of justice.

Note: an AI system referred to in Annex III shall always be considered high risk where the AI system performs a profiling of a natural person.

See also Appendix I – High-risk AI practices.

If the AI system is intended to perform any of the following, the system will not be considered high risk (Article 6(3)):

- a narrow procedural task;
- to improve the results of a previously completed human activity;
- to detect decision-making patterns or deviations from prior decision-making patterns;
- a preparatory task for an assessment.

High-risk AI systems are subject to extensive documentation requirements, transparency obligations and risk-management procedures under the AI Act.

General-purpose AI (GPAI)

The high-risk and prohibited categories encompass specific use cases, and the categorisation relies on the explicit purpose of the systems. In contrast, general-purpose AI models, for example large language models (LLMs), are models capable of performing a wide range of distinct tasks and that can be integrated into a variety of downstream systems or applications (AI Act, Article 3(63)). GPAI, by definition, does not have a specific purpose. A GPAI model can, however, be the foundation of specific applications with specific purposes that could fall into the high-risk category.

Documentation drafted as a result of the obligations on GPAI is unlikely to be available to EBs under the AI Act as access rights are limited to high-risk AI systems applications (AI Act, Article 77). EBs would be entitled to rely on their existing powers and national law but, in most circumstances, it is highly likely that a court order would be needed. GPAI models are broadly included under the algorithmic system category for the purpose of this methodology.

How does the methodology apply the risk categories?

In the EU AI Act, as explained above, there are new powers to obtain information in respect of high-risk systems. The methodology is therefore structured primarily around the distinction between high-risk AI systems and other algorithmic systems. In the case of non-high-risk AI, the EBs are expected to operate under the same informational framework that applies to the rest of algorithmic systems. Step 1 of the methodology helps caseworkers to understand what type of system they are looking at.

The AI Act places additional regulatory requirements on various actors involved in the development, distribution and deployment of high-risk AI systems. For those systems this will provide significant and relevant information about the risk-management measures, the data used and data governance measures in place, technical documentation explaining key design and data choices and the intended purpose of the system, as well as information about testing and monitoring and identified risks of discrimination. This documentation will be an essential resource for equality bodies seeking to identify or assess potential cases of algorithmic discrimination.

Such information will not be available in all, or even most, cases. However, these requirements also assist EBs in identifying and interpreting evidence in respect of AI and other algorithmic systems where no such formal requirements exist. This is because they serve as reference steps for identifying, reducing or eliminating the risk of discrimination and the documentation is often part of standard software/technical development.

The methodology seeks to distinguish throughout between those circumstances where there is a power given to an EB under Article 77 of the EU AI Act to request and access documentation created or maintained under that AI Act in respect of high-risk systems and those cases where no such power exists.

It is important to remember that national legal frameworks often provide equality bodies with information-gathering or investigative powers. Equality bodies that are not Article 77 authorities do not have a direct legal basis under the AI Act for accessing relevant documentation for high-risk AI systems but will still be able to rely on these national and other Union law powers.

Protected characteristics

Throughout this methodology protected characteristics are mentioned. These are characteristics protected by the European Convention on Human Rights (the Convention) and EU Directives.

The European Court of Human Rights has produced a Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention.

Table 1. Protected characteristics covered by European law
(An X in the table means the characteristic is covered by regulation.
An empty cell means it is not featured.)

	Article 14 of the European Convention on Human Rights	Charter of Fundamental Rights of the EU	EU non-discrimination directives
Sex	X	X	X (2004/113/EC, 2000/78/EC, 2006/54/EC, 2023/970/EU, 2010/41/EU)
Race[17]	X	X	X (2000/43/EC)
Colour	X	X	
Language	X	X	
Religion	X	X (or belief)	X (2000/78/EC)
Political or other opinion	X	X	X (2000/78/EC)
National or social origin	X	X (ethnic or social origin)	
Association with a national minority	X	X (membership)	
Property	X	X	
Birth	X	X	
Other status	X		
Disability	Other status	X	X (2000/78/EC)
Age	Other status	X	X (2000/78/EC)
Sexual orientation	Other status	X	X (2000/78/EC)
Nationality	Other status	X (qualified)	
Genetic features	Other status	X	
Marital status	Other status		
Migrant or refugee status	Other status		

17. 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.

How to use the methodology

The methodology adopts a four-stage approach (see also Figure 1 below).

Step 1: identification of AI or algorithmic cases

Step 2: information gathering on the AI or algorithmic system to identify discrimination

Step 3: methodology for assessing received information

Step 4: remedies

Where relevant, the methodology differentiates between the different sources of the cases:

A. a complaint (by an individual or group)
B. an *ex officio* investigation
C. information provided by an MSA

Note: the steps are presented as consecutive steps for structural clarity of this methodology. They are not neatly consecutive, but in practice often circular and iterative.

Step 1

The initial reporting of or information about a case of discrimination where involvement of algorithmic systems may be recognised.

Key questions:

- Is this a case involving a high-risk AI system under the AI Act?
- Is this a case involving an algorithmic system?

Step 2

The next step is to seek information about the identified system, which may support the subsequent identification of discrimination. Step 2 sets out the types of relevant information, documentation and other types of evidence that may be available or accessible to the EBs and their potential sources.

Note: the information identified in this step is analysed in detail in step 3. Accordingly, steps 2 and 3 should be considered in conjunction. Similarly, where information is missing and a legal power exists to obtain it, the remedy is discussed in step 4.

Key question:

- What information is available and how can it be accessed?

Step 3

A full analysis of the relevant evidence is conducted using a set of suggested questions as a guide. These questions are non-exhaustive.

The non-discrimination legal framework is then applied to that evidence.

Key questions:

- Can a prima facie case of discrimination be established?
- Is it likely that the respondent will be able to discharge the burden of proof?
- Considering all the evidence, has unlawful discrimination been established?

Step 4

Consider and apply the available remedies.

Key question:

- Which remedies should be sought or applied?

At all stages, the caseworker will need to consider the following.

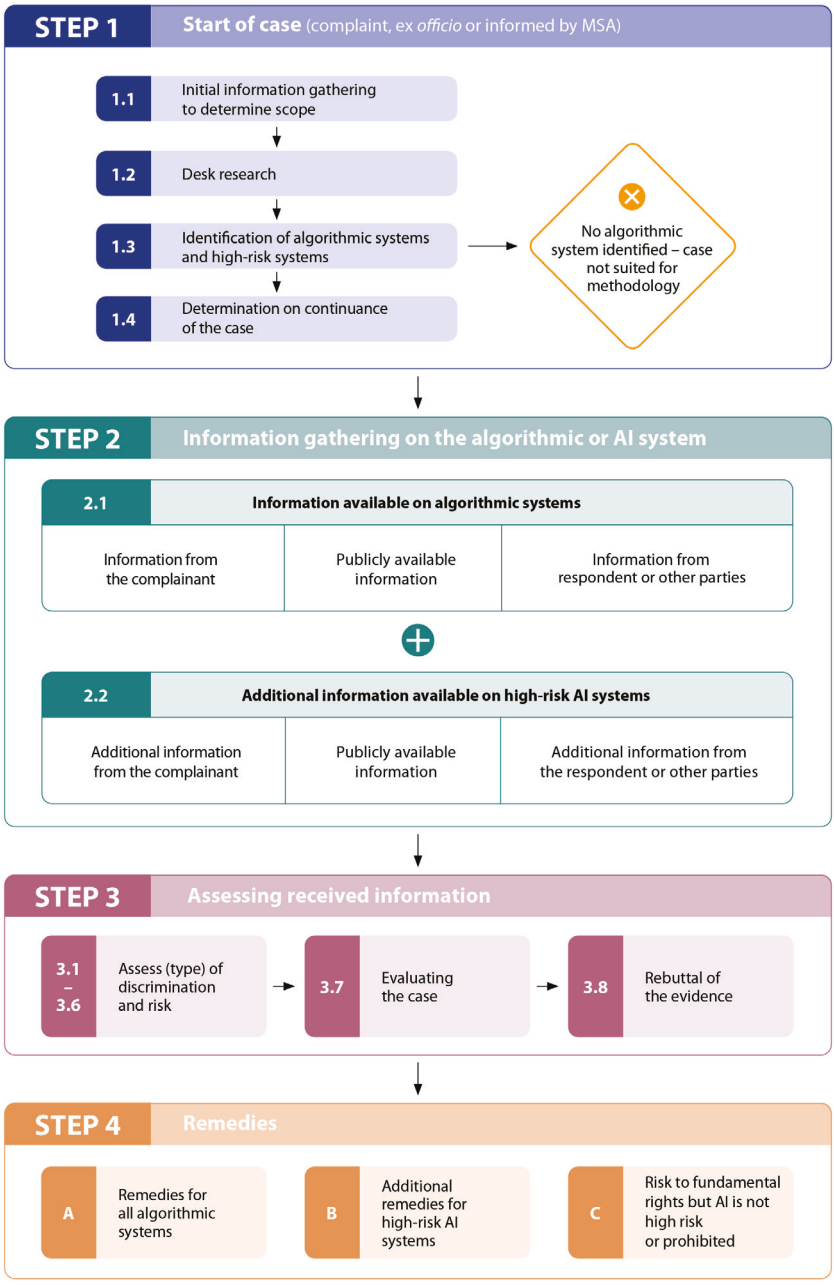
- If there is no arguable discrimination claim, the case should be discontinued.
- If there is no algorithmic system involved, the case should be discontinued under this methodology and considered under the ordinary discrimination process of the EB.

Using experts

It may be necessary to seek expert assistance in respect of some elements of this methodology where, for example, expertise on data or computer science for the technical assessment of either the model or the data is required. The methodology indicates the types of questions that an expert could be asked to answer and when this should be considered. As amendments to Article 77 in the Digital

Omnibus were adopted,[18] equality bodies may be able to seek assistance from the MSA, other public authorities or bodies with expertise in reliance on the mutual assistance provision in proposed Article 77(1)(b).

Figure 1. Steps 1 to 4 of the methodology



18. See above, under "EU AI Act, Article 77: Powers of authorities protecting fundamental rights".

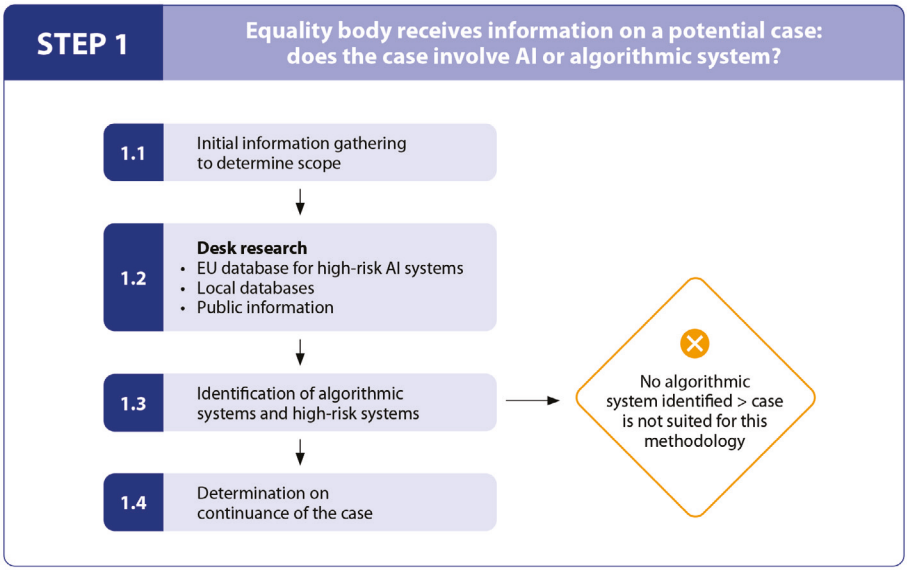
Step 1

Identification of AI or algorithmic systems

The aim of this first step is only to understand if ADM or a (high-risk) AI system is involved and to determine if there is enough information to continue to step 2. In this step no detailed investigation is performed.

Step 1 consists of the following sub-steps.

Figure 2. Step 1 – Does the case involve AI or an algorithmic system?



Note: the steps are presented as consecutive steps for structural clarity of this protocol. These sub-steps are not neatly consecutive, but in practice are often circular and iterative.

Identification of AI and ADM cases differs depending on the source of the case:

A. from a complaint (by an individual or group)
B. as a result of an *ex officio* investigation
C. via information provided by an MSA

How to recognise algorithmic systems and AI

Algorithmic systems can be as simple as the automation of a limited set of human-defined rules. In general, algorithmic systems (including AI) are hard to recognise. Definitions have shifted over the years or are interpreted differently.

In the EU AI Act, the technical definition at Article 3(1) provides that:

> AI system means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[19]

Even when there is agreement on the definitions, algorithmic systems are frequently not recognised by organisations or are referred to using different terms.

An assessment of whether an algorithmic system is used should cover a variety of terms.

All the following terms could indicate the use of algorithmic systems.

- Automation, machine-based, computerised, algorithm-based
- Profiling or the creation of profiles
- Automated decision making or decision-support systems
- A system or computer decides/analyses/compares/recommends/processes a person's data
- A system, computer or camera sees/listens/understands
- Any mention of the calculation of scores, probability, likelihood or an estimation of future behaviour
- Automated risk assessment, automated recognition
- Any mention of statistics
- Any mention of machine learning

The following words could indicate the use of AI.

- Machine learning, deep learning
- A model/machine/computer was trained
- Patterns were learned from data

19. This is supplemented by C(2025) 5053 Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act).

- Based on large language models (LLMs)
- Predictive models

Example: "On the basis of these data, our service provider calculates probability values using mathematical-statistical methods to assess the risk of non-payment and to verify your address."

1.1. Initial information gathering

A. Complaint

When the source of the case is a complaint, there is an initial point at which the complaint is filed. At this stage initial information can be collected on whether an algorithmic system or AI system may be involved. This initial information gathering is lightweight to align as much as possible with existing complaint-receiving processes within equality bodies.

1.1.1. Initial determination of scope and competence

- Source of complaint: telephone, online form, mail, other
- Name and contact details of complainant
- Brief report of the problem
- Which organisation is the respondent (organisation that is the topic of the complaint)
  - Public body or private?
- Assessment of competence
  - Protected grounds?
  - Sector?
- Remedy sought/intended purpose of case
  - Giving advice?
  - Pursuing litigation?
  - Recommending action?

Is this case within the competence of the equality body? Has the complaint already been lodged with another body/entity or is any other entity already involved in the case?

1.1.2. Gathering further information from the complaint

Potentially the complainant will have more information available to them. This section defines sample questions to be asked of the complainant, either via an online form or a (phone) conversation, to identify if an algorithmic or an AI system has been involved.

Both the AI Act and the GDPR impose obligations for transparency towards individuals – data subjects or affected persons – about the use of algorithmic or AI systems. See the boxes containing the relevant provisions below. Relevant information may be provided to individuals through personal correspondence or contractual agreements, typically included in privacy notices or terms and conditions, or otherwise

publicly communicated via the organisation's website or platforms (see 1.2.3 Website and external communications of respondent).

Therefore, already asking them to provide any relevant documents they might have, along with a minimal review of public information, could support the next subsequent step (see 1.2 Further desk research).

Note: those provisions do not cover all cases where AI or algorithmic systems are used and therefore the absence of information simply may mean that more inquiries are necessary.

There are several stipulations in the AI Act that require that people are notified about the use of AI.

- When a high-risk AI system is used in the workplace, workers' representatives and affected workers should have been informed that they are subject to the use of an high-risk AI system (AI Act, Article 26(7)).
- When high-risk AI systems make decisions or assist in making decisions related to natural persons, the natural persons should have been informed by the developer that they are subject to the use of the high-risk AI system (AI Act, Article 26(11)). This information should include the intended purpose and the types of decisions it makes. The deployer should also inform the natural persons about their right to an explanation provided for under this regulation (Recital 93 of the AI Act).
- When natural persons interact directly with AI (through chatbots or voice assistants, for example), they should be informed about it (AI Act, Article 50(1)). This can be done through clear notifications or pop-ups like: "Hey, I am a chatbot."/"Hi, you are now chatting with an AI assistant."/"I am X, an AI assistant here to help you."
- Similarly, individuals should be informed about the operation of emotion recognition systems (an AI system that identifies the anger or satisfaction of customers through facial or voice characteristics) or biometric categorisation systems (an AI system performing gender identification based on a person's hair or face shape, for instance) (AI Act, Article 50(3)).

GDPR

- There are also GDPR transparency requirements (GDPR, Article 5(1)(a), 13, 14), which require the data subject to be notified about the use of algorithmic systems, including information on the controller's identity, the purposes of processing and the existence of automated decision making and profiling (see step 2.1.1 Information provided by the complainant).

This information may appear in the terms and conditions or privacy notice or statement; in relation to the AI Act, the AI Office published the guidance on the AI Act transparency obligations in July 2026.[20]

20. See more here: Code of practice on marking and labelling of AI-generated content – Shaping Europe's digital future.

Questions to ask the complainant and/or consider for the desk research

Note: a complainant may not know what information they have or whether it is relevant. Therefore, a useful starting point is simply to ask: "Which websites/apps were you using?" and "Were you given any paperwork?".

Relevant paperwork may include, *inter alia*, an application submitted by the complainant, letters, e-mails, invoices or consent forms and privacy notices sent by the respondent organisation, contracts between the complainant and the organisation, including, appendices and contractual updates delivered on paper, by e-mail or through app or portal notifications. If available, the relevant documentation should be collected and consulted during 1.2 Further desk research to answer some or all of the following questions.

- Was the complainant told that an AI system was or is being used?
  - When the case applies to the workplace: has the complainant checked with their worker representatives or trade union?
  - If yes: what were they told?
- Was the complainant told that automated data processing was being used?[21]
- Was the complainant asked for permission on the specific data processing or asked to confirm reading a privacy statement or notice?
  - If yes: can the permission request text, privacy statement or notice to be shared?
  - If no: was there any other mention of "this is how we process your information" or "this is how your information may be used"?
- Was there any mention of automation, a computer system performing autonomous tasks or a computer system providing input into a decision? Look out for phrases and language such as the following.
  - A system or computer decides/analyses/compares/recommends/processes a person's data.
  - A system, computer or camera "sees"/"listens"/"understands".
  - Any mention of the calculation of scores, probability, likelihood or an estimation of future behaviour.
  - The use of a computer system to support a process, potentially with a brand name. For example, "We use Clippy/Frank/Maya to process your data and to support our work".
- Does a contract between the complainant and the respondent contain any reference to automation, algorithmic processes, specifically named systems, statistics, performance metrics, rating or scores (such as automated deactivation or reliability scores)?
  - If yes: can the contract or the relevant contractual clauses be shared?
- Where did the interaction or communication with the (respondent) organisation take place?

21. When personal data are used for fully automated decision making, users should have been informed that they are subject to fully automated decision making (GDPR, Article 13(2)(f)).

- In cases of in-person or over-the-phone interaction:
  - if in person, did the other person consult a computer to come to decisions or conclusions?
- In cases of interaction through a computer or through a smart phone:
  - was there an online form filled out?
  - how long after the interaction was there an outcome or a decision (instantly, a few minutes to an hour, a few days, longer)?
  - was permission asked to process personal data, for example a tick-box mentioning personal data or privacy?
  - was any information about any protected attribute (see Protected characteristics) requested in the system interaction?

1.1.3. Quick review of public information

EU database for high-risk AI systems

From 2 August 2026 onwards, an EU database for high-risk systems[22] is expected to be available for high-risk systems before they are placed on the market or put into service. According to the Digital Omnibus on AI, systems put into service before 2 December 2027 for stand-alone high-risk AI systems and 2 August 2028 for high-risk AI systems embedded in products will only require registration if subject to "significant change".[23] The public parts of the database will be available for all.

In cases of complaints relating to systems used in education, employment, government, banking, insurance, administration of justice and elections, and relating to actions/activities such as automation in the identification of individuals, face or voice recognition, emotion recognition, prediction of intentions or risks, a quick search in the database – using relevant keywords that could be, for example, the name of the respondent organisation, the system name or the relevant sector – may be a useful starting point.

- If the respondent is listed in the database as being in any role for a use case that is relevant to the complaint, there is a relative certainty that (high-risk) AI is involved.[24] Proceed to step 1.3.

Note: there are some exceptions to the registration requirements, or it may be that a provider or deployer has failed to comply with their regulatory obligations. Further information about the information available in the database is provided under step 2.2.2: Publicly available information.

22. While this database does not yet exist and it is uncertain what the database design and interface will look like, it is included here because it is expected to become a highly relevant source of information in the future.
23. Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). Available at: https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng, accessed 24 July 2026. In other cases where the high-risk system is intended to be used by public authorities, necessary steps must be taken to comply with the regulation by August 2030, AI Act Article 111(2).
24. Note that when a system is not recorded in this database, it does not mean no (high-risk) AI system is involved; exceptions apply.

Compare to list of use cases

- Appendix C contains a list of common uses of algorithmic systems and AI in different sectors. Do any of these examples appear relevant to the situation, case or process of the complaint? See also Appendix F of AI databases and use cases.

General internet search

- Conduct an internet search for innovation/automation in the described situation, case or process of the complaint or by the respondent organisation.
  - For example, "is AI being used by the [nationality] police?".
  - As an example, for Finland this gives list a of search results including: Finland plans major expansion of police biometric data collection powers – ID Tech.
  - For example, "is AI used in recruitment in [country]?".
  - For Belgium this gives the following result suggesting a third of Belgian companies use AI in recruitment processes: www.anews.com.tr/europe/2023/07/19/in-belgium-one-third-of-companies-use-artificial-intelligence-in-their-recruitment-processes.
  - Take care that the results are search results and not AI generated.

Note: certain practices are prohibited under Article 5 of the AI Act. See Appendix J: Prohibited AI practices for a list.

These steps are indicative only. If the response to these questions demonstrates that it is likely that an AI system or algorithmic system was used, move to step 1.3.

If the information is inconclusive, consider gathering more (public) information during desk research as described in step 1.2.

B. *Ex officio*

Some equality bodies have the mandate to start investigations *ex officio* or *actio popularis* (through national regulation).

In this phase we assume that no complainant from an individual or group of individuals is involved. In later stages of the investigation, the equality body may choose to involve directly affected individuals. For the purpose of this assessment methodology it is assumed that there is a particular field of interest (a sector, an operational area within this sector and potentially specific organisations) already determined, for example, pricing algorithms used by insurers or fraud risk scoring for welfare/benefits.

Information to collect

- Situation, case or process of interest and public information available.
- Relevant (unsettled) complaints by the equality body or other relevant entity. These could be complaints that were not strong enough cases separately or where the complainant withdrew their complaint.
- Indication of involvement of AI or algorithmic systems, if available; see How to recognise algorithmic systems and AI above.

- Details of the organisation that would be subject to this *ex officio* investigation if it were to formally launch (hereinafter, the "respondent"), or in the case of a sector review, a list of organisations that are representative of the sector under review.[25]

Compare to a list of existing cases

- Appendix C contains a list of common uses of algorithmic systems and AI in different sectors. Do any of these examples appear relevant to the situation, case or process of the potential investigation?

When a case is started *ex officio*, it may be already clear that that an AI system is involved. Steps 1.2 and 1.3. are not relevant in this case: move to step 1.4.

C. Informed by MSA

The equality body is expected to receive information from the market surveillance authority (MSA) concerning AI systems that pose a risk of discrimination, specifically in the following cases.

- **Serious incidents (AI Act, Article 73(7))**
  - Where a provider notifies the MSA of a serious incident,[26] the MSA must inform the Article 77 authorities, including the equality body where relevant. Consultation on dedicated guidance on reporting procedures and on a draft incident report template by the Commission concluded on 7 November 2025.[27]
- **Products presenting a risk (AI Act, Article 79 in conjunction with Article 3(19) of Regulation (EU) 2019/1020)**
  - Where the MSA has sufficient reason to believe that an AI system qualifies as a product presenting a risk to the right of non-discrimination, it has a duty to inform and fully co-operate with the relevant Article 77 authorities, including the equality body.

This information may include the following.

- Organisation: public or private body.
- AI system: identification of the system and area of high-risk classification (Annex I or Annex III of the AI Act, including domain and use case).
- Role of the organisation (deployer, provider, other).

25. For example, if an EB opens an *ex officio* investigation into pricing algorithms used by insurers, a representative list of insurers instead of a particular respondent could be used at this stage of the protocol.
26. A serious incident means an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following:
(a) the death of a person or serious harm to a person's health;
(b) a serious and irreversible disruption of the management or operation of critical infrastructure;
(c) the infringement of obligations under Union law intended to protect fundamental rights;
(d) serious harm to property or the environment (AI Act, Article 3(49)).
27. See more at: AI Act: Commission issues draft guidance and reporting template on serious AI incidents, and seeks stakeholders' feedback.

- When notification is based on Article 73 of the AI Act (serious incident):
  - the circumstances of the incident or malfunction;
  - the type of harm that occurred or was suspected;
  - the relationship between the AI system and the incident (how the AI caused or contributed to the incident);
  - any available information on the provider's investigation risk assessment of the incident and corrective actions proposed or implemented.
- When notification is based on Article 79 of the AI Act (risk):
  - the reason for considering that the AI system presents a risk to fundamental rights;
  - (optional, if available) relevant information on already conducted evaluations;
  - (optional, if available) corrective actions proposed or implemented.
- In cases involving a high-risk AI system in the areas of law enforcement, migration, asylum and border control management (points 1, 6 and 7 of Annex III), the MSA will be able to access information on the AI system as recorded in the EU database for high-risk AI systems.

When an equality body is informed by an MSA, there is certainty that a high-risk AI system is involved. Steps 1.2 and 1.3. are not relevant in this case: skip to step 1.4.

1.2. Further desk research

If there is capacity available for desk research, there are several sources that could be consulted to determine whether ADM or AI is expected to be used in the case. This section details the sources and what to look for.

The steps referred to in this section vary in the level of depth and time required to perform this desk research:

▲ steps that could be prioritised;

▼ additional steps for more in-depth desk research.

For example, it should be relatively easy to search the EU database (below) once it is operational and if the respondent is registered in the database. This will provide a quick answer to the question "is an AI system in use?". If the deployer is not registered, further research will be required.

This section does not apply to cases where the source is "Informed by MSA". In this case the MSA will have already determined that a high-risk AI system is involved and therefore the desk research as outlined in this section would be redundant.

1.2.1. EU database for high-risk AI systems

Look up the respondent or any known deployer or provider in the database.

Is the respondent listed as a deployer in part C of the database?[28]

- ▲ Is the respondent the deployer for a use case that is relevant to the complaint? Which organisation is the provider?

Relevant information available in the database for initial identification:

- ► contact details of the provider and authorised representative;
- ► name and contact details of the deployer (only public authorities, EU institutions, bodies and agencies, or persons acting on their behalf);
- ► the URL of the entry of the AI system in the EU database by its provider.

Is the respondent listed in the database as a provider in part A or B of the database?

- ▲ Is the respondent the provider for a high-risk use case that is relevant to the complaint?
- ▲ Is the respondent the provider for a use case that is intended for use in a high-risk domain, but self-assessed to fall under the exception in Article 6(3) of the AI Act? This assessment may be requested by the national competent authorities.

Relevant information available in the database for initial identification:

- ► contact details of the provider and authorised representative;
- ► trade name or other reference enabling identification and tracing of the AI system (this could be useful for example where a high-risk system is used as part of another system);
- ► intended purpose.

If found in this database, then an AI system is being used. Move to step 1.3 and/or 1.4.

If not, look up similar organisations to the respondent in the database.

- ▼ Are similar organisations listed in the database as providers or deployers for a use case that is relevant to the complaint? For example, other similar insurers list AI systems for pricing when the case is about (un)fair pricing, or other similar governments in the same country have listed AI systems for benefit assessment when the case is about benefits denial.

Under Article 49(4), the registration of high-risk AI systems in the areas of law enforcement, migration, asylum and border control management is to take place in a secure non-public section of the EU database referred to in Article 71 and should only include a specific set of information as delineated in Article 49(4). Access to these sections of the database will be limited.

28. Note that only public authorities are required to register as deployers. Other organisations have no such obligation.

For more on the non-public section of the database and transparency aspects in the area of law enforcement, see restrictions on access to information under step 2.2.2 and the box Area of law enforcement under 2.2.4 respectively.

1.2.2. Other databases and inventories for (high-risk) AI systems and algorithmic systems

Some organisations and local governments maintain a local database, registry or inventory of AI systems used. A list of these databases can be found in Appendix F. Not all these databases are relevant. Check only those that are relevant to your national context.

Look up the respondent in the database.

- ▲ Is an algorithmic system or AI listed as used or developed by the respondent, which is relevant to the situation, case or process covered by the complaint?

Look up similar organisations to the respondent.

- ▼ Is an algorithmic system or AI listed as used or developed by a comparable organisation, which would have been relevant to the situation, case or process covered by the complaint, had this complaint been about this comparable organisation?

Compare to the list of existing use cases.

- ▼ Appendix C for a list of common uses of algorithmic systems and AI in different sectors.

Do any of these use cases appear relevant to the situation, case or process of the complaint?

1.2.3. Website and external communications of respondent

Privacy notice/statement

Look for phrasing indicating the use of algorithmic systems, for example any of the following.

- ▲ Purposes that suggest automation, creation of profiles or statistical methods. Refer to How to recognise algorithmic systems and AI and to the questions contained in 1.1.2 Questions to ask the complainant and/or consider for the desk research.
- ▲ Third parties receiving personal data (recipients or categories of recipients). Check for indications of third-party involvement, such as scoring companies or credit reference agencies, which may imply profiling or automated decisions.
- ▼ Contact details of the data controller: is the data controller known to implement AI solutions or automation in the sector of interest? If an AI or algorithmic system exists, the data controller will be typically the deployer of the system and the respondent under the meaning of this methodology.

Other types of communication

Is there any mention of an algorithmic system that may be relevant to the case?

- Search the website of the respondent for articles on their implementation of AI, innovation and automation or FAQs on the respondent's website/platform. The easiest way to search for a specific website is to add "site: [website of respondent]" to the search query. For example, innovation AI site: bigbank.com.
- Check technical job postings for data scientists, AI or machine learning. Is there any mention of an algorithmic system that may be relevant to the case? A job description for a "senior data scientist" by a bank contains the following: "Preventing money laundering and terrorist financing is one of the key aspects for our society and our organization … you will be responsible for optimising our current rule-based transaction monitoring (TM) system and eventually for introducing more advanced analytics methodologies such as machine learning into our TM models." See senior data scientist transaction monitoring – Rabobank.

If applicable: review the website and communications of deployers of relevant high-risk AI use cases.

If any use cases relevant to the case are listed by third-party deployers in the EU database for high-risk AI systems, look at the website of the provider.

- Is the respondent listed on the website as an "organisation we work with" or "trusted by these customers"?
- Is the respondent mentioned in any other way on the provider website? This could be most easily found through an internet search engine. For example, search for [respondent] site: [provider].com.

1.2.4. Further review of public information

Some of the steps mentioned here have already been mentioned in step 1.1. For completeness they are repeated here.

General internet search

- See internet search under step 1.1.3.
- Refine the search conducted under step 1.1.3 by specifically checking if non-governmental organisations (NGOs), national or international bodies or organisations have reported on the use of AI or algorithmic systems in a similar situation, case or process of the complaint, either by the respondent or by similar organisations. Relevant NGOs include Amnesty, AlgorithmWatch and national civil society organisations. For example, in the Netherlands the DPA produces an AI and algorithm risk report twice a year. The search for the Dutch National context could be "[sector of complaint] Autoriteit Persoonsgegevens AI and algorithms risk report".
- Optional: refine the search and include national and international AI strategies.
- Other relevant resources could include the OECD's AI incidents and hazards monitor and the artificial intelligence incident database or reports produced by the Council of Europe such as "Discrimination, artificial intelligence and algorithmic decision making" (Zuiderveen Borgesius 2018).

1.3. Identification of algorithmic or high-risk AI systems

Based on the information collected in steps 1.1 and 1.2, a reasonable determination can be made of whether an algorithmic system or high-risk AI system is used and how certain this determination is.

Reminder: this methodology differentiates only between high-risk AI systems and algorithmic systems. Algorithmic systems include non-high-risk AI systems and ADM systems. For high-risk AI systems, the AI Act imposes extensive transparency requirements and documentation obligations, meaning additional documentation is expected to be available. If an AI system is not a high-risk, the information available and the steps to follow are the same as for simpler algorithmic systems and therefore are combined into a single category.

Type of system

- **High-risk AI system**
- **Algorithmic system**

Certainty

- **Relatively certain**
- **Potentially**

Note: concluding if AI or algorithmic systems are used is a difficult and nuanced assessment at this stage, with very limited information available. The certainty of conclusions as listed below are suggestions, merely intended to provide direction.

EU database for high-risk AI systems

Is the system recorded in the EU database?

- YES in section A or C: there is a high-risk AI system has been identified for this case. It is **relatively certain** that a **high-risk AI system** is used in this case.
- YES, in section B:[29] there is an AI system involved, but none of the documentation that is required for high-risk systems is expected to be available. It is **relatively certain** that an **algorithmic system** is used in this case.
- NO, but there are similar organisations (like another bank) that have listed systems relevant to the case (such as credit scoring systems) in section A or C. Therefore, it may be reasonable to assume that a similar high-risk system is being used by the respondent. For this stage of the methodology assume that it is **relatively certain** that an **algorithmic system** is used in this case. **Potentially a high-risk AI system** is used in this case.

29. Based on Article 6(3) of AI Act, the AI system is not considered to be high risk.

Information provided by the respondent (either to the complainant, in public documents or upon request)

- The respondent stated the use of automation, algorithms or AI for purposes relevant to the case, either directly to the complainant or in the privacy notice/policy. It is **relatively certain** that an **algorithmic system** is used in this case.
- The respondent stated the use of automation, algorithms or AI for purposes relevant to the high-risk AI categories (see Appendix I) either directly to the complainant or in the privacy notice/policy. It is **relatively certain** that an **algorithmic system** is used in this case; **potentially** a **high-risk AI system** is used in this case.
- The respondent has listed an algorithmic or AI system in a public database (see Appendix F) for purposes relevant to the case. It is **relatively certain** that an **algorithmic system** is used in this case.
- The respondent has publicly stated they use of algorithmic systems or AI for purposes relevant to the case in blog posts, press releases or other sources. Note that references to the use of algorithmic systems could be vague or evasive (see step 1.1 for potential phrases used). It is **relatively certain** that an **algorithmic system** is used in this case.

Other information

- Reputable parties such as NGOs and trusted media organisations have reported the use of algorithmic systems or AI by the respondent for purposes relevant to the case. No confirmation by the organisation can be found. It is **relatively certain** that an **algorithmic system** is used in this case.
- Other parties have reported the use of algorithmic systems or AI by the respondent for purposes relevant to the case. No confirmation by the respondent can be found. **Potentially** an **algorithmic system** is used in this case.
- AI and algorithmic systems are frequently used for purposes relevant to the case, as listed in Appendix C. **Potentially** an **algorithmic system** is used in this case.
- Similar organisations are reported to use algorithmic systems for purposes relevant to the case. **Potentially** an **algorithmic system** is used in this case.
- There are contextual clues that indicate that algorithmic systems may be involved in the case. For example, because of the speed of decision making, when complex processes or decisions that require discretion are handled instantaneously or within minutes. **Potentially** an **algorithmic system** is used in this case.
- There are contextual clues that indicate that algorithmic systems may be involved in the case. For example, because of the speed of decision making, when complex processes or decisions that require discretion are handled instantaneously or within minutes and either AI and algorithmic systems are frequently used for purposes relevant to the case, as listed in Appendix C, or similar organisations are reported to use algorithmic systems for purposes relevant to the case. It is **relatively certain** that an **algorithmic system** is used in this case.

1.4. Continuing the case

Steps 1.1. to 1.3 cover the assessment of whether an algorithmic system is likely to be involved. To decide on whether to continue the case, a further assessment should be made of the likelihood of a solid discrimination case. This should be evaluated against established criteria within the equality body. When an algorithmic system is potentially involved this may require imposing a lower threshold of certainty before deciding to continue the claim.

***Manjang v. Uber Eats UK Ltd & Others* (2021)**

This case for race discrimination was brought on the grounds of harassment, victimisation and indirect discrimination following the introduction of facial recognition technology. The claimant, a delivery driver, received an e-mail from Uber Eats (the respondent) notifying him of his permanent suspension from the platform on the grounds that he was "sharing his Uber Eats delivery partner account" and had failed a facial recognition check. He responded stating "your algorithm by the looks of things is racist and this needs to be addressed as it cannot recognise and verify my photos which is probably why I get asked to take photos of myself multiple times a day". Uber Eats contested the discrimination claim and sought to have it struck out at an early stage because, they said, it was based on "factual errors". They then provided information on their grounds of resistance to the claim about the working of the technology, and in response the claimant amended his claim. The tribunal refused to strike out the amended claim recognising that at the point the claimant had pleaded his case there had been a lack of clarity about why his account had been deactivated. Some months later during litigation the respondent stated that the reasons given to claimant that the decision was automated was incorrect and that a human review had taken place. The claimant maintained and the tribunal agreed that there was opaqueness surrounding the reason why the claimant's photos were rejected and his account deactivated. Ultimately an out-of-court financial settlement was reached. This is an example of a case funded and supported by an EB, in this case the Equality and Human Rights Commission (UK).

Table 2. Certainty of high-risk or algorithmic system and likelihood of discrimination

	Low likelihood of discrimination	Medium likelihood of discrimination	High likelihood of discrimination
Relatively certain high-risk AI	High priority case, consider involvement of an (internal) specialist on algorithmic systems	High priority case, consider involvement of an (internal) specialist on algorithmic systems	High priority case, consider involvement of an (internal) specialist on algorithmic systems
Relatively certain algorithmic system, potentially high-risk AI	Medium priority case, consider involvement of an (internal) specialist on algorithmic systems	High priority case, consider involvement of an (internal) specialist on algorithmic systems	High priority case, consider involvement of an (internal) specialist on algorithmic systems
Relatively certain algorithmic system	Low priority case, when continued consider involvement of an (internal) specialist on algorithmic systems	Medium priority case, consider involvement of an (internal) specialist on algorithmic systems	High priority case, consider involvement of an (internal) specialist on algorithmic systems
Potentially algorithmic system	Refer to existing methodologies, instead of this methodology	Low priority case under this methodology, where likelihood of discrimination is medium, but probability of AI system is low; refer to existing methodologies, instead of this methodology	Medium priority case, consider involvement of an (internal) specialist on algorithmic systems

Suspected incorrect classification under the AI Act

Wrong classification as non-high-risk

There is a possibility that providers of AI systems in Annex III areas will avoid the high-risk AI regime by self-assessing in any of the following ways.

- Not an AI system. In this case the AI Act would not apply.
- Not a high-risk system due to exceptions (AI Act, Article 6(3)). In this case the system should still be registered in the EU database under section B. In such a case the provider is required to document their assessment to opt out before placing on the market or putting into service the AI system, and to register the system in the EU database in section B (AI Act, Article 49(2)). There is no

requirement to publish the assessment, but the provider is required to provide the documentation of the assessment on request from the national competent authorities (MSA or notifying body).

- Not a high-risk system because the purpose is not covered by the language of the use cases listed in Annex III of the AI Act (AI Act, Article 6(3)).

If an equality body suspects that a system has been wrongfully assessed to be out of scope of the high-risk AI regime, they should inform the relevant MSA, regardless of whether a case of discrimination can be established (see under step 4, MSA procedure for dealing with AI systems classified by the provider as non-high-risk, and step 4.3).

For the purpose of this methodology the system should be regarded as an algorithmic system, as the information expected to be available for high-risk AI systems will most likely not be available in this case.

Questions to ask

- Is the system covered by Annex III use cases?
- Is the system likely to be an AI system? See How to recognise algorithmic systems and AI.
- Does it fall under the list of practical examples? (See Appendix C and/or the list produced by the Commission when available, Article 6(4)).
- Check section B of the database. The provider of the system has an obligation to register both themselves and the system under Article 49.

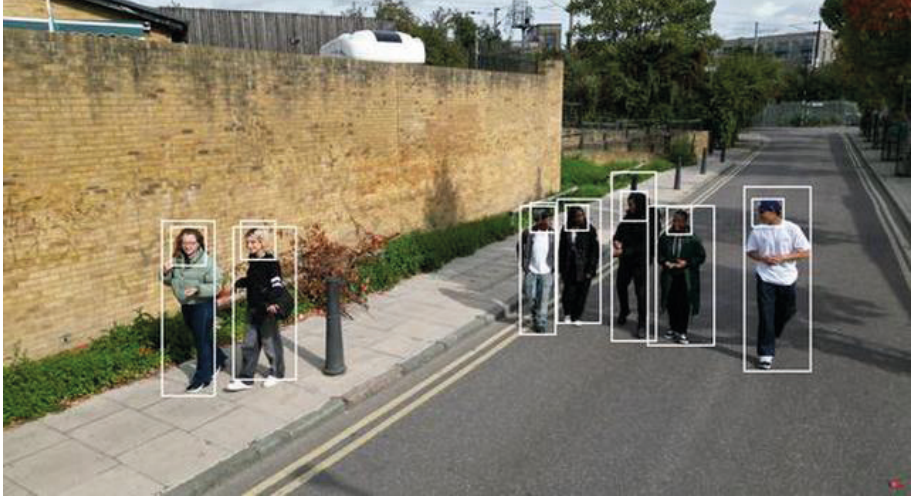
Suspected prohibited system

Certain practices are prohibited under the AI Act (see Appendix J – Prohibited AI practices).

If the EB encounters a prohibited system or practice:

- as these practices are prohibited, the use itself violates EU law. Immediate action should be taken to notify the relevant MSA, regardless of whether a case of discrimination can be established;
- additionally, when an EB concludes that a practice currently not included in this list does violate fundamental rights, they should compile the evidence and provide reports to the competent authorities in the relevant member state and the Commission (see step 4.3).

Cases involving prohibited practices may also be high-risk systems and/or have caused discrimination and a decision will need to be taken by the EB on whether further action relating to discrimination is required.



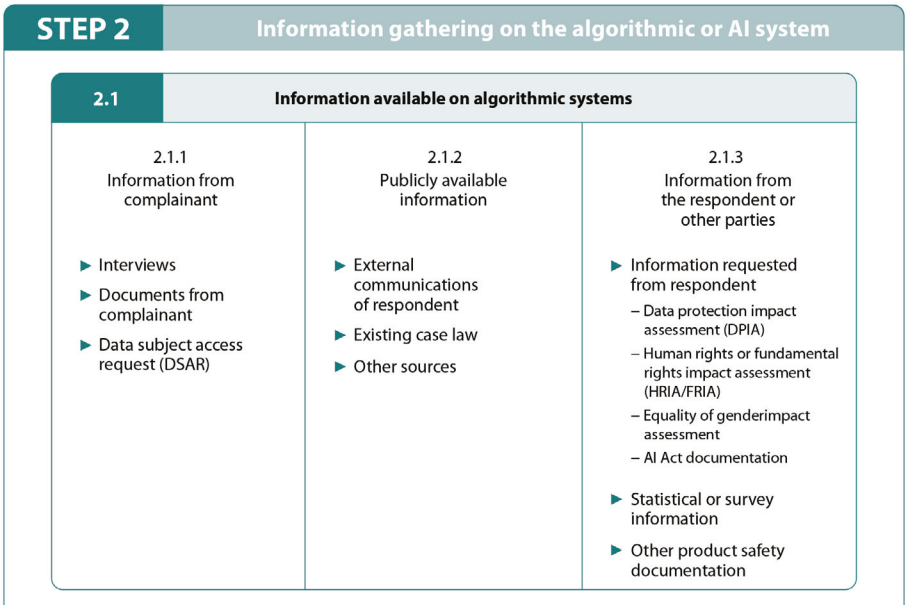
Step 2

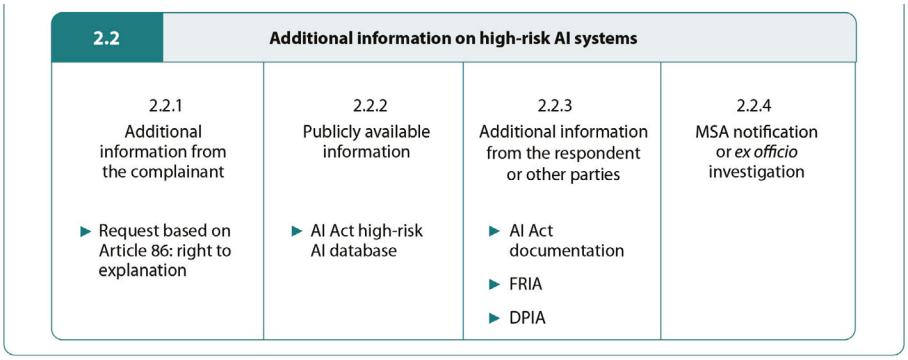
Information gathering on the algorithmic or AI system to identify discrimination

Step 2 identifies the types of information that may be available or accessible relating to both the system and the likelihood of establishing discrimination. It provides guidance on potential sources and how to gather the information.

Step 2 consists of following sub-steps.

Figure 3. Step 2 – Information gathering to identify discrimination





If an EB is not an Article 77 authority and/or the system is not identified as high risk, step 2.2 (for example, equality impact assessment and statistical or survey information) can still be used as framework guidance to enable any EB to request comparable information from the deployer or provider, relying on their investigative or information-gathering powers, and to evaluate any response or lack of response under step 3. However, note that respondents are not legally obliged under the AI Act to provide such documentation in these circumstances (although they may be under other legislation, for example product safety or consumer law).

The analysis of this evidence gathered under step 2 is conducted under step 3. In practice, these steps are typically carried out together.

By step 2, one has identified with a degree of certainty that an algorithmic system or AI system is involved in the case under examination, and potentially its classification as a high-risk AI system.[30] The next step is to seek information about this system, which may support the subsequent identification of discrimination in step 3.

There are three categories of sources.

1. Information that may be provided to the EB by the complainant. Such information may be available or accessible to complainants through their personal experience of the contested process, their correspondence with the respondent and the exercise of their information rights, primarily under the GDPR and the AI Act.
2. Other information may be publicly available.
3. Information that the EB may request from the respondent through the exercise of its national or Union law-derived investigative and information-gathering powers, including those granted under the EU AI Act.

Remember that information may also be disclosed or requested during pre-action correspondence or in the course of litigation.

30. If it has not been possible to identify an AI or algorithmic system, discontinue with this protocol and revert to your ordinary procedures.

Note: step 2 does not seek to be exhaustive; other types of information or information sources may also be available. National legal frameworks, including freedom of information legislation or rules concerning transparency of documents, may provide EBs with information-gathering or investigative powers, which go beyond those referred to in the methodology. Access to information can be also supported by new powers of inquiry from standards directives (see Introduction and step 4).

Known obstacles to obtaining information

Strategies deployed to obtain information, such as freedom of information requests, may run up against challenges and constraints, particularly relating to arguments around confidentiality and operational requirements. In France, for example, a freedom of information request made by CSOs to gain clarity on a risk-scoring system used by the social welfare administration managing family benefits only resulted in the release of the source code of former models (as opposed to the current model) and redacted lists of variables used (Council of Europe 2025a; *La Quadrature du Net and Others v. Premier ministre and Ministère de la Culture* 2024; see also Big Brother Watch 2025).

In *Kelly v. National University of Ireland* (C-104/10), where the applicant alleged sex discrimination after being refused access to a professional development programme and requested from the education institution information about the qualifications of other candidates from the education institution, the CJEU clarified that secondary Union legislation does not confer such individual right to access such data. However, the CJEU held that it is for the national courts to determine whether, in the circumstances of the case, public disclosure of these data is necessary in order to give effect to the objectives of the relevant legislation, namely Directive 97/80/EC.

The CJEU may similarly in the future further interpret the relevant provisions of the non-discrimination directives to ensure effective judicial protection against discrimination, in a way that facilitates claimants' access to information already in the phase leading up to the prima facie case (Farkas and O'Farrell 2015).

It may be useful to keep a manageable, searchable record of sources consulted. This can help identify patterns of discrimination and save valuable caseworker time. Suggested headings for literature reviews could include:

- source (including a link)
- keywords (proxy discrimination, bias mitigation, for example)
- summary
- relevance (discrimination found to exist in facial recognition system, for example).

2.1. Algorithmic systems

2.1.1. Information provided by the complainant

The complainant will often have very relevant information to provide for the identification of potential discrimination. Such information may be available or accessible to them through their personal experience in the contesting process or their correspondence with the respondent and may be based on their information rights, particularly those under the GDPR (see the box below).

When the case is handled as part of an *ex officio* investigation or is identified by an MSA, there is no direct complainant involved. For the purpose of information collection, consider the following.

- Involving complainants from other/older/uncompleted complaints or consider if a complaint is already lodged with another body/entity.
- If applicable, suggest collective exercise of the GDPR right of access in high stake cases.[31]

GDPR transparency obligations and data rights

The GDPR includes *ex ante* transparency obligations and *ex post* access rights, which allow data subjects to be informed about the fair use of their personal data.

Ex ante

- Under Article 5(1) and Recital 60 of the GDPR, personal data shall be processed fairly and in a transparent manner in relation to the data subject, who shall be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data are processed.
- Under Articles 13 and 14 of the GDPR, when personal data are processed data subjects shall be provided with information about the identity and contact of the data controller, the purpose of processing, the legal basis for the processing, the categories of personal data where data are obtained from third

31. Although the GDPR, the AI Act and the LED offer limited opportunities for collective representation, scholars have argued that the collective exercise of individual rights can nonetheless be fruitful (Mahieu, Asghari and van Eeten 2018). For example, multiple individuals could submit access requests, and the resulting insights could be shared with a trusted intermediary through data donations. Such collective efforts, through individualised actions, could create a larger knowledge pool concerning the use of data by specific actors or sectors. Similarly, the collective – yet individual – exercise of a right to access under Articles 15 and 22 of the GDPR, or the right to an explanation under Article 86 of the AI Act, by data subjects or affected persons, could offer gateways to gain wider knowledge of the functioning of AI systems. However, under the proposed amendments to the GDPR right of access in the Digital Omnibus regulation proposal, the effectiveness of access requests as both individual and collective transparency tools may be significantly reduced. See more below Making and obtaining a response to a data subject access request (DSAR) pursuant to Article 15 of the GDPR.

parties or publicly available sources, and the existence of automated decision making, including profiling.[32]

This *ex ante* information is typically more general and often included in privacy notices or statements.

Qualifying ADM

- Under Articles 13(2)(f) and 14(2)(g) of the GDPR, data subjects should be explicitly informed about the existence of solely automated decision making and profiling referred to in Article 22 of the GDPR, and be provided with meaningful information about the logic involved as well as the significance and envisaged consequences of such processing for the data subject.

As solely automated decision making is permissible under Article 22(2) of the GDPR only if the decision is:

- necessary for entering into, or the performance of, a contract;
- authorised by Union or member state law;
- based on the data subject's explicit consent, it should also be possible for the EBs to discover the relevant provisions of the contract, the law authorising the processing or the consent and what exactly was consented to, for example in a signed written statement, electronic form or e-mail.

Ex post

- Under Article 15 of the GDPR data subjects have the right to request access to their personal data, including information on the categories of the personal data, the purposes of the conducted processing, the recipients or categories of recipients of the personal data, and the existence of automated decision making, including profiling.

Qualifying ADM

- Under Article 15(h) of the GDPR, in cases of solely automated decision making and profiling referred to in Article 22, data subjects have the right to also request meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The EDPB encourages controllers, as "good practice", to provide meaningful information about the logic involved and to explain the significance and envisaged consequences of ADM and profiling even for non-qualifying ADM (Barros Vale and Zanfir-Fortuna 2022: 16).

Note: national jurisdictions may provide additional rights concerning the disclosure of documents. For example, in Sweden a person who applies for a job, promotion or training opportunity but is not selected has a right to request and receive written

32. There seems to be a growing consensus that this applies also to non-qualifying ADM, as a consequence of both articles requiring controllers to disclose what the purposes of processing are in combination with Regulation (EU) 2016/679, Recital 60 (Barros Vale and Zanfir-Fortuna 2022: 16).

information from the employer regarding the education, work experience and other qualifications of the person who was selected in order to be able to compare qualifications (Swedish Discrimination Act, section 4).

For countries not covered by the GDPR, the provisions in national legislation should be considered.

Key cases: SCHUFA Holding (2023) and *CK v. Dun & Bradstreet Austria GmbH and Magistradt der Stadt Wien* (2025)

(Numbers in square brackets relate to paragraphs in the decision.)

Whether an automated system was in use and what information must be provided to a data subject has been an issue in the context of the GDPR where specific provisions apply in respect of "solely automated processing including profiling" (Article 22). Three conditions need to be met for Article 22 to be engaged.

- There must be a "decision" (see Recital 71, which confirms this is broad in scope and gives specific examples of the automatic refusal of an online credit application or e-recruiting practices without human intervention).
- The decision must be based "solely on automated processing (including profiling)".
- This decision, based solely on automated processing, must produce a "legal or similarly significant effect" for the individual.

When these conditions are met, organisations employing an automated decision-making system must be able to provide the data subject with a "meaningful explanation of how the decision was reached". This is very similar language to that used in Article 86 of the AI Act, "right to an explanation".

SCHUFA Holding

In case C-634/21 SCHUFA Holding (Scoring), the CJEU examined a case where a private company provided credit assessments to its partners such as banks. To reach the decision on creditworthiness, an individual's characteristics were compared with data on how other people with comparable characteristics had behaved. A score was then assigned using mathematical and statistical procedures to indicate, for example, how likely a person was to repay a loan [14].

The complainant, OQ, was refused a loan by a bank (a third party) as a result of negative information transmitted to the bank by SCHUFA. OQ requested information on the personal data relied on and requested erasure of some data that were allegedly incorrect [15].

- SCHUFA replied informing OQ of her score and outlined, in broad terms, the methods for calculating the scores. However, referring to trade secrecy, it refused to disclose the various elements taken into account for the purposes of that calculation and their weighting. Last, SCHUFA stated that it limited itself to sending information to the bank and it was the bank that made the actual decision. In effect, they argued the score was not a "decision" [16].

In response to the three questions posed, the court held as follows.

- Decision: the concept of decision was broad enough to include the result of calculating a person's creditworthiness in the form a probability value concerning that person's ability to meet payment commitments in the future [47].
- "Based solely on automated decision making including profiling": it was common ground that SCHUFA's activity met the definition of profiling and the condition was met.
- "legal or similarly significant effect": An insufficient probability value leads in almost all cases to the refusal of the bank to grant the loan applied for. As the third party draws "strongly" on the probability value, this condition was also met [48].

As a consequence the court held that where the "probability value established by a credit information agency and communicated to a bank plays a determining role in the granting of credit, the establishment of that value must be qualified in itself as a decision producing vis-à-vis a data subject 'legal effects concerning him or her or similarly significantly [affecting] him or her' within the meaning of Article 22(1) of the GDPR".

The court also reiterated the need:

- to prevent discriminatory risks arising from profiling;
- for appropriate mathematical or statistical procedures for the profiling;
- for technical and organisational measures to be in place in particular to ensure that inaccuracies in personal data are corrected and the risk of errors minimised;
- for the data to be secured.

Importantly, the court also held that member states cannot adopt regulations that authorise profiling in disregard of the requirements laid down in Articles 5 (principles relating to data processing) and 6 (lawfulness of processing) of the GDPR and cannot definitively prescribe the results of the balancing of the rights and interests at issue in legislation [70].

Dun & Bradstreet

Explanations must enable the data subject to understand and, if necessary, challenge the decision and exercise their data rights. Mere communication of a complex mathematical formula such as an algorithm or a detailed description of all the steps in an automated decision-making process will not satisfy this requirement as they would not be sufficiently concise and intelligible [58-59].

"Meaningful information about the logic involved" must describe the procedure and principles actually applied in such a way that the data subject can understand which of his or her personal data have been used in what way in the automated decision making at issue. The complexity of the operations is not considered capable of relieving the controller of the duty to provide an explanation [61].

In the context of credit profiling, the CJEU held that a court may find it sufficiently transparent and intelligible to inform the data subject of the extent to which a variation in the personal data taken into account would have led to a different result [62]. This may not be the case for all algorithmic systems.

Where the controller takes the view that this information cannot be provided without disclosing third-party details or trade secrets, the data controller is required to provide the allegedly protected information to the competent supervisory authority or court, which must balance the rights and interests at issue with a view to determining the extent of the data subject's right of access provided for in Article 15 of that regulation.

These two cases are a guide to the approach the CJEU may take when considering the extent to which information should be made available and in what form under the GDPR and by analogy explanations required under the AI Act.

Interview with the affected person

Complainants who are making a complaint about discrimination based on one or more protected grounds will often have relevant information about the characteristics they have provided to the respondent either recently or in the past. It may also be useful to gather other information about their protected characteristics and occasions on which those characteristics might have been disclosed. Be mindful of your own data-protection obligations. Consider questions such as the following.

- When was your first and any subsequent contact with this organisation/government department? If there has been previous contact with the organisation/government department before the event that is subject of the complaint, information about protected characteristics may have been provided at that point.
- Were you asked to complete forms?
- If so, what forms were you asked to fill in?
- Consider the list of protected characteristics. Were you required to provide information on or tick boxes relating to any of these?
- Consider the list of known proxies in Appendix E. Were you asked to provide information about any of these?

Documents from the complainant

Relevant information may be contained in documentation available or accessible to the complainant. This might include:

- documents submitted by the complainant (application forms, correspondence, data access or other requests);
- documents provided by the respondent to the complainant (any contracts between the respondent and the complainant along with their appendices, data-processing information or privacy notices and internal communications, including contractual updates).

Making and obtaining a response to a data subject access request (DSAR) pursuant to Article 15 of the GDPR

Data subjects have the right to request access to their personal data from the data controller (usually the deployer of the system) under Article 15 of the GDPR. Properly

handled DSAR responses may contain highly relevant information (see step 3 for details), tailored to the individual's specific case, including:

- the categories of the personal data processed and a digital copy of these data;
- the purposes of the conducted processing;
- the recipients or categories of recipients of the personal data;
- the existence of automated decision making and/or profiling along with meaningful information about the logic involved and the envisaged consequences of such processing for the data subject.

If a complainant has not yet submitted a DSAR, it is recommended to encourage them to do so before proceeding further with any complaint or investigation. While there are no formal requirements on how to make a DSAR, it is advisable to submit the request in writing and record it (keep a copy of any e-mail or letter, keep any proof of post or delivery, take a screenshot if using an online form, portal or customer service channel). For a template see Appendix A.

Non-compliance with GDPR obligations regarding DSARs is widespread. Therefore, it is common to encounter either a lack of response, delayed action or the provision of inadequate or incomplete information after submitting a request. Complainants exercising their rights as data subjects should be prepared for possible follow-up communication, including reminders and additional clarification requests to the organisation. In high-stakes cases consider working together with the relevant national DPA (see Co-operation across sectors).

The Digital Omnibus regulation proposal introduces changes to the data subject's right of access under the GDPR. The proposed amendment to Article 12(5) of the GDPR[33] has been criticised (Skiotytė and Sadauskaitė 2026). If adopted, it would allow controllers to refuse or charge a fee for DSARs that are considered excessive or pursue "non-data-protection" purposes. It should not affect valid requests made to enforce data subjects' data rights.

2.1.2. Publicly available information

External communications of respondent

Relevant information may be communicated by the respondent on their website or platform, including in the FAQ pages, terms and conditions, or privacy notices, in accordance with the applicable GDPR transparency obligations (see the box on GDPR transparency obligations and data rights above).

Take note particularly of references to the purpose of the system, the purposes of data processing, the types of data processed, including any reference to sensitive data – also referred to as special categories of data – and any reference to the

33. Recital 35, Article 3, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725 and (EU) 2023/2854, and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus). Available at: EUR-Lex - 52025PC0837.

existence of (qualifying) ADM or profiling, its logic and consequences. These might indicate the use of algorithms or protected characteristics (for more details see steps 3.2 and 3.3).

> Public administrations are in some countries (like Finland) subjected to information obligations and must publish information regarding the use of ADM systems on their website and inform subjects of such use when making decisions. However, there is mostly no systematic national or transnational record despite local initiatives to create databases of AI and ADM applications (as in Belgium and Finland). Thus, EBs face difficulties in exercising their mandate to investigate, monitor, identify and challenge cases of algorithmic discrimination and support victims (Council of Europe 2025a).

Existing case law

Research case law covering either similar AI or algorithmic systems or automated decision-making processes. This can include domestic case law, European jurisprudence (including from the European Court of Human Rights and the CJEU) and foreign national case law, given that algorithmic systems and platforms often operate according to similar logics and recurring patterns across different countries.

As EU case law on AI and algorithmic regulation remains nascent, also consider examining GDPR-related jurisprudence, particularly decisions addressing automated decision making, as these can provide supportive guidance. Consider consulting the following.

- Databases such as Case law – EUR-Lex or the Case Law Database of the European Union Agency for Fundamental Rights for CJEU cases or Court cases, using keywords such as "artificial intelligence", "automated decision making", "profiling" and "credit scoring" to review existing judgments or monitor pending national courts' requests to the CJEU for preliminary rulings relevant to relevant aspects of the AI Act or the GDPR.
- For databases tailored to AI or algorithmic systems, consider also Case Law Database – Tech Litigation, which collects litigation efforts against automated systems, including judgments, decisions and opinions from national and international courts as well as data-protection authorities. In addition the DAIL – the Database of AI Litigation – Ethical Tech Initiative, which compiles US litigation data involving AI and algorithmic systems, may provide valuable insights into emerging litigation trends related to algorithmic discrimination, systemic flaws and discrimination risks, linked to specific types of technologies, including relevant information on US-based companies operating within the European Union, either as providers of similar AI systems or as data controllers (such as Clearview AI).

Some civil society organisations are beginning to compile databases specifically focused on cases of algorithmic discrimination (Algorithm Watch reporting form). These databases will be more useful if EBs contribute to them by reporting their own litigation or investigation outcomes. This must be done in compliance with data protection and litigation privilege principles.

- GDPR Enforcement Tracker – list of GDPR fines and fines | European Data Protection: for an overview of fines and penalties that data-protection authorities

within the EU have imposed under the GDPR, listing fines, including country, authority, date, fine amount, controller/processor, sector and type.

- Automated decision making under the GDPR: report by the Future of Privacy Forum: for a case law collection on ADM under the GDPR as of April 2022.
- National case law databases.

Other sources

There is a wide range of sources of data that may be useful in the context of identifying, investigating or proving a case of algorithmic discrimination.

- Country reports from the European Commission against Racism and Intolerance (ECRI) 7th monitoring cycle will take into account AI.
- Reports from civil society organisations (CSOs), covering either similar AI or algorithmic systems or similar decision-making processes.
- Findings from UN monitoring bodies, including the Committee on the Elimination of Discrimination against Women (CEDAW), Committee on the Elimination of Racial Discrimination (CERD), Committee on the Rights of the Child, the Committee against Torture (CAT), Special Rapporteurs, the World Health Organization (WHO) and the Committee on Economic, Social and Cultural Rights.
- Findings from other international bodies, such as the Office for Democratic Institutions and Human Rights of the Organization for Security and Co-operation in Europe (OSCE/ODIHR) and the Organisation for Economic Co-operation and Development (OECD). In this respect, the OECD register of AI Incidents and Hazards (OECD AI Incidents Monitor, an evidence base for trustworthy AI – OECD.AI) may be particularly relevant.
- Findings from domestic specialised bodies, including ombudspersons, equality bodies and NGOs.
- Administrative registers, such as central and local population registers.
- Complaints data such as statistics emanating from the police, prosecutors and court case files and registers.
- Academic and ad hoc research, including findings from EU research institutions such as the European Union Agency for Fundamental Rights (FRA) and European Institute for Gender Equality (EIGE). A search by domain in the MIT AI Risk Repository may also be insightful.
- Comparative information on case law, policies and practices across the member states ("European consensus" data).

2.1.3. Information provided by the respondent or other parties

Information requested from the respondent using national or other Union law powers

Equality bodies could request information from respondents and other parties, for example the deployer or provider of the system (if this is a different organisation from the respondent), by exercising their investigative and information-gathering powers under relevant legislation, including national laws implementing the standards

directives,[34] freedom of information legislation and international instruments such as the Council of Europe Framework Convention on Artificial Intelligence,[35] or by using collaborative channels with national data-protection authorities.

Information may be disclosed during investigations, negotiations and pre-action correspondence or in the course of litigation.

Inquiries: standards directives (Article 8)

Article 8 of Directives 2024/1499 and 2024/1500 could strengthen equality bodies' rights of access to information, particularly:

- under Article 8(1) of the standards directives, member states must empower equality bodies to conduct an inquiry into whether a breach of the principle of equal treatment has occurred;
- under Article 8(2) of the standards directives, member states must provide a framework for conducting inquiries that enable equality bodies to carry out fact-finding, including:
  - effective rights to access information and documents that are necessary to establish whether discrimination has occurred;
  - appropriate mechanisms for equality bodies to co-operate with relevant public bodies for that purpose.

It is important to note that Article 8(3) provides for member states to entrust another competent body with these powers. This could, for example, be the MSA. In that case it would be the MSA exercising the Article 8(1) and (2) powers. Where such a competent body has completed its inquiry it shall provide the equality body, upon its request, with information about the results of the inquiry.

If the MSA was entrusted with these powers, it is important to note that in the AI Act this requires co-operation with the EB (Article 79(2)).

- Inquiries could be particularly relevant in a case involving systems classed as non-high risk where it has proved difficult to obtain documentary evidence or where there is a suspicion of group discrimination but insufficient evidence in individual cases.

Note: no inquiries can be initiated or continued with while court proceedings in the same case are pending. Inquiries are likely to be governed by national law provisions.

34. Under Article 16 of the standards directives, equality bodies have a variety of data-collection powers, including collecting data to produce reports to conduct independent surveys (Article 16(2)) and the right to access statistical data where necessary to make an overall assessment of the situation regarding discrimination in the member State and for drawing up reports (Article 16(3)).
35. The Council of Europe Framework Convention on AI (2024) provides that parties shall adopt or maintain measures to ensure adequate transparency and oversight requirements (Article 8), and to ensure accountability and responsibility for adverse impacts on human rights (Article 9). Particularly, Article 14 requires parties to guarantee accessible and effective remedies, including documenting and providing information on AI systems with significant human rights impact to authorised bodies and, where appropriate, affected persons, so that individuals can contest AI-driven decisions and lodge complaints with competent authorities.

Data protection impact assessment (DPIA)

Any processing of personal data that is likely to result in a high risk to data subjects' rights due to its nature, scope, context or purposes requires the data controller to carry out a DPIA in accordance with Article 35(1) of the GDPR. Accordingly, DPIAs are highly relevant in cases involving automated decision making and profiling through algorithmic systems (Article 35(3) of the GDPR). However, aside from a narrow set of deployers of high-risk AI systems who have publishing obligations under the AI Act (see also DPIA under step 2.2.3 below), there is no legal requirement under either the GDPR or the AI Act for the deployer to publish or provide the DPIA to an equality body. Any control over the impact assessment is left to the initiative of the DPAs – collaboration channels with DPAs might be relevant in that regard. This should not discourage the equality body from making such a request. Some organisations may agree to provide the DPIA if available – either under Article 35(3) of the GDPR or voluntarily – or may even choose to publish a summary of it. The DPIA may be requested during pre-action correspondence or if litigation is brought.

Human or fundamental rights impact assessments (HRIA/FRIA)

An explicit obligation to carry out any type of FRIA is foreseen in the AI Act only for certain deployers and providers of high-risk AI systems (see also fundamental rights impact assessment under step 2.2.3 below). For other algorithmic or AI systems, no such obligation exists under the AI Act. However, this does not prevent providers from adopting such instruments voluntarily (European Center for Not-for-Profit Law and Danish Institute for Human Rights 2025; FRA 2025), based on their overarching obligation to respect and protect fundamental rights established at EU and national levels, and as a means of enhancing the accountability of AI operators in this regard (Mantelero 2024).

Particularly, an HRIA is a general term for the process and the tool of identifying, evaluating and addressing potential and actual adverse impacts of products or activities on human rights and there are various forms in which it can be carried out. The HUDERIA methodology and model developed by the Council of Europe is one type of human rights risk assessment (Council of Europe 2025c, 2026).

Similarly, an HRIA or FRIA may have been carried out by developers on a voluntary basis for non-high-risk AI systems – including under their own due diligence or human rights commitments or in accordance with frameworks such as the UN Guiding Principles on Business and Human Rights. National or regional laws, policies or practices may also require human or fundamental rights impact assessments to be conducted and published.

In all these cases, equality bodies may seek disclosure of these assessments as part of their information-gathering powers.

Equality or gender impact assessment

Where such assessments are required under national law, equality bodies may request them. There may be no legal requirement to conduct or provide them.

Documentation under the AI Act framework

Where a system is not classified as high risk, equality bodies may still request comparable information from the deployer or provider, relying on their investigative or information-gathering powers. While respondents are not legally obliged to have drafted and/or provided such documentation for non-high-risk or non-AI systems, equality bodies may be guided by the AI Act framework in structuring their requests and evaluate the respondent's reaction – or inaction – accordingly at step 3 and step 4.

Surveys and statistical information

Equality bodies may conduct or access surveys, including sample surveys that chart the experiences of groups exposed to discrimination, and opinion surveys that measure the prevalence of prejudices (standards directives, Article 16). They may also access relevant official statistical sources, such as those compiled by national statistical bureaus in the context of the EU non-discrimination directives, as well as data gathered through population censuses and other major sources like the Labour Force Survey (LFS) and the Survey on Income and Living Conditions (SILC).

Standards directives

- Under Article 16(2) of Directives 2024/1499 and 2024/1500, equality bodies may conduct independent surveys concerning discrimination.
- Under Article 16(3) of Directives 2024/1499 and 2024/1500, equality bodies must be able to access statistics related to the rights and obligations derived from the EU anti-discrimination directives where necessary to make an overall assessment of the situation regarding discrimination in the member state, and to draw up periodic reports on the state of equality in their member state.

Documentation under other product safety legislation

For non-high-risk products sold by a business to a consumer, there may be requirements under the General Product Safety Regulation[36] (GPSR) and MSA Regulation,[37] which include obligations and documentation requirements similar to those in the AI Act. This is outside the scope of this methodology because the powers belong to the MSA; however, this is mentioned because the GPSR is considered a safety net for non-high-risk AI (Recital 166 of the AI Act) and its requirements may lead to relevant documentation being available either directly to the individual or by the equality body acting in co-operation with the MSA. For example, manufacturers covered by the regulation are required to ensure their product is accompanied by clear instructions and safety instructions for consumers (Article 9(7)) and to draw up technical documentation and conduct risk assessments that must be made available to the MSA (Articles 9(2)-(3) and 15).

36. Regulation (EU) 2023/988.
37. Regulation (EU) 2019/1020.

2.2. Additional information available for high-risk AI systems

2.2.1. Additional Information available to the complainant

Making and obtaining a response to an explanation request pursuant to Article 86 of the AI Act

This right can be asserted in addition to the DSAR request (see Making and obtaining a response to a data subject access request (DSAR) pursuant to Article 15 of the GDPR). Any person subject to a decision that significantly and adversely affects them, which is taken based on the output of a high-risk AI system, has a right to obtain information on the role of the AI system in the decision-making process and the main elements of the decision. These should be clear and meaningful explanations. Properly handled responses may contain highly relevant information, including the input data and decision's influencing criteria (see step 3 for details) for the subsequent identification of prima facie discrimination. If a complainant has not yet submitted such a request, it is recommended to encourage them to do so before proceeding further with any complaint or investigation. For a template see Appendix B.

This right only applies to the extent that the right is not otherwise provided for under Union law. For example, if the algorithmic system is a fully automated system processing the personal data of the affected person, it may be that the right to an explanation is provided under the GDPR at Articles 13-15 (Regulation (EU) 2016/679) When the respondent dismisses the explanation request with this motivation, a follow-up request under the GDPR (other relevant Union law) would be the next step (unless already exercised). For a template see Appendix A.

2.2.2. Publicly available information

EU Database

See also 1.2.1 EU Database.

In step 1, you conducted a preliminary check of the EU database. If the respondent is listed, you should have already identified whether they are listed in the database as:

- a provider, listed in section A or B of the database:
  - for a high-risk use case that is relevant in the situation of the complainant;
  - for a use case that is intended for use in a high-risk domain, but falls under the exception in Article 6(3) of the AI Act;
- a deployer, listed in part C of the database:
  - a deployer for a use case that is relevant in the situation of the complaint; which organisation is the provider?

Below are the main points of interest in the database (AI Act, Annex VIII).

Section A: high-risk AI systems

- Contact details of the provider and authorised representative.
- Trade name or other reference enabling identification traceability of the AI system (this could be useful for example where a high-risk system is used as part of another system).
- Intended purpose.
- Information used by the system (data, inputs) and its operating logic (not applicable to systems in law enforcement, migration, asylum and border control).
- Status of the AI system (for example, is it still on the market?).
- Type, number and expiry date of the certificate issued by the notified body and name or identification number of that body and a scanned copy of the certificate (not applicable to systems in law enforcement, migration, asylum and border control).
- Member states where the system is or has been marketed (useful for co-operation with other authorities).
- A copy of the EU declaration of conformity (AI Act, Article 47).
- Electronic instructions for use (not applicable to systems in law enforcement or migration, asylum and border control).

Section B: AI system for which the provider has concluded that it is not high-risk

- Contact details of the provider and authorised representative.
- Trade name or other reference enabling identification and tracing of the AI system.
- Intended purpose.
- Relevant Article 6(3) condition and justification for why the system is not considered high risk (not applicable to law enforcement, migration, asylum, or border control).
- The status of the AI system (is it still on the market?).
- Member states where the system is or has been marketed.

Section C: deployers of high-risk systems (AI Act, Article 49(3))

- Name and contact details of deployer (only public authorities, EU institutions, bodies and agencies – or persons acting on their behalf).
- URL of the AI system's entry in the EU database (as registered by the provider).
- Summary of the fundamental rights impact assessment (FRIA) (not applicable to law enforcement, migration, asylum, or border control).
- Summary of the data-protection impact assessment (DPIA).

Not all high-risk AI systems are listed in the public section of the EU database.

The table below shows in which use cases information should be provided in the database.

Table 3. Information available in EU and national-level high-risk database

Public section (Article 49(1)-(3)), (except private deployers unless acting for a public body)	Non-public section (Article 49(4))	National implementation/ registry (Article 49(5))
All the information described below is required and is included in the public section of the database.	Limited amount of information is required and it is included only in a secure non-public section of the database.	Registration requirements apply only at national level.
Education and vocational training	Law enforcement	Critical infrastructure
Employment, worker management and access to self-employment	Migration, asylum and border control	
Essential services and benefits	High-risk AI systems under testing	
Administration of justice and democratic processes	Biometrics used for law enforcement, migration, asylum and border control purposes	

Restrictions on access to information

According to Article 49(4)(d) of the AI Act, for high-risk AI systems in law enforcement, migration, asylum and border control management (points 1, 6 and 7 of Annex III), information on the AI system as recorded in the EU database is registered in a non-public section and accessible only to the European Commission and the relevant MSAs. For these purposes only the data-protection authority or the European Data Protection Supervisor (EDPS, for the Commission) will be the relevant MSAs (Article 74(8) and (9)) and have access to the information in the database.

This does not mean that the material those records are based on are also unavailable. It does however mean that more is required to justify access to the documents and that access could be refused. EBs who are Article 77 authorities have a power to request and access any documentation created or maintained under the regulation (see below, step 2.2.3). Any such request must be sufficiently well justified to demonstrate that it is necessary for effectively fulfilling their mandate within the limits of their jurisdiction.

The act also makes very clear that market surveillance activities "shall in no way affect the independence of judicial authorities or otherwise interfere with their activities when acting in a judicial capacity" (Article 74(8)). This means that in respect of any relevant information that should be made available to the EB or an individual through judicial procedures, the restrictions of Article 74(8) do not apply.

The availability of sensitive material, even through these procedures, is likely to be governed by other confidentiality requirements and public and national security interests (see Confidentiality).

If legal bases for information sharing between equality bodies, market surveillance authorities and other Article 77 authorities is established (see Co-operation across sectors), then it would be possible for equality bodies to access information obtained by market surveillance authorities under Article 71(4) and 49(4) (Council of Europe 2025b).

2.2.3. Additional information provided by the respondent or other parties

AI Act documentation and reporting obligations

See also EU AI Act, Article 77: Powers of authorities protecting fundamental rights.

The AI Act creates obligations for providers and deployers of high-risk AI systems to create and maintain various types of documentation throughout the system's life cycle. Equality bodies who are Article 77 authorities have the power to request and access any documentation created or maintained under the AI Act in accessible language and format, necessary for effectively fulfilling their mandates within the limits of their jurisdiction.[38] (EU AI Act, Article 77)

This documentation is listed in the table of different types of technical documentation below.

It is advised to request all this information, as all these documents together provide a clear picture of the use, design, data and risks of the system.

Step 3 provides detailed explanations of what this information will show and how you can use it.

The documentation will likely be organised based on universal and sector-specific documentation standards developed by the industry in recent years, including references to "datasheets" and "model cards" in Annex IV. For equality bodies it would be helpful to be aware of these two types of documentation (Mittelstadt 2024). The required structure and content of these types of documentation will be bound by Joint Technical Committee-21 (JTC-21) standards (see below, Harmonised standards).

See also Co-operation across sectors.

The following describes a list of requirements that should be met for high-risk AI systems under the AI Act. While not all requirements explicitly require documentation, it is safe to assume that at least internal documentation on each of these requirements will exist.

38. Equality bodies that do not fall under Article 77 do not have an additional direct legal basis under the AI Act for accessing relevant documentation for high-risk AI systems and will have to rely on their existing powers. It remains questionable if they will be able to gain sufficient insight into the functioning of high-risk AI systems to effectively carry out their mandates.

Table 4. Requirements for high-risk AI systems under the EU AI Act

Requirement (article)	Description of obligation	Role
Risk management system (Article 9)	Risk-management system that identifies and analyses reasonably foreseeable risks to health, safety or fundamental rights, according to risk-management measures.	Provider
Data and data governance (Article 10)	Training, validation and testing data sets shall be subject to data governance. Practices include design choices, data collection and origin, relevant preparation, formulated assumptions, examination of biases and appropriate measures to prevent bias.	Provider
Technical documentation for high-risk AI systems (Article 11, Annex IV)	General description of AI system and detailed description of certain elements and processes. A more detailed description is offered in the table below.	Provider
Record keeping (Article 12)	Systems should record events relevant for identifying a risk to health, safety or fundamental rights and facilitate post-market monitoring. This includes recording period of use, reference database, input data and identification of natural persons involved in the verification of results.	Provider
Instructions for use (Article 13) and **human oversight (Article 14)**	Operations for systems should be sufficiently transparent. This includes characteristics, capabilities and limitations of the system, alongside its intended purpose and performance metrics. Next to that, human oversight and resources needed for the functioning of the system should be included.	Provider to deployer
Quality management system (Article 17)	Documentation of policies, procedures and instructions, including compliance strategy, design and quality control techniques, examination prior, during and after development. Also includes technical specifications and systems for data management. Finally, documentation regarding serious incident response, communication with authorities, record keeping, resource management and responsibility division.	Provider

Requirement (article)	Description of obligation	Role
Automatically generated logs (Article 19)	Providers must keep automatically generated logs for at least six months. Financial institutions maintain the logs pursuant to the relevant financial services law.	Provider
Automatically generated logs (Article 26)	Deployers must keep automatically generated logs at least six months. Financial institutions maintain the logs pursuant to the relevant financial services law.	Deployer
Fundamental rights impact assessment (Article 27)	Although exceptions apply, deployers must perform an assessment of the impact on fundamental rights that the use of the system may produce. This includes the processes in line with intended purpose, description of time frame and frequency, categories of persons afflicted, specific risks of harm, human oversight measures and measures taken in case risk materialises.	Deployer
EU declaration of conformity (Article 47, Annex V)	Provider must draw up a (machine readable) written, signed EU declaration of conformity for each high-risk AI system, available to national authorities for 10 years after it has been placed on the market, which states it meets the requirements set out in section 2 of the AI Act.	Provider
CE marking (Article 48)	Systems are subject to the general principles set out in Article 30 of Regulation (EC) No. 765/2008 and shall be applied a CE marking.	Provider
Post-market monitoring data (Article 72)	Providers must establish a post-market monitoring system, which collects, documents and analyses relevant data on the performance of the system, to allow for compliance evaluation.	Provider
Incident reporting (Article 73)	Providers are required to report serious incidents to the market surveillance authorities of the respective member state.	Provider to the MSA. The MSA to involve EBs.

The technical documentation required from providers under Article. 11 of the AI Act, in combination with Annex IV of the AI Act, will serve as a particularly useful resource for EBs.

The following table zooms in on this technical documentation and points equality bodies towards those required elements that may be relevant for the purpose of applying this methodology.

Table 5. Different types of technical documentation under Article 11 and Annex IV (adapted with permission from Mittelstadt 2024)

Type of documentation	Explanation
1. General description of the AI system	This includes: ▸ intended purpose ▸ interactions with the system ▸ version management and reflection ▸ appearance in software and hardware, or products it is a component of ▸ hardware it is intended to be used on ▸ user-interface and instructions for the deployer.
2. Design specifications	This includes: ▸ methods and steps for the development of the system ▸ design specifications; logic, algorithm and key choices, including assumptions and optimisation choice ▸ relevance of chosen parameters ▸ expected output and its quality ▸ possible trade-offs regarding compliance.
3. System architecture	Explanation of the structure of software components, their interaction and integration alongside computational resources used for development, training, testing and validation.
4. Data requirements	Data requirements include datasheets describing training methods, techniques and datasets used with information about their origins, scope and characteristics, obtainment, labelling procedures and cleaning methods.
5. Human oversight	Assessment of the human oversight measures implemented in accordance with Article 14, with technical measures needed in order to facilitate interpretation of the AI system by deployers.
6. Performance measures	Validation and testing procedures used, along with information about the main characteristics of testing data, metrics used for measuring accuracy, robustness and compliance, as well as potentially discriminatory impacts. Also contains all test logs and test reports, including predetermined changes.
7. Capabilities	Detailed information about the monitoring, functioning and control of the AI system is required, specifically its capabilities and limitation. This includes degrees of accuracy for specific groups.

Type of documentation	Explanation
8. Risk management	Risk-management system as described in Article 9.
9. Post-market monitoring	A detailed description of the system in place to evaluate the system's performance post-market in accordance with Article 72.
10. Other EU legislation	Harmonised standards applied, copy of EU declaration of conformity (Article 47).

Harmonised standards

Harmonised standards are technical standards currently under development by European standardisation organisations (CEN/CENELEC) that, if followed, will confer providers of high-risk AI systems with a "presumption of conformity" with the AI Act. In practice, this will likely cover a wide range of information elements, including those needed to support understanding of how the AI system works, its characteristics, capabilities, strengths, limitations and performance, in line with the legal text (Soler Garrido et al. 2024)

The following standards under development have been considered particularly important for setting the requirements of technical documentation available to equality bodies.[39]

- **JT021036** "Artificial intelligence – Concepts, measures and requirements for managing bias in AI systems": the purpose of this standard is to define "concepts, measures and requirements for assessment and treatment of bias in AI systems. This includes bias unwanted by the AI provider and AI deployer according to their specification of the AI system, in the context of the AI Act".
- **JT021008** "AI trustworthiness framework", parts 1 (logging), 2 (accuracy and robustness) and 3 (transparency and human oversight): the purpose of this standard is to define terminology, concepts, requirements, and guidance on logging, accuracy, robustness, transparency and human oversight.
- **JT021024** "AI risk management": the purpose of this standard is to define requirements and provide guidance for risk management of AI systems throughout the entire life cycle of the AI system. This document requires providers to establish objective criteria for risk acceptability but does not specify acceptable risk levels.

These standards are unlikely to define thresholds or explain how different treatment between people or groups of people would be illegal discrimination. According to Mittelstadt (2024), EBs should be aware that standards will set expectations about how bias can be measured and mitigated in AI systems but will not determine whether these biases are illegal or unethical.

39. For a list and description of all standards currently being developed see CEN/CENELEC, "CEN/CLC/JTC 21 Work Programme" CEN - CEN/CLC/JTC 21, accessed 25 June 2026. Other standards, including pre-existing international standardisation work (such as ISO/IEC standards) can be also relevant when addressing bias and transparency in AI systems. International standards are typically not free of charge and are subject to intellectual property protections, challenging the ability of equality bodies to access them.

Standards, conformity assessments and certificates

High-risk systems in conformity with harmonised standards shall be presumed to be in conformity with the requirements of section 2 of the AI Act (requirements for high-risk ai systems). However, it is important to note that compliance with transparency or other obligations does not indicate that use of AI system or its output is lawful under regulation or other law and should be without prejudice to other transparency obligations for deployers of AI systems laid down in Union or national law (Recital 137). Providers must list the harmonised standards applied to the AI system. Where harmonised standards have not been used, providers must explain how the requirements of the AI Act (Chapter III, section 2, of the AI Act) have been otherwise met, for example through usage of other relevant standards and technical specifications. This should enable equality bodies to determine when a relevant bias, trustworthiness or harmonised risk-management standard has been followed.

Impact of a presumption of conformity

Any presumption of conformity does not preclude investigation or taking action in respect of discrimination or other human rights risks. First, the AI Act itself recognises that an AI system that is compliant with the regulation may still present risk and at Article 82 provides a procedure for dealing with this situation. Similarly, Article 7(3) of the General Product Safety Regulation (EU) 2023/988 (which may apply to non-high-risk AI systems) provides that the presumption of conformity with the general safety requirement in the regulation shall not prevent the MSA from taking all appropriate measures under the regulation where there is evidence that, despite the presumption, the product is dangerous.

Note: under the MSA Regulation (EU) 2019/1020 where an economic operator presents test reports or certificates attesting to the conformity of their product with Union harmonisation legislation, the MSA must take "due account" of the report or certificate.

Fundamental rights impact assessment

The requirement to conduct a fundamental rights impact assessment (FRIA) applies only to certain deployers of high-risk AI systems, as provided for in Article 27 of the AI Act and Annex III 5(b) and (c) of the AI Act. This includes:

a. deployers of high-risk AI systems that are public bodies or private entities providing public services;
b. deployers of high-risk AI systems used to evaluate the creditworthiness of natural persons or to establish their credit score (except for AI systems used for the detection of financial fraud), and those used to assess risks or determine pricing in life and health insurance.

Under the Digital Omnibus on AI there is recognition that there is cross-over between the FRIA and the DPIA. Thus, it may be necessary to request the DPIA if it is cross-referenced rather than incorporated into the FRIA.[40]

Following the completion of the FRIA, the deployer is, under Article 27(3) and (5) of the AI Act, obliged to notify the competent MSA of the FRIA's results by submitting a filled-out (standardised) template. In addition, a summary of the FRIA's findings must be submitted by the deployer as part of their registration process in the EU database, for those who have registration obligations under Article 49(3) of the AI Act. Deployers under the second category (those in the credit and insurance sector) are not subject to this obligation. Equality bodies are therefore expected to find a summary in section C of the EU database, as set out in Annex VIII, only for the mandatory FRIAs conducted by public bodies or private entities deployers falling under the first category.

Note: the application of both obligations is limited in the case of public authorities deploying high-risk AI systems in the areas of law enforcement, migration, asylum, and border control. Under Article 49(4) of the AI Act, a summary of the FRIA's findings is not to be submitted to the EU database at all – not even in its secure, non-public section. In addition, under Article 27(3) of the AI Act, such deployers, in exceptional cases – including for reasons of public security – may be exempt from the obligation to notify the market surveillance authorities (MSAs) of the FRIA's results, following the derogation from the conformity assessment procedure described in Article 46(1) of the AI Act (see also the box below on the area of law enforcement). The possibilities for equality bodies to access information in such cases are therefore limited based on the AI Act.

Deployers of other categories of high-risk AI systems – for example, a recruitment company using AI to screen or select candidates – are not legally required to carry out an FRIA. However, this does not necessarily mean that an FRIA is not conducted in such cases. Some organisations may do so pursuant to national legislation, in accordance with frameworks such as the UN Guiding Principles on Business and Human Rights, or to align with their own due diligence or human rights commitments. In these cases, equality bodies may seek disclosure as part of their information-gathering powers.

Providers of high-risk AI systems do not fall under the requirement to conduct a fundamental rights impact assessment of the specific type referred to in Article 27 of the AI Act. However, conducting an FRIA as a general tool for identifying, evaluating and addressing potential or actual adverse impacts on fundamental rights, rooted in the human rights impact assessment (HRIA) framework, is part of the conformity assessment and provider's obligation for a risk management and quality management system, as set out in Articles 9(2), 17(1)(g) and 43 of the AI Act (Mantelero 2024). This type of impact assessment would typically follow a standards-based approach and may likewise be requested, together with the rest of the documentation maintained under the AI Act, by equality bodies exercising their powers under Article 77 of the AI Act (see above, under 2.1.3).

40. Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). Available at: https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng, accessed 24 July 2026.

In addition to the legal requirements under the EU AI Act, national or regional laws, policies or practices may require human or fundamental rights impact assessments to be conducted and, in some cases, made public. In these cases, equality bodies may seek disclosure as part of their information-gathering powers.

Data protection impact assessment (DPIA)

Any processing of personal data that is likely to result in a high risk to data subjects' rights due to its nature, scope, context or purposes requires the data controller to carry out a data protection impact assessment (DPIA) in accordance with Article 35(1) of the GDPR. Accordingly, DPIAs are by definition highly relevant in cases of high-risk AI systems involving personal data processing, automated decision making and profiling (cf. Article 35(3) of the GDPR).

However, submission of summaries of DPIAs in the EU database (section C) is required only for certain narrow sets of deployers of high-risk AI systems, who are required to register their use of AI in the EU database under Article 49(3). This includes public authorities, Union institutions, bodies, offices and agencies – or persons acting on their behalf who use high-risk AI systems. For the rest of deployers and high-risk AI systems there is no direct legal requirement under either the GDPR or the AI Act to publish or provide the DPIA to an equality body. Any control over the impact assessment is left to the initiative of the DPAs – collaboration channels with DPAs might be relevant in that regard. This should not discourage the equality body from making such a request, as part of their information-gathering powers under national law. Some organisations may agree to provide the DPIA if available or may even choose to publish a summary of it. The DPIA may be requested during pre-action correspondence or if litigation is brough.

The Digital Omnibus regulation proposal[41] requires the EDPB to draw up single, EU-wide lists of processing activities that do, or do not, require a DPIA, alongside a common methodology and template,[42] which is expected to replace the current fragmented system of national lists and harmonise these lists at the EU level.

2.2.4. MSA notification or *ex officio* investigation

The equality body can expect to receive information from the MSA about AI systems that represent a risk to non-discrimination rights or are involved in serious incidents infringing those rights. For details on the type of information to be expected, see 1.1 C: Informed by MSA.

EBs could obtain the AI Act documentation from the MSAs if an MSA has already accessed the same from the provider. This could accelerate the process of access

41. Article 3 Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), EUR-Lex - 52025PC0837 - EN - EUR-Lex, accessed 25 June 2026.
42. The European Data Protection Board was consulting in May 2026 on a DPIA template, which is available here: www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template_en.

for EBs. Respondents cannot prevent MSAs from sharing the documentation with EBs under the guise of trade secret protection, particularly where EBs request the documentation through the MSA (Council of Europe 2025b). For an analogous example of this being applied in practice see *CK v. Dun & Bradstreet Austria GmbH and Magistradt der Stadt Wien*, paragraph 76.

When the case is handled as part of an *ex officio* investigation or a notification by an MSA, consider:

- seeking the disclosure of documents from the MSA that are necessary for the EB investigation;
- convening a round table or workshop with relevant NGOs or other interested organisations and using the discussion to gather relevant information;
- raising awareness and conducting consultations to identify affected persons or groups, including through surveys or other participatory information-gathering processes.

Area of law enforcement

Possibilities for information gathering will be more limited in the context of law enforcement, making it more difficult to identify the use of AI or algorithmic systems and any resulting discrimination.[43]

AI Act

- Under Article 49(4) of the AI Act, the registration of high-risk AI systems in the areas of law enforcement, migration, asylum and border control management not only is to take place in a secure non-public section of the EU database referred to in Article 71 of the AI Act but should also only include a specific set of limited information, excluding for example information on input data and its operating logic. This non-public database is further accessible by the MSAs designated for law enforcement and border control AI systems in accordance with Article 74(8) and in principle not accessible to the EBs. For further information see Restrictions on access to information under 2.2.2.
- In line with Article 27(1) of the AI Act, law-enforcement authorities are, as public authorities, required to conduct a fundamental rights impact assessment (FRIA) prior to deploying a high-risk AI system. However, two exceptions apply in this regard. First, under Article 49(4)(c) of the AI Act, such deployers shall not submit a summary of the FRIA's or DPIA's findings to the EU database – not even in its secure, non-public section. Second, they may, in exceptional cases, including for reasons of public security, be allowed by the MSA to place a high-risk AI system on the market or put it into service without complying with conformity assessment procedures or in "urgent" cases without authorisation at all (Articles 46(1) and 46(2) of the AI Act). This would under Article 27(3) of the AI Act also include exemption from the obligation to notify the MSA of the FRIA's results.

43. For a comparison between algorithmic data rights in the GDPR and the LED, see González Fuster (2020).

Note: Articles 27 and 46 of the AI Act do not provide any exemption from the requirement to conduct the FRIA altogether, and the condition in Article 46(1) is specifically limited to the "limited period while the necessary conformity assessment procedures are being carried out". Article 46(2) further requires that, in urgent cases, authorisation be sought "during or after the use, without undue delay".

It is important to note that if the authorisation is subsequently refused:

- the use of the high-risk system shall be stopped with immediate effect;
- all the results and outputs of such use shall be immediately discarded.

The possible routes for equality bodies to access information related to both the DPIA and FRIA are discussed below

Law-enforcement directive

In addition, the law-enforcement directive (LED)[44] provides for several exceptions and possible restrictions to informational rights of individuals through national transpositions, if it is necessary in order to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties and to protect public and national security (Article 13(3) and 15 of the LED).

Accordingly, practices differ among member states regarding the type of information that is to be provided and how it could be accessed; therefore, reference to national law is crucial in this area.

Automated decision making

- Article 11 of the LED prohibits certain forms of automated processing, including profiling, and requires that such processing be explicitly authorised by Union or member state law subject to appropriate safeguards for the rights and freedoms of the data subject. The minimum level of protection required is the right to obtain human intervention on the part of the controller. It will be necessary to consider national frameworks governing automated processing by law enforcement to discover what information about automated processing should be available. For different transposition in various member states see Vogiatzoglou and Marquiene 2022; see also Recital 38.
- Article 13 and 14 of the LED does not explicitly stipulate information obligations regarding the use of automated decision making, including profiling.

Information disclosure

- Under Article 13(1) of the LED, data controllers are obliged to provide certain minimum information, including their identity and the contact details of the controller, the data subjects' right of access to their personal data and the intended purposes of the data processing.

44. Reference to the LED with regard to information sources shall not be deemed to be exhaustive; other instruments in the broader area of freedom, security, and justice such as SIS II Council Decision, VIS and EURODAC may also contain substantive and procedural rules on the rights of data subjects, including the rights to information and access.

That information does not concern a certain data subject, but a certain processing procedure and all data subjects potentially affected by it. It is usually made available on the competent authority's dedicated website. It has been reported that it is not always easy or possible to find the relevant information on the website of the centralised entity governing the law-enforcement authorities, national police authority or the competent ministry (Vogiatzoglou and Marquiene 2022).

- Article 13(2) of the LED enlarges the scope of information to be shared with data subjects, including the legal basis for the processing and, where applicable, the categories of recipients that the personal data shall be shared with, and, where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject. Under Article 13(3) this can be delayed, restricted or even omitted under national law if such a measure meets the standards of being necessary and proportionate in a democratic society.

Such information, if specific enough, can be offered on the website, along with the minimum information.

Right of access

- Under Article 14 of the LED, data subjects are granted the right to access more information about the data-processing activities than the general information made available to the public, including the purposes of the processing operation, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed, as well as communication of the data undergoing processing and of their origin.

Unlike the GDPR, the article does not explicitly provide for the right to be informed about the existence and the logic of automated decision making nor the potential consequences for the data subject. However, law-enforcement authorities may be obliged under national laws to disclose information about the way an individual was profiled.

- Under Recital 43 of the LED the provided information does not need to include an actual copy of the data processed, as for example in the GDPR; instead, a full summary is sufficient.
  The content of the response – when access is not refused on formalistic grounds – is often reduced to standardised replies that are brief and devoid of substantive information yet still deemed formally compliant (Erdogan 2024).
- Under Article 15 of the LED, the right of access may be delayed, restricted or even omitted under national law, if such a measure is necessary and proportionate in a democratic society for the protection of, *inter alia*, public or national security, or for the unimpeded conduct of official or legal inquiries, investigations or proceedings.

Access request

- Article 14 and 17(3) of the LED foresee two types of procedure for the exercise of the right of access. First, the "direct access" procedure contained in Article 14 of the LED, where individuals can turn directly to the law-enforcement body, the controllers, with questions about their personal data. Second,

an exceptional procedure, the "indirect" access, where the right of access is undertaken by the national data-protection authority (DPA) acting as an intermediary.

National laws implementing the system of indirect access, such as in Belgium where indirect access is the default, have been criticised for their structural and procedural shortcomings (Dimitrova and De Hert 2024), which restrict the effective monitoring of data-processing activities and the communication of relevant information to the data subjects concerned.

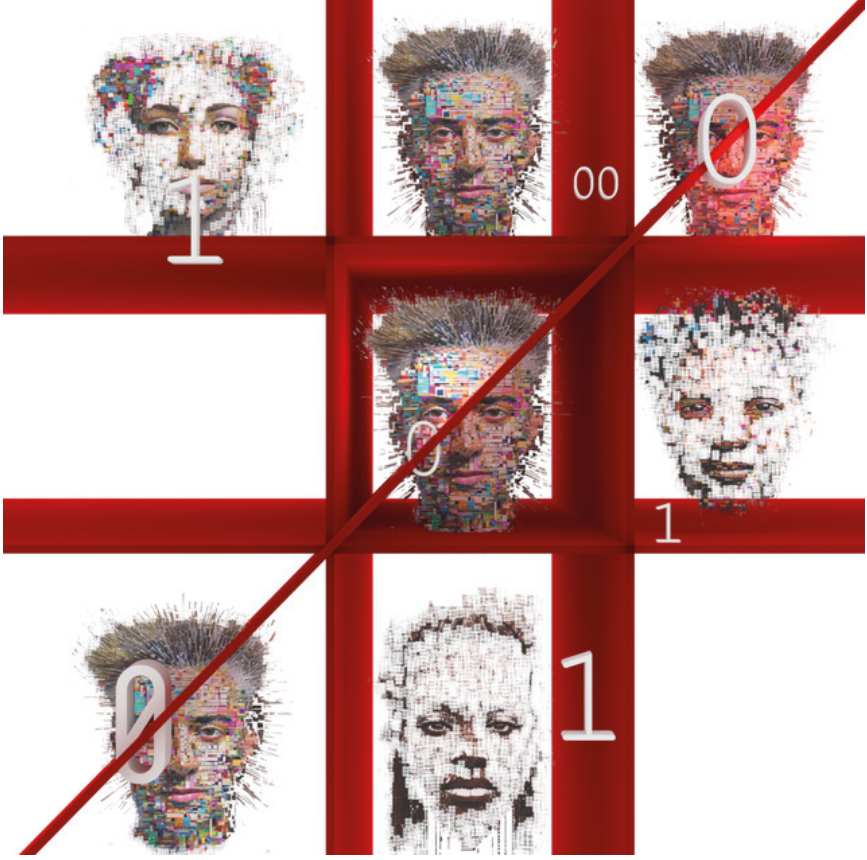
Note: where information is gathered by a competent authority for law-enforcement purposes, it falls within the scope of the LED – for example, data relating to an individual's previous criminal history. Where the information is scraped from another public source or collected for purposes other than law enforcement (such as civil, employment or education status), it falls under the scope of the GDPR. In certain AI systems used by law enforcement, both types of input data may be used, and care must therefore be taken to determine whether the applicable information rights are governed by the GDPR or the LED. This situation becomes even more complex where private companies are involved in software development or in processing or controlling relevant data (see Erdogan 2023). In cases of uncertainty, specialist law advice should be sought.

Records of processing activities

- Under Article 24 of the LED, controllers are obliged to keep a registry of processing operations, including information on the purposes of the processing; the categories of recipients to whom the personal data have been or will be disclosed; and, where applicable, the use of profiling. Those shall be made available to the data-protection authorities upon request (for collaboration possibilities with DPAs, see Co-operation across sectors).

Data-protection impact assessment (DPIA)

In the context of law enforcement, Article 27 of the LED requires a data-protection impact assessment where a type of processing using new technologies is likely to result in a high risk to the rights and freedoms of natural persons. DPIA obligations will differ in member states based on national transpositions. Article 29 of the Data Protection Working Party recommended that national legislators place an obligation upon controllers to carry out a DPIA in connection with automated decisions. However as with the FRIAs, law-enforcement authorities are not required to submit a summary of it to the EU database (Article 49(4)(c) of the AI Act).



Step 3

Methodology for assessing received information

Step 3 introduces the types of discrimination caused by AI systems whether used for automated decision making or to assist decision makers.

The introduction to concepts sets out the types of discrimination and applies them to an AI context. New concepts for equality bodies may include proxy discrimination and variables. It also introduces identifying and establishing a presumption or prima facie case of discrimination.

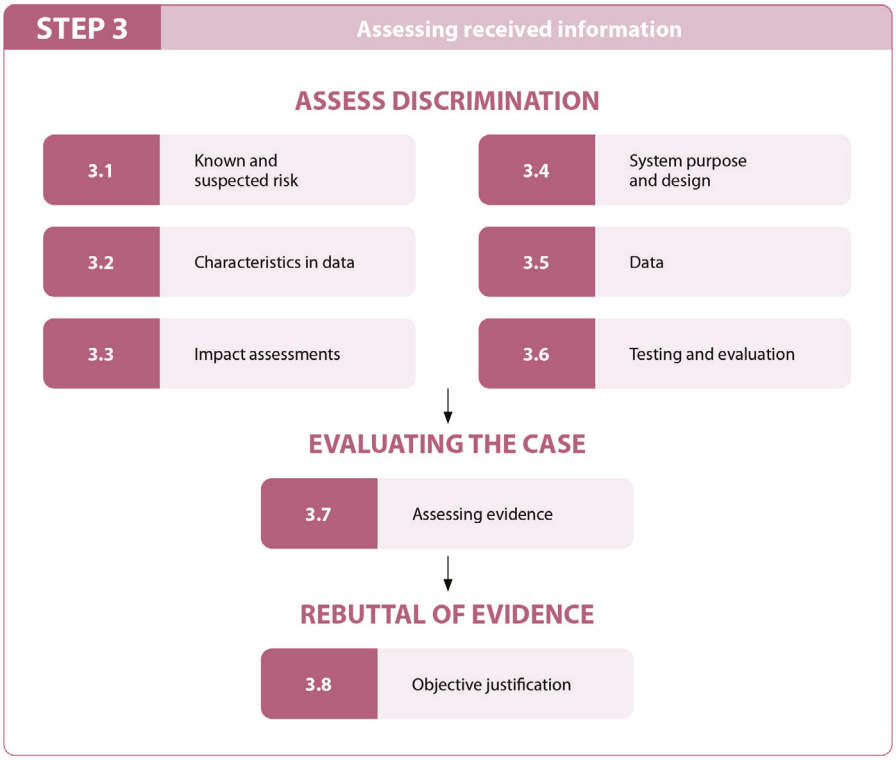
The operative part of step 3 is designed to help caseworkers evaluate the information received under step 2 and the sample record sheet at Appendix K can be used alongside to record that information. In steps 3.2 to 3.6 the caseworker is provided with a short explanation, a set of questions to consider, potential sources of information that may help answer those questions and example indicators of discrimination or discriminatory practice.

Step 3.7 draws all those findings together and provides a guide to assessing whether a presumption of discrimination is made out and, importantly, what to do when the available evidence is insufficient or there is a lack of transparency.

Step 3.8 provides guidance on evaluating the likelihood that the respondent may be able to rebut or provide a justification for any discrimination.

It is not expected that caseworkers will be able to answer all questions or have access to all documents or evidence. Instead, we hope that it will enable caseworkers to do the best with the information that is available and to understand its relevance.

Figure 4. Step 3 – Assessing received information



In step 2, you should have started the process of gathering relevant documentation and other evidence. In step 3, you will use that evidence to assess whether you can establish a presumption or prima facie case of discrimination and also whether there is a likelihood that the respondent will be able to rebut any presumption of discrimination or provide a justification.

For many of the sub-steps in step 3, technical expertise may be useful. This should be an expert with a good understanding of statistics, data science and AI. Concepts that are core to the development of algorithmic systems such as training data, ground truth labels, outputs and inputs are not further explained in this methodology; these are assumed to be basic knowledge in the fields of statistics, data science and AI. When employing a technical expert, make sure the expert understands both data science and non-discrimination principles.

In some cases, MSAs or other agencies in the member state will have the technical expertise required that may be used by equality bodies (see Co-operation across sectors).

Additionally, sometimes sectoral expertise may be helpful to understand patterns of historical and existing inequalities in the sector where the system is applied. When employing sectoral expertise, it may be helpful to employ experts with a background in social sciences and empirical research as this background helps bridge the gap between the sectoral expertise and technical expertise. Where this is not possible it may be necessary for the EB to conduct further research on historical and other inequality to be able to assess the possibility as to whether this has affected the system. For example, known over-policing of certain communities or gender income disparities.

A recommendation to involve experts is mentioned where applicable at each sub-step.

Note: as identified under the methodology, the new Article 77(1)(b) on requirement of co-operation and mutual assistance may result in the MSA or another public authority or body under the act being able to provide the required expertise.

Note: where insufficient information is available you will need to consider either:

- the impact of lack of transparency on the burden of proof (see transparency under step 3.7); or
- requesting an evaluation of the system and testing by the MSA (see step 4.2.1).

A reasonable level of knowledge of discrimination law is expected for using this methodology, but the basic concepts are restated in the beginning of this step to better show how they connect to algorithmic systems.

Introduction to concepts

Types of discrimination

Direct discrimination

A person is treated less favourably in comparison to how others in a similar situation are or would be treated, and the reason for this is a particular characteristic they hold that falls under a protected ground (and, only in EU cases concerning age/disability and genuine occupational requirement cases, there is no justification).

Example of direct algorithmic discrimination

In Finland, a man was denied a loan by a financial institution, which used a scoring system based on data such as place of residence, gender, age and mother tongue to assess the risk of loan default. It was found that the man would have been approved for the loan had he been a woman or had Swedish as his mother tongue. Furthermore, no individualised risk assessment was made regarding his likelihood of defaulting; he was simply refused the loan based on statistical assumptions related to his gender and mother tongue. The Finnish National Non-Discrimination and Equality Tribunal concluded in 2018 after a request for an investigation by the Non-Discrimination Ombudsman that this was a case of direct discrimination.

Further reading

- Assessment of creditworthiness, authority, direct multiple discrimination, gender, language, age, place of residence, financial reasons, conditional fine, Tribunal of Finland (2018)

Indirect discrimination

An apparently neutral provision, criterion or practice (PCP) that puts members of a protected group at a particular disadvantage in comparison to others in a similar situation, unless:

- the PCP is objectively justified by a legitimate aim; and
- the means of achieving that aim are appropriate and necessary.

There is no authoritative decision as of yet in respect of whether or not some or all automated decision-making processes are a provision, criterion or practice but there is a strongly held view among some practitioners that they almost certainly are: "In our view, automated decision-making processes which utilise algorithms are almost certainly PCPs for the purpose of an indirect discrimination claim" (Allen and Masters 2019).

Example of indirect algorithmic discrimination (Deliveroo case)

Deliveroo's algorithmic "self-service booking" system for allocating work shifts was found to be indirectly discriminatory, particularly on the grounds of belief (participation in collective action such as strikes) and disability. By relying on participation and reliability statistics, apparently neutral criteria, the system in practice disadvantaged riders who abstained from work for legitimate reasons, such as strikes, illness or care responsibilities, by reducing their scores and consequently their access to future work opportunities.

The "blindness" of the statistics used, that is, the system's failure to take account of reasons for unavailability linked to protected grounds, resulted in different situations being treated similarly, leading to a disproportionate impact on protected groups.

Further reading

- *Filcams Cgil Bologna and Others v. Deliveroo Italia S.R.* (2020)
- Purificato (2021)

Multiple discrimination

Discrimination can occur based on more than one ground. For example, a person may suffer discrimination based on race and based on gender or disability. There are several different terms used to describe discrimination that occurs on more than one ground. Some examples of terms used are "multiple discrimination", "cumulative

discrimination", "compound discrimination", "combined discrimination" and "intersectional discrimination" (Fredman 2016). These all have subtly different meanings. For this methodology, it is important to recognise that the basis of discrimination may be multifaceted (Xenidis 2021).

Intersectional discrimination

"In essence … intersectionality is a way of thinking about identity and its relationship to power" (Crenshaw 2015).

Intersectional discrimination is different from other forms of multiple discrimination in that it is not simply an addition of discrimination based on single grounds, but different personal characteristics overlap and cannot be separated. Social, economic, cultural and institutional structures interlock and form a complex system that creates (and perpetuates) inequality (Crenshaw 1991). For example, social categories such as age and gender can overlap to create advantage or disadvantage depending on the circumstances. Inequality can change depending on circumstances and facts and is sometimes time and location dependent. For example, a non-migrant woman may be "less" equal than a man but more equal than a migrant woman. Social inequalities can also shape power relations. These interlocking structures of inequality are mirrored in the real-world data used to design, build and test algorithmic systems. In addition, machine learning approaches used to build AI systems are able find interacting patterns that are not known or not evident from basic data analyses. In that way algorithmic systems can lead to intersectional discrimination (Xenidis 2021). Although intersectional discrimination was rejected by the CJEU in the Parris case (C-443/17), some commentators suggest that this needs to be revisited particularly in light of the increasing recognition of the phenomenon in Union law such as the Pay Transparency Directive 2023/970/EC and Directive (EU) 2024/1385 on combating violence against women and domestic violence (Howard 2024).

Proxy discrimination

Discrimination based on the use of characteristics, known as proxies, that are not themselves assigned to any of the explicitly prohibited grounds of discrimination (see protected characteristics), but that correlate with a protected ground, is referred to as proxy discrimination. While EU legislation does not explicitly recognise or refer to proxy discrimination, it is a theoretical construct that helps to understand how algorithmic discrimination may arise.

- Proxy discrimination may be direct discrimination if there is an inseparable connection between the chosen – neutral – characteristics and the explicitly protected ones (pregnancy and gender, for example: *Dekker v. Stichting Vormingscentrum voor Jong Volwassenen (VJV-Centrum) Plus*, 1990; *Dita Danosa v. LKB Līzings SIA*, 2010; *Andersen v. Region Syddanmark*, 2010; *VL v. Szpital Kliniczny im. dra J. Babińskiego SPZOZ v. Krakowie*, 2021).
- Alternatively, proxy discrimination may be indirect discrimination if the provision, criterion or practice, including proxies, impact persons with protected characteristics in a disproportionate manner (for an explanation of this in practice, see *Jyske Finans v. Ligebehanlingsnævnet*, 2017(C-668/15)).

Key case: *Dekker v. Stichting Vormingscentrum* (1990)

An employer was in direct contravention of the principle of equal treatment (Council Directive 76/207/EC) on the implementation of equal treatment for men and women as regards access to employment, vocational training and promotion and working conditions when it refused to enter into a contract of employment with a female candidate suitable for the job where refusal was based on the possible adverse consequences of employing a pregnant woman because the national sickness scheme assimilated pregnancy to sickness. The court recognised that only women could be refused employment on the grounds of pregnancy and there is constituted direct discrimination on the grounds of sex.

Proxy variables

In the context of non-discrimination law, "proxies" or "proxy variables" refer to characteristics or combinations thereof that are not themselves listed among the explicitly prohibited grounds of discrimination under the relevant legal framework, but that correlate with those grounds in such a way that their use can lead to unlawful discrimination. One example of this is a postcode: a postcode is not discriminatory in itself; however, if many migrants or people of a particular ethnic origin live in a certain area, it can function as a proxy for a prohibited ground, namely ethnic origin.

Proxies can be recognised by over-representation: if people with a specific protected attribute are over-represented in a group, then identifiers of this group are likely to be proxies. Thus, in the above example, because people of different origins are over-represented in certain neighbourhoods, a postcode can be recognised as a proxy.

When a proxy is used as input to an algorithmic system, this could indicate potential discrimination. Note that depending on the type of proxy, the use of proxies can indicate both direct and indirect discrimination (Weerts et al. 2024). Certain characteristics are known, through research on the topic and relevant case law, to be proxies for protected characteristics. Proxies may also be identified by understanding and analysing the specific context in which an algorithmic system is applied, considering existing historical inequalities and demographics.

For details and examples of different types of proxies, see Appendix E.

In the Chez case (C-83/14), a collective measure (placing electricity meters in a "Roma" district at a height of between six and seven metres rather than less than two metres in other districts) was imposed on a district inhabited by mainly, but not exclusively, persons of Roma origin. If that measure proved to have been introduced and/or maintained for reasons relating to the ethnic origin common to most of the inhabitants of the district concerned, it would be considered direct or indirect discrimination, including against those inhabitants of that district of non-Roma origin. This was a matter for the national court to determine by taking account of all the relevant circumstances of the case and of the rules relating to the reversal of the burden of proof that are envisaged in Article 8(1) of Directive 2000/43.

Algorithm example: college grant check

This example should help to explain how proxies work. In this case "living close to parents" and "following vocational education" acted as proxies for "non-European migrant background".

The Education Executive Agency of the Netherlands (DUO) performs checks to ensure that disbursed college grants are properly granted. This process is known as the college grant check (in Dutch abbreviated to CUB). Suspicion emerged that the now ceased CUB process was discriminatory against students with a migration background. This suspicion was based on the appeal procedures initiated by students who were found to have wrongly received grants, in which lawyers realised that their clients overwhelmingly came from migration backgrounds. Investigation brought to light that a fraud risk scoring system was used in this process to prioritise investigations into (il)legitimate use of the grants.

Algorithm Audit performed an analysis of the algorithmic system, differences in treatment in the separate steps of the CUB process and investigated whether the inputs to the system could be considered proxies.[45] The system was found to use three inputs: the age of student, the level of education and the distance between their address and their parents. Nationality, migration background or any other information about race or ethnicity were not used in the fraud scoring system.

The key findings of Algorithm Audit were that:

- the CUB process overall led to unequal treatment of students with a non-European migration background;
- the risk profile assigned higher risk scores to students with a migration background; students with a non-European migration background were twice as likely to be assigned to a high-risk category than students of Dutch origin;
- the further manual selection of students for control reinforced the over-representation rather than reduce it. Students with a non-European migration background were 6.2 times more likely to be selected for a check, which involved an invasive home visit, than students of Dutch origin.

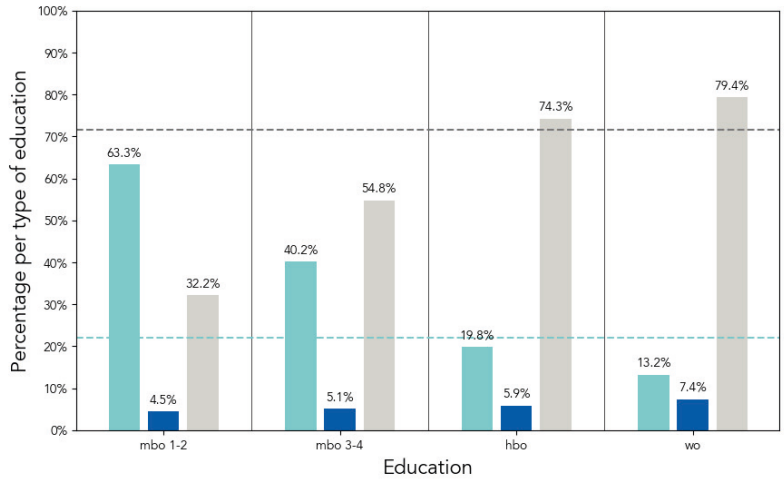
A Dutch court concluded that this practice was not objectively justified and constituted indirect discrimination (Rechtbank Overijssel 2024).

Detailed analyses showed that the risk scoring system assigned higher risk scores to students in the lower educational levels (vocational education) and students living closer to their parents. Both variables were shown to correlate (strongly) with migration background and are thus proxies for migration background (see the graphs below).

45. Algorithm Audit was granted full access to both the algorithm and DUO's internal data. Because of the General Data Protection Regulation (GDPR), DUO does not collect or process information on the origin of students for the purpose of the CUB process. To perform these analyses, DUO and Algorithm Audit collaborated with the Dutch national office of statistics (Netherlands Statistics or CBS). CBS provided aggregated statistics on the country of birth and country of origin based on populations defined by Algorithm Audit for each of the process steps (risk category, selected for control, outcome control, appeal procedure, outcome appeal) and input variables (education, age, distance to parent(s)).

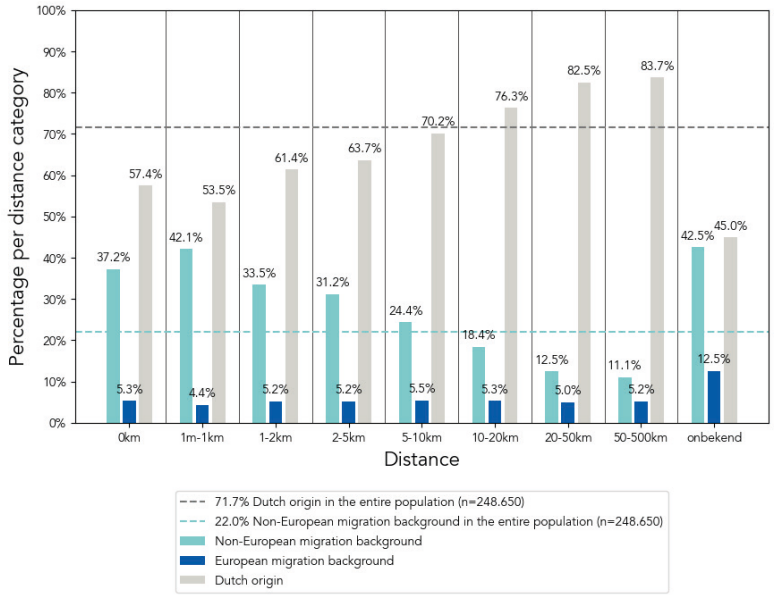
Graph 1

Distribution of students with a (non-)European migration background and students with Dutch origin per type of education in the college grant population-2014 (n=248.650)



Graph 2

Distribution of students with a (non-)European migration background and students with Dutch origin per distance category in the college grant population-2014 (n=248.650)



Source: Algorithm Audit

For a full explanation, see Algorithm Audit 2024a and 2024b.

Comparators

A comparator is a person in a similar situation to the complainant but who does not share the protected characteristic assumed to be the reason for the discrimination.

Note: it is possible for two groups of people to be considered in an analogous situation for the purpose of one complaint but not another. It is therefore always important to assess the comparator in light of the aim of the contested measure (Council of Europe and European Union Agency for Fundamental Rights 2018: 44-49).

Choosing the right comparator will be important when assessing evidence in algorithmic systems in particular when assessing the aim of the system and the training, testing and validation measures and the actual testing and evaluation. In particular, it may be necessary to assess whether protected characteristics data were used to train the algorithmic system and what choices have been made when testing the system. This is discussed in more detail in sections 3.3, 3.5 and 3.6.

Establishing a presumption of discrimination

According to the non-discrimination directives, when persons who consider themselves wronged because the principle of equal treatment has not been applied to them establish before a court or other competent authority facts from which it may be presumed that there has been direct or indirect discrimination, it shall be for the respondent to prove that there has been no breach of the principle of equal treatment.[46] See also step 3.8.

This means that the complainant must come forward with enough evidence to give rise to a presumption of discrimination.

After this the burden of proof shifts to the respondent. In practice, domestic courts have a margin of appreciation in determining when the evidence presented by the complainant is sufficient to shift the burden of proof to the respondent.[47]

Evidence may include statistical data,[48] written documents – if they have content related to the discrimination or relate to the specific case of the applicant – and reports and analyses from relevant sources (see data collected in step 2), situation testing (see under step 3.6), common-sense assessments, witness testimonies and inferences drawn from circumstantial evidence. The CJEU emphasises the importance of considering "all the circumstances surrounding the practice at issue" (C-83/14 CHEZ, paragraphs 80-84). Accordingly, both statistical and qualitative data can be used to establish a presumption of discrimination and there is an argument that both should in fact be used.

What is "equality data"?

In the context of the methodology, we refer to both quantitative (including statistical) and qualitative data as "equality data", drawing on the following definition given

46. Directive 2000/78/EC, Article 10, Directive 2006/54/EC, Article 19, Directive 2000/43/EC, Article 8.
47. In practice this will often be different for direct and indirect discrimination. For further reading see Farkas and O'Farrell (2015).
48. For more on statistics as evidential elements, see below, "Approach to Statistical data".

in the "Guidelines on improving the collection and use of equality data" (European Commission 2021) as:

> any piece of information that is useful for the purposes of describing and analysing the state of equality. The information may be quantitative or qualitative in nature. It could include aggregate data that reflect inequalities or their causes or effects in societies. Sometimes data that are collected primarily for reasons other than equality-related purposes can be used for producing equality data. (European Commission 2021: 8)

Equality data are used for, among other things, "providing reliable evidence in administrative or judicial cases regarding discrimination through data that point to direct or indirect discrimination; and supporting advocacy and awareness raising in the field of equality and non-discrimination" (European Commission 2021: 9).

Further reading

- "Handbook on identifying and using equality data in legal casework" (Ilieva 2024)
- "Strategic litigation handbook" (Equinet 2017)
- "Handbook: artificial intelligence, judicial decision-making and fundamental rights" (JuLIA Project 2024)

How to use step 3

The sections below outline the guiding questions that can assist equality bodies in determining whether there is a prima facie case of discrimination. The aim is to show where in the information collected in step 2 the relevant evidence may be found, what to look for in the evidence and how to use the evidence to prove discrimination.

Each section in this part follows the following basic structure.

- An explanation of what should be assessed by the EB.
- Questions to consider when assessing the information.
- Potential sources of information.
- Indicators of discrimination.

Sections 3.7 and 3.8 then provide a framework to assess whether the evidence collected is sufficient to support a prima facie case of discrimination involving an AI or algorithmic system (3.7 Assessing whether the evidence is sufficient) and to evaluate the likelihood that the respondent may be able to rebut it or provide a justification for any discrimination (3.8 Can the respondent show the difference in treatment is not discriminatory?). This will help determine whether any action should be taken against the respondent. There will necessarily be some cross-over in the process and examination of evidence between these tasks.

It is extremely unlikely an EB will be able to access all of the information or answer all of the questions in this step. Instead, they are meant as a guide to the types of information that might be available and how they could be assessed on both an individual basis and then collectively.

A suggested record sheet has been provided in Appendix K, which is meant as an aid and can be adapted to the individual EB needs.

Further reading

Some of the concepts in step 3 will be new or unfamiliar. The resources below explain these in more depth.

- Wachter, Mittelstadt and Russell, 2020, Why fairness cannot be automated: bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, Volume 41, July 2021.
- Mittelstadt, 2024, How to use the Artificial Intelligence Act to investigate bias and discrimination: A guide for equality bodies, *Equinet*.

3.1. What are the known or suspected risks of discrimination?

The use of algorithmic systems in certain contexts can come with an inherent risk of discriminatory practices. When algorithmic discrimination has previously been shown in a similar use case in a similar sector, this could indicate a broader risk of discrimination that also applies to the case under assessment. For example, where it is shown that facial recognition used in policing is discriminatory, it is likely that facial recognition used for other purposes will also be discriminatory.

3.1.1. Is the type of algorithmic system or the domain in which it is applied explicitly referenced in the AI Act for its risks of discrimination?

The AI Act refers to both "sectors" and "use cases" within sectors.

When algorithmic systems are used in sectors where historical inequalities exist and/or where discrimination has been shown to frequently occur, this should raise increased suspicion of discrimination. Algorithmic systems are based on real-world data. Existing inequalities and human biases are reflected in the data and therefore often appear and may be exacerbated in the algorithmic system.

Historical data bias: algorithm example, Amazon recruiting tool

Amazon developed an AI recruiting tool trained on historical resumes that reflected a predominantly male applicant pool. As a result, the system "taught itself that male candidates were preferable". Although the system did not explicitly use gender as an input, it relied on proxy data correlated with being female – such

as the word "women's" ("women's chess club captain", for example) or degrees from women's colleges – and systematically downgraded applications from women candidates (Dastin 2018).

Many of the high-risk use cases in the AI Act were determined to fall in the high-risk category by the EU precisely because of a risk of discrimination. Recitals 54 and 56 to 60 of the AI Act explicitly mention the risk of discrimination, the perpetuation of historical inequalities and specific vulnerabilities. Even if a system is not technologically complex and/or is not AI, the use of (rule-based) algorithmic systems for these use cases comes with a similar risk of discrimination. Appendix I describes high-risk AI areas and use cases.

A use case that is explicitly referenced in the AI Act warrants an additional level of scrutiny. Additionally, supporting equality data, both qualitative and quantitative, may be available for these cases and can often be found in case law, academic, CSO or government reports. See also section 2.1.2, Existing case law, and Other sources.

Note: if the system is a high-risk AI system and recorded in the EU database, including in section B,[49] then by definition it is explicitly referenced in the AI Act and therefore potentially poses a high risk of discrimination.

Questions to consider

- Is the algorithmic system a "type" of technology known to create a risk of discrimination, such as profiling (Article 6(3) and Recital 53), predictive risk analytics (Recital 42) or biometrics and emotion recognition (Annex III (1), Recitals 44 and 54)?
- Was the decision or treatment experienced related to one of the following sectors?
  - Education and vocational training (Annex III (3), Recital 56).
  - Employment, worker management and access to self-employment (Annex III (4), Recital 57).
  - Access to and enjoyment of public services and benefits (welfare) (Annex III, (5)(a)).
  - Credit scoring (Annex III (5)(b), Recital 58).
  - Life and health insurance, (Annex III (5)(c), Recital 58).
  - Access to and eligibility for healthcare services (Annex III (5)(a), Recital 58).
  - Law enforcement (Annex III (6), Recital 59).

49. Where a system is in section B of the EU database it has been self-assessed by a provider as being used in a high-risk sector but not posing a risk on the basis of a narrow set of exceptions (see the AI Act, Article 6(3)). While documentation required under the AI Act will most likely not be available, this system is applied in a domain explicitly referenced in the AI Act for its risks of discrimination.

- Migration, asylum and border control (Annex III (7), Recital 60).
- Administration of justice (Annex III (8)(a), Recital 61).
- Administration of democratic processes (Annex III (8)(b), Recital 61).

- If the case was related to one of the sectors above, does the case cover a use case, listed in the relevant section of Annex III (including the relevant recital)?

Potential sources of information to assess a generally established risk of discrimination

EU AI Act

- Article 6, Annex III and recitals – these describe high-risk types of AI.
- Article 5 – this describes prohibited AI practices and Recitals 28 to 45.

Other

- Commission's guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act.
- Forthcoming: Commission guidelines on classification of high-risk AI systems and related requirements.[50]

Indicators of a risk of discrimination

If any of these indicators hold, this in itself is not evidence for discrimination. However, these indicators could indicate a system with a risk of discrimination:

- if the system is a high-risk AI system in sections A or C;
- for non-high-risk:
  - if the system is intended for use in either a sector in which there is an identified risk of discrimination (Annex III or recitals); and/or
  - if it is a type of technology in which there is a known risk of discrimination.

Record whether the system is a high-risk system or not or whether it is intended for use in any of the sectors or areas identified as posing a risk of discrimination in the AI Act.

50. At the time of editing this methodology, the Commission has published draft guidelines for consultation: Commission seeks feedback on the draft guidelines for the classification of high-risk artificial intelligence systems.

Suspected incorrect classification under the AI Act

If an equality body suspects a system to be wrongfully self-assessed as not a high-risk AI system or not recognised as a prohibited AI practice (see suspected prohibited AI systems under step 1.4), they should inform the relevant MSA, regardless of whether a case of discrimination can be established (see also step 4).

3.1.2. Has a known risk of discrimination in this sector or technology been identified by national or regional authorities, national or international CSOs or human rights organisations?

Reporting by ombudsman institutions, civil society and academia and existing jurisprudence can show a pattern of unequal outcomes for a specific protected ground.

Use the information gathered in step 2 to assess whether this system or type of system is already known or suspected of producing a discriminatory outcome. Any relevant information may also help you to perform the next steps.

In this step, sectoral expertise would be beneficial.

Potential sources of information to assess a generally established risk of discrimination

- EB monitoring, research or investigations
- Reports from CSOs national and international bodies
- Existing case law
- Internet searches
- Experts

Indicators of discrimination

- Discrimination has been identified or is suspected by others in the specific use of algorithmic systems by the respondent that the current case covers.
- Discrimination has been identified or is suspected by others in highly similar uses of algorithmic systems as the case covers, indicating a potential pattern of discrimination.

Record the area in which there is a known risk, the technology and any other relevant information and evidence. For example:

Sector: law enforcement

Technology: facial recognition, biometrics

Sources of information: Research by an NGO/academia, AI Act Article 5 (prohibited systems), Article 6 (high risk) and Annex III.

Use cases that should be considered high risk or prohibited under the AI Act

If the identified pattern of discriminatory outcomes for a specific algorithmic use case is strong and consistent but it is not in the lists in Annex III, EBs should consider reporting the use case to the Commission for it to be added to the list under Article 7 (see step 4.3.2).

If the EB finds an AI practice to fundamentally contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights enshrined in the Charter, but it is neither prohibited nor considered high risk under the AI Act (see step 4.3.2).

3.2. Are there any known protected characteristics or proxies in the inputs or data sets?

The input data for an algorithmic system defines the output and thus the result. Therefore, if a protected characteristic (see protected characteristics) or a proxy (see proxy discrimination) is used as input to the algorithmic system, there should be a suspicion of discrimination.

In this step sectoral expertise is useful.

Questions to consider

- Are any personal data processed revealing protected characteristics or proxies for protected characteristics?
- Are protected characteristics or known proxies (see Appendix E) referred to in any of the relevant documents?
- Are protected characteristics or known proxies mentioned directly as inputs to the system (either in training, testing or in use)? This could be phrased as "X, Y and Z are used to predict/calculate".
- Is one of or a combination of the inputs to the system a likely proxy to a protected attribute, based on sectoral knowledge? Answering this question may require consulting national statistics or sectoral experts with knowledge on how inequalities exist and relate in a specific sector. For example:
  - in countries where a tax deduction exists for healthcare-related costs, people with a disability are likely to be over-represented in those who utilise this deduction. Thus, the use of this deduction is a likely proxy for disability;
  - in many countries people with a migration background are under-represented among those with university degrees, therefore the level of education is a likely proxy for race/ethnic background.
- Are any of the proxies mentioned inextricably linked to a protected characteristic? See Appendix E.
- Can the suspicion of a (selection of) input(s) being a proxy be supported by evidence? For example, are statistics available from a national bureau of statistics

or academic research that show over- or under-representation of a group with a protected characteristic in a specific sub-group of the inputs? For example:
  - if educational degree is one of the inputs that is suspected to be a proxy for ethnic background, are statistics available that show that people with a migration background are over-represented in the group with vocational degrees?

Note: gathering this evidence may require expert contribution by collaborators with experience in data analytics.

- Is the system trained, tested or validated on information containing protected characteristics? (See step 3.5)

Potential sources of information to understand the inputs to the system

Complainant

- List of information provided by the complainant to the respondent.
- Explanations, motivations and substantiation provided to the complainant about the treatment.

GDPR, Articles 13 and 14: information provided to the data subject

- Information provided to the data subject (complainant) at the time they provided the data (Article 13 of the GDPR).
- Information provided by a controller where the personal data were not obtained directly from the data subject (Article 14 of the GDPR).
- The logic involved in cases of automated decision making (Articles 13(2)(f) and 14(2)(g)).

GDPR, DSAR response

- The categories of personal data concerned (Article 15(1)(b)): the data controller must provide a copy of the personal data undergoing processing. This may include data provided by third parties (Article 14 of the GDPR).
- Potentially: input variables or parameters used for decision making and how they came about (for example, using statistical information) and their respective weight at aggregated level (opinion of AG Pikamäe in SCHUFA Holding, 2023, paragraph 58).

EU AI Act, Article 86: explanation request

- Input data and main elements of the decision.

Publicly available

- EU database for high-risk AI systems: section A high-risk AI systems – a description of the information used by the system (data, inputs) and its operating logic.
- FAQs on the platform.
- Public company communications.

Respondent

From the provider:

EU AI Act, Article 11 and Annex IV: technical documentation

- Annex IV (2)(b), the general logic of the AI system and of the algorithms, the rationale and assumptions made, including with regard to persons or groups of persons in respect of whom the system is intended to be used; the main classification choices; what the system is designed to optimise for, and the relevance of the different parameters; the description of the expected output and output quality of the system.
- Annex IV (2)(d), a general description of the data sets, information about their provenance, scope and main characteristics.

From the deployer:

EU AI Act, Article 27: fundamental rights impact assessment

- The categories of natural persons and groups likely to be affected by the algorithmic system (Article 27(1)(c) of the EU AI Act).

Other

- Contractual clauses.
- Desk research, existing case law and statistics on over- and under-representation in the relevant domain.

Indicators of discrimination

- Direct use of protected characteristics in the system
- Use of proxies that are inextricably linked to a protected attribute in the system
- Use of known proxies in the system
- Use of protected characteristics or proxies to train, test or validate the system

All the above require evidence that these inputs lead to unequal treatment. Indicators *a* and *b* are indicative of direct discrimination. Indicators *c* and *d* are indicative of indirect discrimination.

- Record direct use of protected characteristics. Where are they used and how?
- Record any use of protected characteristics or proxies that have or are believed to have an impact on the outcome of the system. Investigate the technical design of the system and influence of the (suspected) proxies on the outcomes of the system. The fact that a proxy is used as an input is by itself not enough

as evidence for discrimination. The next step is to evaluate the evidence to understand if the use of these inputs leads to unequal treatment.[51]

- For any proxy, include evidence or arguments for why the EB considers them to be proxies.

3.3. Assessment of risks to fundamental rights (risk assessments, HRIA, FRIA and DPIA)

Providers and deployers of high-risk AI systems have various and different obligations to identify and document risks of discrimination. For algorithmic systems that are not high risk, AI providers and/or deployers may well have identified and documented discrimination risks as part of their GDPR compliance (particularly in a DPIA) or own business and human rights due diligence (United Nations 2011). New obligations may also be introduced because of the Council of Europe Framework Convention on AI.

Risks of discrimination are usually identified in a fundamental rights impact assessment (FRIA), data-protection impact assessment (DPIA) and/or other risk-management procedures. If done properly, these processes should identify and record any risks of discrimination presented by an AI system or processing data using an AI system and any mitigating measures taken and their impact.

In technical document and risk assessments, bias or fairness may be mentioned instead of inequality or discrimination.

In this step both technical and sectoral expertise would be beneficial.

Fundamental rights impact assessment: AI Act

The requirement to conduct a FRIA only applies to certain deployers of high-risk AI systems (see step 2.2 for more detail).

The FRIA (and other assessments) should include a range of information that should highlight potential gaps and harm to rights, including non-discrimination. This includes:

- information on how the deployer will use the high-risk AI system as intended by the provider;
- how long and how often the system will be used;
- how the human oversight measures have been implemented;
- the categories of natural persons and groups likely to be affected;
- the specific risks of harm to fundamental rights, including non-discrimination considering information provided by the provider;

51. An input into the system that indicates a protected ground, or a known proxy, and that does not overlap with a protected ground may not in itself be enough to support a discrimination claim. See for example the STAR case in Denmark. In that case, the prediction tool used "ancestry" or "origin" as a predictive character. The board determined that "ancestry" when used in the profile tool "does not indicate anything about ethnic origin". www.retsinformation.dk/eli/accn/W20220951825. For further details, see Equinet 2022: 23-24.

- the arrangements for internal governance and complaint mechanisms that the deployer will use if the risk materialises.

If the deployer should have performed a FRIA but has not or has not included relevant information, see step 4.

DPIA

A DPIA[52] should consider all risks to the rights and freedoms of natural persons resulting from the processing of personal data, not just privacy risks. This also includes discrimination risks (Article 29 of the Data Protection Working Party, 2017a). The EB may need to co-operate with the data-protection authorities.

Questions to consider

Information on the various risk assessments performed by the provider and deployer should be cross-referenced with each other and any discrepancies noted.

- Has the provider or deployer identified relevant fundamental rights risks the other did not?
- Where one party has conducted more than one risk assessment or more than one type of risk assessment is there consistency in respect of identified risks? Are any risks identified in one assessment missing in another (unless there is a good explanation; for example, the risk only arises in respect of a child and is specifically considered in the child risk assessment)?

For all algorithmic systems, including high-risk AI:

- Has discrimination (or other risk to fundamental rights) been identified by the provider or deployer?
- Has the provider put a risk-management process in place?
- How were risk-management procedures and impact assessments used to determine biases or inequality in the data or the system? How is bias defined or scoped?
- Are there any unmitigated risks? Where possible, check risks referred to in the technical documentation against the risk-management system.

Note: where discrimination has been identified and claimed management measures put in place this will require further investigation (see step 3.6, testing and evaluation). If the system is high risk and the EB is an Article 77 authority they can request access to the Article 9 risk-assessment documentation.

In cases involving a high-risk AI system:

- is any risk-management process compliant with the requirements of Article 9?

In cases involving a high-risk AI system, where a FRIA is required from the deployer:

- has the FRIA has been correctly performed? It should not be a tick-box exercise;

52. The European Data Protection Board was consulting in May 2026 on a DPIA template, available here: https://www.edpb.europa.eu/public-consultations/template-for-data-protection-impact-assessment_en.

- has the deployer involved any relevant stakeholders when conducting the risk assessment? (Recital 96 provides for this possibility);
- should stakeholders have been consulted, for example people likely to be affected by the system? (see the Bridges case below);
- if a consultation process did take place, consider contacting those people consulted but be aware they may be under a duty of confidentiality or non-disclosure agreement;
- check that any risks of discrimination identified in the technical documentation (Article 11) are all referred to in the risk-management system documentation (Article 9). If they are not, a presumption of discrimination may arise.

Potential sources of information on risks and risk assessments

Complainant

GDPR, Articles 13-15, Information provided to the data subject

- The existence of automated decision making and/or profiling (Articles 13-15, 21 and 22 of the GDPR).
- The logic involved in the ADM used (Articles 13(2)(f), 14(2)(g) and 15(1)(h) of the GDPR).

Publicly available

- EU database for high-risk AI systems: section C deployer: summary of the DPIA and FRIA (unless law enforcement or migration control).

Respondent

From the provider:

EU AI Act, Article 9, risk-management system

- Providers are required to establish a risk-management system in respect of high-risk AI systems. It shall be a continuous iterative process and requires:
  - risk identification: the identification and analysis of the known and the reasonably foreseeable risks to fundamental rights (Article 9(2)(a));
  - risk management: the adoption of appropriate and targeted risk-management measures (Article 9(2)(d)), including the provision of information and training to deployers to eliminate or reduce risk (Article 9(5)(c) and Article 13);
  - testing: ensure the system has been tested for the purpose of identifying the most appropriate and targeted risk-management measures (Article 9(6));
  - particular groups: when implementing the system consideration must be given to whether the system is likely to have an adverse impact on persons under the age of 18 and, as appropriate, other vulnerable groups (Article 9(9)).

However, risk management is only required in respect of those 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".

EU AI Act, Article 10, data and data management (see step 3.6 training, testing and validation data)

EU AI Act, Article 11 and Annex IV, technical documentation

- Annex IV (2)(g) requires the technical documentation to include information about any potentially discriminatory impacts.
- Annex IV (3): detailed information about the monitoring, functioning and control of the AI system, in particular with regard to its capabilities and limitations in performance, including the degrees of accuracy for specific persons or groups of persons on which the system is intended to be used and the overall expected level of accuracy in relation to its intended purpose; the foreseeable unintended outcomes and sources of risks to health and safety, fundamental rights and discrimination in view of the intended purpose of the AI system; the human oversight measures needed in accordance with Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the deployers; specifications on input data, as appropriate.

From the deployer:

EU AI Act, Article 13, transparency and provision of information to deployers

- Instructions for use provided to the deployer by the provider Article 13(3):
  - known or foreseeable circumstances of intended use or misuse that may risk fundamental rights;
  - (when appropriate, its performance regarding specific persons or groups of persons on which the system is intended to be used;
  - when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the high-risk AI system.

EU AI Act, Article 26(9), data-protection impact assessment: performed using the information provided by the provider/GDPR, Article 35, data-protection impact assessment (DPIA)

EU AI Act, Article 27(1)(d), fundamental rights impact assessment

- The specific risks of harm to fundamental rights, including non-discrimination considering information provided by the provider.

Other

- Assessment conducted by using the Council of Europe's risk and impact assessment of AI systems from the point of view of human rights, democracy and the rule of law (HUDERIA methodology).
- Some organisations will conduct and publish an HRIA or FRIA, DPIA or child rights impact assessment voluntarily. There may be an "ethics" assessment.
- Any other (risk) assessments shared by the respondent.
- Freedom of information requests, where available.

Key case: *R (Bridges) v. Chief Constable of South Wales Police*, 2020

(Numbers within square brackets denotate paragraph numbers in the judgment.)

Bridges was a case decided by the Court of Appeal in the United Kingdom that considered whether a public authority had breached human rights or failed to comply with duties to assess equality impacts under the domestic Equality Act 2010 before implementing live facial recognition. The public sector equality duty requires a public authority to pay "due regard" to the need to eliminate discrimination, harassment, victimisation and other relevant conduct, advance equality of opportunity and foster good relations between persons who share a relevant characteristic and persons who do not. The court held that the duty:

- must be fulfilled before and at the time a policy (to use facial recognition) is being considered;
- must be exercised in substance, with rigour and an open mind – it is not a tick-box exercise;
- is non-delegable, which can create very real difficulties for public authority deployers relying on third-party providers, particularly if insufficient information about a systems performance was provided or the authority did not have sufficient expertise or experience to understand the information or system [199].

In addition, if material relevant to the assessment is not available there is a duty to acquire it – this may require additional consultation with relevant groups. Finally, provided there is rigorous consideration of the duty so that there is a proper appreciation of the potential impact of the decision on equality objectives and the desirability of promoting them it is for the decision maker to decide how much weight should be given to factors informing the decision.

Overall, the court held that compliance with the duty "requires the taking of reasonable steps to make enquiries about what may not yet be known to a public authority about the potential impact of a proposed decision or policy on people with the relevant characteristics, in particular for present purposes race and sex" [181].

Having a human in the loop, on its own, was held to be unlikely to discharge the statutory duty because the duty regulates the process not the substance of a decision.

And the court recognised that humans make mistakes [185].

Similar observations are likely to apply to risk assessments under the AI Act.

Indicators of discrimination

A risk of discrimination that has been identified but not mitigated, monitored or justified should be considered a strong indicator.

- Direct reference to discrimination, bias or unfairness in the FRIA.
- Direct reference to discrimination, bias or unfairness in the DPIA.
- In case bias is mentioned as a risk, the meaning and types of bias are not defined or inappropriately defined in the documentation.

- No or inadequate risk-management procedures in place, for identified risks of discrimination, bias or unfairness.
- Unmitigated risk of discrimination is clear on the documentation.
- Insufficient testing.
- Direct reference to a risk of a breach of fundamental rights in either the FRIA or DPIA:
  - where there is a risk of a breach of fundamental rights at all this should flag a requirement for further investigation to ensure the system is non-discriminatory.
- An incomplete, cursory or inaccurate FRIA or DPIA would warrant further investigation.
- Failure to consult relevant stakeholders to identify risks where they clearly should have been included (for example, a system designed to make decisions about people with disabilities that did not consult any persons with disabilities or representative organisations before deployment may have failed to conduct the FRIA with the care required).

- Record any risks to discrimination identified by the provider or deployer and any measures identified to mitigate that risk.
- Consider and record whether there are any clear and obvious failures in the risk assessment, DPIA or FRIA.

3.4. What is the algorithmic system intended to do and how does it do it?

To understand whether algorithmic discrimination has occurred, EBs should understand the system itself, at least in general terms. Understanding the system's purpose and design and how it works helps to evaluate the following.

- What is the purpose of the system?
  - Is the purpose related to an area where there has been historical discrimination in respect of the protected characteristic(s)?
  - Is the data used appropriate for the purpose (see step 3.5)?
- How do inputs contribute to the outputs?
  - Does an input identified in step 3.2 influence the output and lead to a potential difference in treatment?
- Whether the algorithmic system impacts either the decision-making process as a whole or the final impact for the affected group.
  - What size role does the system have? For example, is it the sole decision maker or does it assist decision makers?
  - Is the algorithmic system the whole system or just one part of a much bigger system that may involve other algorithmic systems?

Within information about intended use and design you should be looking generally to see whether the design choices appear appropriate for the intended purpose and the actual use. In this step both technical expertise and sectoral expertise are useful.

The information available to the EBs should ultimately enable the EB to understand what the AI system does, how it does it through meaningful information about the logic involved, the significance of the processing and the envisaged consequences for the individual and why various choices in relation to design and data were made. When the algorithmic system is understood to be qualifying ADM or a high-risk AI system used for impactful decision making, the availability of this information is required. However, if the documentation does not enable this understanding there may be issues relating to lack of transparency (see below, Transparency, under step 3.7).

The design of the system may also be particularly important later on when you look at ways in which the respondent may seek to rebut any presumption of discrimination or justify decisions taken.

Questions to consider

Purpose and use

- How is the algorithmic system supposed to be used?
  - What is the intended purpose?
  - How is it used in practice?
  - In cases where the system is provided by a supplier: is it used by the deployer as intended by the provider?
- Who is the system designed for?
  - What were the design choices (see the box below) made in respect of the persons or groups of persons for whom the system is intended to be used?
- Are there any assumptions made about persons or groups of persons for whom the system is intended to be used? For example, this system is expected to be used by adults only, or this system is assumed to be used in a specific sector, or for a specific population. Are these assumptions rational and justified?
- How does the system influence the treatment of people?
- In cases where there is a human decision maker responsible for making choices that influence the treatment of people (human-in-the-loop):
  - are there any guidelines or protocols issued to decision makers to help them understand how to use the AI system or interpret the output?
  - does the relevant person have the necessary competence, training and authority to override a decision made by an AI system?
  - has the relevant person been trained to understand and interpret the outputs of the system and recognise where bias may arise and intervention be required?

Note: merely the existence of a human-in-the-loop does not mean that the system does not influence the treatment of people, since the human-in-the-loop is influenced by the outputs of the system to a greater or lesser extent.

How the system works

- What is the system designed to optimise for?
  - Was it designed to optimise for something (slightly) different than its intended use case? For example, was it optimised to predict errors, but is now used to predict fraud?
- Does the system use group characteristics to produce outputs on an individual (profiling)?
- How does the system handle deviations?
  - How does the system handle deviations from expected behaviour (error or unusual activity, for instance)?
  - Are all deviations treated in the same way, regardless of the underlying reason?
- Was the system designed for fairness and equality?
  - Was fairness or non-discrimination part of the design?
    - Is the context-specific notion of fairness explicitly defined?
    - What steps were taken to design for fairness and equality?

Influence of inputs

- How was the choice of any (pre-trained) model or algorithm made?
  - Is this procedure documented and available to deployers of the system?
- Which criteria influence the system's output?
  - Are relevant protected attributes and/or proxy variables in the data processed or relied on as the basis for an ADM or profiling (such as input to create a profile, information on the profile)?
  - Are metrics available on the weight/influence of specific input on the output?
- Which criteria are given the most weight in the system or decision?
  - Could the respondent argue that protected attributes and/or proxies have a negligible impact on the output?
- What is the cumulative impact of several proxy variables together, such as factors like postcode + education?
- Are the data used or given most weight arbitrary or irrelevant for the purpose they are used?

Potential sources of information to understand the system's purpose, design and how it works

Complainant

GDPR, Articles 13-15, information provided to the data subject

- The existence of automated decision making and/or profiling (Articles 13-15, 21 and 22 of the GDPR).
- The logic involved in the ADM used (Articles 13(2)(f), 14(2)(g) and 15(1)(h) of the GDPR).

GDPR, Article 15(3): DSAR

- The scope, nature and the level of detail of the information that will be provided in response to a DSAR request may vary. In the case of qualifying ADM, it is required to include the following, but for other algorithmic systems (parts of) this information may also be included:
  - input variables or parameters used for decision making and how they came about (such as using statistical information) and their respective weight (opinion of AG Pikamäe SCHUFA Holding, 2023, paragraph 58);
  - the effect of an input variable on the score; explanation of why the data subject was assigned a particular score; list of possible profile categories and counterfactuals;
  - the underlying calculation principle: detailed explanations of the method of calculating the score value; assignment of the data subject to an evaluation result, list of profile categories (Barros Vale and Zanfir-Fortuna 2022);
  - the existence of automated decision making and/or profiling and meaningful information about the logic involved as well as the significance and the envisaged consequences of such processing for the data subject (Article 15(1)(h)).

EU AI Act, Article 86, AI Act: right to an explanation

- The role of the AI system in the decision-making process. For example: "The AI system [name/designation of the AI system] was used for [description of the specific function of the AI system, like analysing data, evaluating criteria, performing voice analysis for emotion recognition, etc.]. The AI system contributed to the decision-making procedure by [analysing the data and providing an assessment of the relevant parameters, for example]".
- The processing logic: "The system analysed the input data using [description of algorithms or models, like decision trees] to perform [description of the objective, such as risk assessment]".
- Output: "Based on this analysis, the AI system generated the following output, which was incorporated into the final decision: [Description of the output, a score, a classification, for instance]".
- Impact of the decision taken on the affected person: "The decision has the following potential impact on you: [impact on creditworthiness, access to certain services, financial impact, etc.]. These impacts are relevant as they could significantly affect your ability to [explain the consequences, such as participation in programmes or receipt of offers for financing]".
- Weighting of criteria: "The key influencing criteria were weighted as follows: [brief explanation of the importance of each criterion]".

Respondent

From the provider

EU AI Act, Section A (5) and (6) of Annex VIII on high-risk AI systems

- Description of the intended purpose of the AI system, basic and concise description of the information used by the system (data, inputs) and its operating logic.

- For law enforcement/migration control there may be additional information in the database available to the relevant MSA.

EU AI Act, Article 11 and Annex IV, technical documentation

- (1)(a) The intended purpose.
- (1)(d) The description of all the forms in which the AI system is placed on the market or put into service (such as software packages embedded into hardware, downloads or APIs).
- (1)(h) A basic description of the user-interface provided to the deployer.
- (2)(b) Design specifications and general logic. See above, 3.2: Are there any known protected characteristics or proxies in the inputs or data sets?

From the deployer

Article 13, Transparency and provision of information to deployers

- The provider must provide (Article 13(2)), instructions for use for the deployer.
- Article 13(3)(b)(iv), where applicable, the technical capabilities and characteristics of the high-risk AI system to provide information that is relevant to explain its output, and (3)(b)(v), its performance regarding specific persons or groups of persons on which the system is intended to be used.
- Article 13(3)(c), the changes to the high-risk AI system and its performance that have been predetermined by the provider at the moment of the initial conformity assessment, if any.

Other

- Desk research
- Contractual clauses
- FAQs on the platform
- Public company communications

Indicators of discrimination

Strong indicators

These indicators together could support a prima facie case

- Suspected criteria (as identified in step 3.2) have a not insignificant influence on the system output.
  - When a protected characteristic or proxy that is inextricably linked to a protected characteristic has a not insignificant influence on the system output, this is a clear indication of direct discrimination.
  - When a (suspected) proxy has a not insignificant influence on the system output this is an indication of indirect discrimination.
- The output of the system (a least in part) determines the treatment of individuals.

Other indicators

- Intended use, assumptions and/or design choices are suspected to reflect or amplify historical inequalities, leading to unequal treatment.
- Design choices favour one group of people over another.
- System optimises for historically advantaged groups.
- System is not used for the intended purpose it was developed/provided.

- Record the purpose of the system and what it optimises for.
- Record proxies and protected characteristics that influence the system outputs and, when available, metrics on their weight/influence on the output.

3.5. Training, testing and validation data

Data are used to develop and test algorithmic systems. Even rule-based algorithmic systems that are designed manually are validated relying on data. Data are always an imperfect representation of reality. Biases and existing inequalities are reflected in the data. Assessment of biases and inequalities in the data can be used to argue that the resulting system leads to discriminatory outcomes. Note that understanding biases in the data will not by itself show unequal treatment. However, together with other complementary sources of analyses, it contributes to a prima facie case and can be used to motivate requests for additional testing.

When statistical equality data are available, this section is additionally relevant for considering the validity and reliability of the data used to calculate these statistics. In that case this section should be read in conjunction with section 3.6.

Within the data, you should be looking generally to see what information the respondent has given on how they have trained and tested their system. You may be able to identify from this any key discrimination issues; for example, no women were included in the dataset, the training data were from a city but the system is used in a rural area, etc.

In other cases, you may need to use technical and sectoral expertise to identify whether the system is trained and tested on representative, relevant, accurately and appropriately measured and generalisable datasets.

Some key issues to consider would include a variety of biases. These biases are not independent of each other: one bias will influence another.

- Whether it is likely that there is historical bias in the data. In all domains where there is a historical or current inequality this inequality is reflected in data, unless this is very carefully corrected for. Examples are past over-policing of black communities and periods of unemployment owing to child or other caring responsibilities impacting gender equality.
- Whether there is representational bias in the data. For example, does the target population reflect the use population? For example, data that are representative of Lisbon may not be representative for Porto. Data representative of Helsinki

30 years ago may not reflect today's population. There may be additional issues created by who is represented in the data and by how much. For example, in health data there could be an under-representation of women and/or an over-representation of women who are pregnant. Any of these could skew the data and impact outcomes. Additionally, pay attention to how minorities are represented in the data. For example, when certain accents have not been included in a voice recognition system, this system will work less well for these accents. If hijab-wearing people have not been included in the data for facial recognition, there is the possibility that people with hijabs are not recognised well.

- Whether there is a selection bias in the data. This is the case when there are only data for a specific sub-group of the data. For example, in loan acceptance there is only information on who defaults on their loan for the group that received the loan in the past. Police patrol data only includes information on the areas where the police did patrol. Fraud data may only include the group who was investigated for fraud in the past. Recruitment data contains less information on applicants whose CVs were never selected for further steps. This could skew the data, especially if people with a specific protected characteristic were historically over- or under-represented in this context.
- Whether there is measurement bias in the data. This is the case when the labels (the measurement) do not reflect the concept they are intendent to measure. For example, if you want to measure fraud in welfare benefit but decide that all incorrect awards of benefits are relevant to consider, the result will be that you include innocent mistake as well as fraud. This in turn can have a disparate impact on certain groups, for example those with low literacy, a low level of education and those who do not speak a national language as a first language. Another form of measurement bias is when human biases (or human discrimination) influence the recorded labels that are now considered the ground truth. Any situation where the ground truth labels are the result of a human evaluation with some level of individual discretion, there is a risk that human biases resulted in a measurement bias. Examples are teacher evaluations, recruitment data or fraud investigations.

Questions to consider

Consider the below questions with bias and inequality in mind. All questions below are subjective, nuanced and context specific. Answering these will require a good understanding of the sector and its existing inequalities and of the systems and the technology used. The result of this assessment will mostly provide direction for further assessment or can be used to build a prima facie case.

Note that in the case of manually designed algorithmic systems there will not be any training data. In some AI systems the training data do not include labels. In that case there is still an expectation of test data, which do include some form of labels to test if the model provides correct or acceptable outputs.

Training, testing and validation data

- How were training, testing and validation data sets chosen?
- What training/testing/validating data were collected?
- What are the sources of those data?

- For what purpose were the data originally collected? Do any potential issues arise from their use in a different context? For example, if data were collected for the purposes of assessing health, does reusing them for insurance purposes raise any potential measurement bias issues?
- What methods were used to collect the data?
  - Do these methods appear reasonable, in the sense that they reasonably result in reliable, relevant data for the intended task of the algorithmic system?
  - Did they ensure the data were representative and appropriately measured? Can it reasonably be expected that the data generalise to the domain and context in which the algorithmic systems are now applied?
  - Were additional data collected (or labelled) to be used as training/testing/validation data? Was a random sample used to collect data?
- Where the dataset is sourced from a third party, how was it procured? Were the third-party-provided data vetted?
- Are there historical inequalities that are likely to be reflected in the data (see the section on biases above)? Also consider multiple/intersectional discrimination here.
- Are minorities reflected enough in the data? This is particularly relevant to algorithmic systems that are applied in sectors where culture, background and physical appearance may influence outputs.

Labels

- How reliable are the labels?
- Do the labels match the purpose of the systems? In other words, do the labels measure what the system is supposed to predict?
- Can correctness be objectively determined? Has this been determined?
- In cases where there is human judgment involved in the labelling, could human biases have skewed the labels? Are there any reasons to suspect discrimination?

Existing mitigating measures

- How was data quality assessed?
  - What steps were taken to address any quality issues discovered, such as completing or removing data?
- What measures were taken to ensure the data were representative, relevant, accurately measured and generalisable?
- How were any potential bias and inequality in the dataset mitigated?
  - Were any bias-mitigating measures[53] implemented?
  - For which biases were these implemented? Are there any recognised biases for which no mitigating measures were implemented?

53. Bias-mitigating measures could be any measures taken to prevent bias in data or in a system. These could include random sampling, additional data gathering to increase representativeness of data, strict protocols for evaluation of cases, four-eye review in evaluation of cases, reweighing of data and many other measures.

- What techniques were used?
- Is information available on the effectiveness of these bias-mitigation measures?

Potential sources of information to assess the data used

Complainant

EU AI Act, Article 86, right to an explanation

GDPR, Articles 13-15, information provided to the data subject

Publicly available

EU database for high-risk AI systems

- Section A, high-risk AI systems – information used by the system, including data and inputs.
- Section C, deployer – summary of the DPIA and FRIA (unless used for law enforcement or migration control).

Respondent

From the provider:

EU AI Act, Annex IV(2)(d), technical documentation

- "Where relevant, the data requirements in terms of datasheets describing the training methodologies and techniques and the training datasets used, including a general description of these datasets, information about their provenance, scope and main characteristics; how the data were obtained and selected; labelling procedures (such as for supervised learning) and data-cleaning methodologies (outlier detection, for example)."

EU AI Act, Article 10, data governance and management practices

- Providers are required to have implemented appropriate practices to the level that the datasets are "relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used. Those characteristics of the data sets may be met at the level of individual data sets or at the level of a combination thereof".

This covers at least:

- relevant design choices;
- data collection and use (Article 10(2)(b), (e) and (g));
- data preparation processing operations, including annotation and labelling (Article 10(2)(c));
- formulation of assumptions particularly in respect of measurement and representation (Article 10(2)(d));

- explicitly with a view on bias, they are required to examine and "take appropriate measures to detect, prevent and mitigate possible biases" (Article 10(2)(g)) in the datasets that are likely to "have a negative impact on fundamental rights or lead to discrimination prohibited under Union law" (Article 10(2)(f)).

EU AI Act, Article 17(1)(f), quality management

- Written policies, procedures and instructions shall include: "systems and procedures for data management, including data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purpose of the placing on the market or the putting into service of high-risk AI systems".

From the deployer:

EU AI Act, Article 13(b)(vi), instructions for use

- The provider should provide "when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the high-risk AI system" (in the information provided to deployer by provider).

EU AI Act, Article 26(4)

- To the extent the deployer exercises control over the input data, that deployer shall ensure that input data are relevant and sufficiently representative in view of the intended purpose of the high-risk AI system.

Other

- Documentation initiatives
- Datasheets for datasets
- Model cards for model reporting
- Applied data governance and quality standards – when the respondent mentioned the use of standards, these standards can be used to understand what the respondent committed themselves to.
- For law enforcement/migration control there may be additional information in the database available to the relevant MSA.

Indicators of discrimination

The indicators below show issues with the data, which can contribute to a prima facie case by indicating generally that unreliable or biased data are used and can be used to motivate requests for additional testing. This is likely to be an incomplete list. There may be other considerations resulting from the above that are not listed here.

- General data issues:
  - not representative (geographical area, sector);
  - improperly sourced (repurposed);
  - not up to date;

  - there is selection bias;
  - there is measurement bias in the sense that the label reflects a different concept than what is predicted or labels are generally unreliable.
- Indicators of data quality issues related to discrimination:
  - data are not representative of all those affected;
  - high likelihood of reflecting historical or persisting inequalities;
  - selection bias is likely to lead to over or under-representation of groups with protected attributes;
  - measurement bias is likely to affect groups with protected attributes;
  - there is an indication of discrimination in the sourcing, creation or labelling of the data.
- Decisions in respect of data are insufficiently documented.
- No mitigation measures or mitigation measures can be shown to be effective.

Indicators of non-compliance with the AI Act's high-risk systems

While non-compliance with the AI Act is not the focus of this assessment methodology, any indication that the requirements of the AI Act are not met can inform remedial action (see step 4).

- The provider cannot show that they have implemented practices that ensure the datasets are "relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used. Those characteristics of the data sets may be met at the level of individual data sets or at the level of a combination thereof". Or they cannot provide documentation as evidence of this.
- The provider has not performed bias testing, or has not tested of all the relevant biases.
- The provider has not implemented effective measures to prevent and mitigate biases they detected or suspect.

- Record any general data issues, any issues relating to data quality, issues of insufficient documentation and any concerns about mitigation measures.
- Record any data issues related to inequality and discrimination, any concerns about mitigation measures and – where available – an argument for how these would lead to unequal treatment in the current case.
- Record any indicators of non-compliance with the AI Act's provisions relevant to data.

3.6. Testing and evaluation

The results of testing and evaluation can provide valuable information for assessing whether discrimination has occurred. The core question here is whether the algorithmic system provides unequal results for different groups of individuals. One way to show this is through statistics on the outputs of the system.

When statistical equality data are available, these data should be evaluated for validity and reliability (see below). It is therefore relevant to consider the validity and reliability of the data used to calculate these statistics. Therefore, this section should be read in conjunction with section 3.5.

In this step technical and sectoral expertise can be helpful.

To test outcomes for different groups with different protected characteristics, there need to be data available on these protected characteristics. For example, to test if a system produces different outputs for men and women, one needs to know for each of the test data subjects who is a man and who is a woman. These data might not always be available. In this case testing should focus on characteristics that are available, including those that are or might be related to protected attributes. For example, data on ethnic background may not be available, but data on nationality are, or for facial images there may be no data available about racialised people but the colour value of facial images could be used.

Acquiring (additional) statistical data

When statistical data are not available or are insufficient to assess algorithmic discrimination, there are some options that may help to acquire (additional) statistical data.

Evaluation and testing by the MSA

Where an EB is unable to ascertain whether an infringement of rights under Union law has occurred, Article 77(3) of the AI Act enables the EB to make a "reasoned request to the MSA to organise testing of the system through technical means". The EB should be closely involved with the testing.

Recital 157 makes clear that the procedure under Article 77 should be applied to high-risk AI systems presenting a risk to fundamental rights, prohibited systems placed on the market (Article 6), put into service or used in violation of prohibited practices in the act (Article 5) and AI systems that are either high risk or not high risk and have been made available in violation of the transparency requirements of the regulation and present a risk (Articles 6(4) and 50).

Testing by the EB or in collaboration with third parties

Equality bodies may create their own equality data while exercising their monitoring and other mandates under the discrimination and/or equality body directives and regulations or otherwise. However, care may need to be taken when using these data as there is a risk that it would not be considered independent when exercising a litigation function. It is currently unclear how the confidentiality obligations

in Article 78 of the AI Act would impact the use of information obtained for one purpose on civil litigation (cf. criminal and administrative proceedings that are explicitly referred to).

Consider whether the evidence on which you are seeking to rely was obtained:

1. as a result of the equality body exercising their independent and impartial adjudication role or monitoring and data-processing role; or
2. for the purposes of litigation.

If the data were created for 1, the independence of those data might be questioned. As noted by Equinet:

> Where an equality body litigates based on its own data, the court could, in theory, struggle to see such data as external and independent. All the more, where an equality body adjudicates cases, relying (in part) on its own equality data, parties to a case and other observers could question such a practice on at least two grounds: is the body an impartial adjudicator if it proactively identifies and uses evidence that favours the alleged victim; and is such evidence credible if the body itself produced it, being by definition pro-equality/pro-victims. Such potential (perceived) fair trial/equality of arms issues could affect an equality body's overall credibility in society, including its reporting role. (Ilieva 2024)

Statistical analyses of the algorithmic system

In cases where the algorithmic system and relevant data are available to the EB, the EB could perform their own statistical evaluation. Both fairness metrics and enforcement methods have been implemented in a range of open-source fairness toolkits. These toolkits can be used to measure performance gaps in algorithmic systems or datasets made available to them. Much used examples include IBM AI Fairness 360 and Microsoft Fairlearn, but there are many others available. There is not a single specific recommended toolkit as each have their own advantages and drawbacks (Mittelstadt 2024).

Situation testing

"Situation" testing can also be used to generate evidence of discrimination. Situation testing is an experimental method where pairs of test subjects are established that differ only in a protected characteristic to test differences in treatment.

In some contexts, such as algorithmic recruitment, a viable option is to gather statistical data about a specific algorithmic system through (discrimination) situation testing. In various countries, including the United Kingdom, the Netherlands, France, Denmark, Finland and Sweden, situation testing has been admitted as a valid form of evidence (European Commission 2019). Situation testing on a large scale can also produce statistical data and has been applied in many different contexts, such as access to employment, housing and other kinds of goods and services. The results of testing are regarded as admissible evidence in several EU countries. To secure credible results, the EB might need to collaborate with expert parties to conduct the testing (Makkonen 2016).

Collaboration with statistics institutes/using general statistics

General statistics may be used to argue that the use of proxies leads to a difference in treatment. For example, in the Dutch example of the college grant checks:

- the algorithm differentiated on education level;
- according to general statistics from the Dutch Bureau of Statistics, students with a non-Western migration background are over-represented in the lowest education levels: there are about twice as many students with a non-Western migration background as would be expected compared to all students (StatLine – Mbo; studenten, niveau, leerweg, migratie 2005/'06-2021/'22);
- it follows, without accessing specific background data for individual students, that using education background in the algorithmic systems leads to unequal treatment.

Courts' approach to statistical data

On the necessity of statistical data

Statistics by themselves do not necessarily disclose discrimination or a discriminatory practice (*Hugh Jordan v. the United Kingdom*, Application No. 24746/94, European Court of Human Rights).[54] They are among the relevant forms of evidence that may be used to establish or rebut a prima facie case of direct or indirect discrimination. Courts may generally be more inclined to accept statistical evidence presented by complainants to establish a prima facie case of direct discrimination than to rely on such evidence from respondents to rebut it, reflecting the informational imbalance between the parties and the recognised difficulties complainants face in substantiating discrimination claims (Makkonen 2007). It will be for the national court to assess whether the statistics available are "valid" and can be taken into account (see Enderby, Case C-127/92, paragraph 16).

Statistical data and direct discrimination

In a direct discrimination case, statistics can reveal the existence of a discriminatory pattern and thereby form evidence of direct discrimination in relation to an individual complaint. However, the use of statistical evidence is usually not required for the purposes of making a prima facie case of direct discrimination.

Statistical data and indirect discrimination

Statistical data are particularly useful in the case of indirect discrimination, where a complainant may use statistics to demonstrate that the application of an apparently neutral practice or rule has a disproportionate effect or impact on a specific group of persons in comparison to others in a similar situation (FRA 2018: 242).

54. Statistics showed a difference between the number of those killed of different religions but not whether those killings were unlawful or through excessive use of force by the members of security forces (paragraph 154).

In particular, "where an applicant is able to show, on the basis of undisputed official statistics, the existence of a prima facie indication that a specific rule – although formulated in a neutral manner – in fact affects a clearly higher percentage of women than men, it is for the respondent Government to show that this is the result of objective factors unrelated to any discrimination on the grounds of sex" (*Hoogendijk v. The Netherlands* 2005).

No strict threshold has been set but a substantial figure usually has to be achieved to show differential impact, that is, "far greater number" (Ingrid Rinner-Kuhn 1989) or "considerably lower percentage" (Helga Nimz 1991; Maria Kowalska 1990) or "far more" (M. A. De Weerd 1994), although submitting statistical data to prove indirect discrimination is not a formal requirement (see *D.H. and others v. the Czech Republic* 2007: paragraph 188).

However, precise statistical data are not required, particularly if the party claiming to be discriminated against does not have access to these statistics or has difficulty accessing them (Minoo Schuch-Ghannadan 2019).

Using other data and evidence

Proof as to the practices or beliefs of others towards those belonging to the same protected category may be enough. For example, a practice of placing children in separate classes based on their insufficient command of Croatian was only applied to Roma students, which gave rise to a presumption of differential treatment despite statistics failing to establish discrimination. The European Court of Human Rights has made clear that "indirect discrimination may be proved without statistical evidence" (*Oršuš and Others v. Croatia* 2010).

In cases involving algorithmic systems, other factual information and evidence may also suffice to establish prima facie discrimination. For example, in the Deliveroo case, the court did not require extensive statistical tests or complex data analysis. Instead, the design of the system per se – as reconstructed at a basic level from available information such as contractual clauses, platform FAQs, the respondent's external and internal communications, and testimonies from affected individuals – combined with an assessment of its foreseeable effects was sufficient to demonstrate a disproportionate disadvantage and to establish prima facie discrimination.

Evaluating statistical equality data by the respondent

For the purposes of equality law, statistical data must be both valid and reliable.

The tests for validity and reliability should be applied throughout. The following three-step process may assist.

- Has the approach taken by the provider or deployer in testing and evaluation been based on or produced valid and reliable statistical data?
- Is your statistical evidence seeking to challenge the respondent both valid and reliable?
- Is any statistical evidence in rebuttal valid and reliable?

For statistical data to be considered "valid", the following criteria should be met.

- Generally appear to be significant.
- Cover enough individuals.
- Capture phenomena that are not fortuitous or short term.
- As a whole be "relevant and sufficient".

Reliability of statistical data implies stability or consistency of the measurement/test applied. A measure of discrimination for example is reliable to the extent to which the measuring procedure yields the same results in repeated trials. For example, if one measures the number of reported equality incidents per year, but the number of competent (equality) bodies changes over time, this will have a negative effect on the reliability of this measure and will also impact on its comparability over time. No measure is reliable; reliability is therefore always a matter of degree.[55]

Choice of equality metrics

In data science several metrics have been identified to measure different notions of what is fair. These metrics have not been informed by non-discrimination law and the overlap between measures of fairness in the field of data science and AI, and notions of equality, are not always clear (Weerts et al. 2023). Unfortunately, it is mathematically impossible to create a system that is fair according to all technical metrics.

Therefore, it is crucial to determine what a difference in treatment and a particular disadvantage (as integral to discrimination) means in the context of the case at hand and to choose the metrics that most closely overlap with this. Note that simply presenting any fairness metric that shows the system to be "fair" on this metric does not constitute a system that results in equal treatment. Where there is unfairness, it will be important to consider why that decision to employ that set of equality metrics was made and what measures have been taken to address the resulting inequality.

Demographic parity measures whether the probability of a certain prediction is the same for two groups. This metric is most relevant when one output is disadvantageous over other outputs for the people involved. This reflects the concept of unequal treatment best in examples such as fraud prediction (when one group is suspected of fraud more often than the other group) or recruitment (when one group is selected for an interview more often than the other). In many cases demographic parity is the relevant metric, unless there are compelling reasons to rely on another metric. Note that demographic parity is also sometimes referred to as independence, group fairness, statistical parity, disparate impact, equal selection rate or equal acceptance rate.

55. See European Commission 2021: 20; Enderby, 1993, paragraph 17; Seymour-Smith, 1999, paragraph 62. On the general requirements for statistics in non-discrimination cases; see *Enderby v. Frenchay Health Authority and Secretary of State for Health*, paragraph 17.

Other relevant metrics rely on errors in the system and test whether the systems result in more errors for one group over the other. This type of metric is most relevant when harm stems overwhelmingly from errors in the systems, not the output itself. Examples where error-based metrics are the most relevant are facial recognition and diagnostic testing in medicine. See Table 6 below for an overview of potentially relevant metrics .

It is unlikely that a one-size-fits-all approach to testing will be sufficient. Instead, it will be relevant to consider both the statistical models used and their limitations and the surrounding circumstances such as the decision-making organisation and the processes they adopt (Barocas et al. 2023). As such, "numbers" without context will have insufficient meaning to be valid or reliable.

Even when demographic parity is chosen as the primary metric, it is advised to additionally consider a metric that considers errors. There is a requirement for providers to set an "expected level of accuracy" for specific groups of people (AI Act, Annex IV(3)).

Equality statistics can be presented as a ratio or as separate metrics between groups. Some examples follow.

- Demographic parity statistics in a recruitment setting can be expressed as: 25% of male applicants are invited for an interview and 15% of female applicants are invited after automated CV selection. This can also be expressed as a ratio: 0.15/0.25 = 0.6.
- Equal opportunity for cancer screening can be expressed as: 75% of men who have cancer are detected by the screening tool and 65% of women who have cancer are detected by the screening tool. This can also be expressed as a ratio: 0.65/0.75 = 0.87.

Table 6. Description of fairness metrics

(adapted with permission from Mittelstadt 2023)

Metric	Description	Applicable when	Example
Demographic parity	Different groups should receive the positive outputs ate the same rate. Demographic parity could be referred to as independence, group fairness, statistical parity, disparate impact, equal selection rate or equal acceptance rate.	▸ Situations where a particular output itself (and not errors) is disadvantageous. ▸ Situations where historical data are expected to be prejudicial. ▸ Situation where there are no reliable labels (no agreed-upon ground truth).	Recruitment, loan acceptance, fraud detection, access to education.

Metric	Description	Applicable when	Example
Equal opportunity	Different groups should receive false negatives at the same rate. Could also be referred to as false negative error rate balance.	▶ Situations where the overwhelming harm comes from false negatives. ▶ There are reliable labels (agreed-upon ground truth).	Disease screening.
Predictive parity	The percentage of false positives, among all positives, should be the same for different groups. Could also be referred to as outcome test or positive predictive value parity.	▶ Situations where the overwhelming harm comes from false positives. ▶ There are reliable labels (agreed-upon ground truth).	Facial recognition by the police to identify a person of interest.
False positive rate balance	Different groups should receive false positives at the same rate. Could also be referenced as predictive equality.	▶ Situations where the overwhelming harm comes from false positives. ▶ There are reliable labels (agreed-upon ground truth).	Facial recognition by the police to identify a person of interest.
Equalised odds	True positive and false positive rates should be the same for different groups. Could also be referred to as conditional procedure accuracy equality and disparate mistreatment.	▶ Situations where the harm from false positives and false negatives should both be considered. ▶ There are reliable labels (agreed-upon ground truth).	Treatment of illness by performing a risky surgery.

Evaluating statistics provided by the respondent

To evaluate the validity of statistical equality metrics, EBs should at least consider three issues.

1. Generally, the quality and biases in the data used to compute the metric (see step 3.5).
2. The design of the metric and choice of comparative groups.

In considering the way in which a provider of a system has identified and measured any performance gaps, EBs should pay particular attention to how the decision to measure has been taken and which groups of people are being compared. This is an important decision in the context of non-discrimination law where defining appropriate "disadvantaged" and "comparator" groups is often key. (Mittelstadt 2024). The choice of groups may (deliberately) hide real-world unequal outcomes.

EBs are advised to:

- consider what appropriate "disadvantaged" and "comparator" groups would be considered, prior to looking at the respondent statistics;
- consider whether the respondent has chosen and defined the same groups and, if not, the EB should consider what information is added or lost in the choices of the respondent;
- consider intersectional groups, because focusing solely on single-characteristic groups hides intersectional inequalities;
- in order to understand comparator groups chosen by the respondent, look at explanations provided by the respondent**,** particularly any information on the extent to which a variation in the personal data taken into account would have led to a different result;
- in cases where the respondent has not reported on relevant fairness metrics or has narrowly defined impacted groups, consider acquiring additional statistical data (see the box "Acquiring (additional) statistical information" above) (Mittelstadt 2024).

Statistical equality metrics are frequently part of broader performance reports that include a variety of test results measuring various aspects of a system's performance, such as accuracy (how often the system makes the correct prediction) and robustness (resilience against errors, unanticipated behaviours and real-world changes (drift)). It is valuable to EBs to understand the performance in general, as the performance of the system is highly relevant in the assessment of algorithmic discrimination, specifically when considering a potential objective justification (see step 3.8) where core questions will involve ascertaining if the system is suitable or appropriate and necessary.

3. Relevance of the metrics to the current system as applied in practice.

The metrics should reflect the current algorithmic system. The tests applied may have become out of date or the process around the system may have changed (for instance, the system applies a government policy and that policy has changed).

Take note that the metrics reported should reflect the system after any mitigating measures to "debias" or prevent discrimination are applied. If these measures are manual, EBs should ensure the statistics reflect the outcome after this manual intervention.

Where a high-risk AI system has been given a certificate of conformity following an assessment, it will be presumed to comply with the data requirements in Article 10(4) of the AI Act, namely "that they take into account to the extent required by the intended purpose the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting within which the high-risk AI system is intended to be used".

It is likely that these considerations will guide the application of the "validity" test (see more on statistical data under step 3.6), but it is important to note that this presumption can be rebutted. Equality bodies may wish to consider, in particular, whether the data used in fact meet these requirements for the given use of the AI system. If the system is being used other than for its intended purpose, this presumption will not apply.

Questions to consider

On general performance testing

- Which aspects of performance have been tested?
- How and where has the system's performance across individuals and groups of people been recorded?
  - Will these figures be updated over the life cycle of the system? If so, how?
- What potential impacts on individuals and groups of people have been considered in carrying out performance testing?
- Was any form of harm chosen as a focal point for testing (such as false positives or false negatives)?
- What measures were used for performance testing?
- Have confusion matrices been produced through performance testing?
- How were testing results validated?
- Are the data used to carry out performance testing sufficiently representative, relevant and accurately and appropriately measured (see step 3.5)?
- Does performance testing by the respondent meet the tests of validity and reliability?

Statistical equality data

- Which (types of) statistical equality data, fairness metrics or bias tests were used?
  - Do the metrics chosen by the respondent reflect equal treatment for the specific context? (Usually demographic parity unless there are clear justifications for other metrics, see Table 6 above).
  - In cases where there are error-based metrics, were the same forms of harm considered as in regular performance testing? (For example, when regular performance testing used a metric focusing on false positives, did equality testing do the same?) When testing for equality based on performance, logically the most relevant performance metric should also be used for this equality test. An unmotivated choice of a different metric could point to an omission in the equality testing.

  - What is the justification or basis on which these were chosen?
  - Were others considered and/or rejected? If so, why/not?
  - Was the range of tests used covering different protected characteristics sufficiently broad to capture different types of potential discrimination or impacts affecting different (intersectional) groups?
  - Have relevant "comparator" groups been chosen for each test?
  - Are these considerations included in the system's technical documentation?
- Were any (types of) fairness enforcement or de-biasing methods used?
  - What is the justification or basis on which these were chosen?
  - Were others considered and/or rejected? If so, why/not?
  - Are these considerations included in the system's technical documentation?
- What benefits and harm resulted from fairness enforcement or de-biasing?
  - Which groups of people did/will this impact?
  - Were the secondary effects on equal treatment for other groups investigated?
- How were testing results validated?
- Are the data used to calculate the statistics sufficiently representative and relevant, and accurately and appropriately measured (see step 3.5)?
- Do the statistical data provided by the respondent meet the tests of validity and reliability?

Potential sources of information to assess statistical equality data

Complainant

GDPR, Article 15(1)(h), meaningful information about the logic involved

Respondent

From provider

EU AI Act, Article 10, data and data governance

EU AI Act, Article 11, technical documentation (Annex IV(2)(g)):

- "the validation and testing procedures used, including information about the validation and testing data used and their main characteristics; metrics used to measure accuracy, robustness and compliance with other relevant requirements set out in Chapter III, section 2, as well as potentially discriminatory impacts; test logs and all test reports dated and signed by the responsible persons, including with regard to predetermined changes as referred to under point (f)".

EU AI Act, Article 11, logs

Other information that could be requested from the respondent:

- access to the system
- example (synthetic) datasets

- any reports on the performance or reliability of the system, including error matrices
- information on the type of testing and methodology of testing performed, including potential (harmonised) standards applied
- any reports on bias and fairness testing performed
- information on the type of testing and methodology of testing performed, including potential (harmonised) standards applied
- voluntary HRIA or FRIA, DPIA, ethics or child rights impact assessment
- any other (risk) assessments shared by the respondent
- freedom of information requests.

Indicators of discrimination

- There are gaps in outputs or errors between groups of persons of protected characteristics, based on the most relevant metrics that reflect equal treatment for the specific case.
- The most relevant metrics that reflect equal treatment for the specific case are not available or irrelevant metrics are applied.
- There are gaps in outputs or errors between groups of persons of protected characteristics, based on other metrics (other than the metric that most closely reflects equal treatment for the specific case).
- Not all impacted groups have been included, or the impacted groups have been too narrowly defined, not considering intersectional discrimination.
- Correct groups were identified and relevant metrics are applied but conclusions do not stand up to scrutiny, for example because of data issues.
- It only reports one tested metric rather than the results of multiple fairness metrics (such as precision, recall, error rates).[56] Testing on multiple metrics may be needed to reveal different kinds of performance gaps.

Cumulative indicators of discrimination

All the earlier mentioned indicators can work cumulatively; these are some examples.

- Risk of discrimination identified by provider/deployer (see step 3.3) but testing did not cover complete set of individuals and/or groups at risk of harm – consider in particular proxies, multiple and intersectional discrimination. For example, it tested for sex discrimination but not race or ethnicity while risk of racial discrimination was identified.
- (Risk of) discrimination identified by third parties (see step 3.1) but testing did not cover complete set of individuals and/or groups at risk of harm – consider in particular proxies, multiple and intersectional discrimination. For example, it

56. In data analyses different metrics can be used to reflect different aspects of the performance of a system. For example, precision focuses on the accuracy of positive predictions (avoiding false alarms), and recall measures the ability to detect all actual positive instances (avoiding missed events).

tested for sex discrimination but not race or ethnicity while in existing similar cases people have been disadvantaged based on race and pregnancy.

- Input criteria are strongly related to protected attributes or proxies are used in algorithms (see step 3.3) and no testing is performed to understand if equal treatment requirements are met for the protected group.

- Record any output or treatment gaps as revealed in the statistics.
- Record any issues with the reported statistics (such as the wrong metric or data issues).
- Record any gaps in testing.
- Combine the results of this step with the previous step's results to understand if together a case of prima facie discrimination can be argued and/or the respondent has successfully rebutted the presumption or justified the discrimination (if looking at justification, see also 3.4 to consider the aim of the system).
- Record the conclusion.

Example: Smart Check Amsterdam

This model was designed to screen applications for welfare and identify those most likely to involve major errors, flag them and send the cases to an investigations department for further scrutiny. The aim was to reduce those flagged for investigation.

Fifteen characteristics were considered, including a variety of factors such as whether the applicant had previously applied for or received benefits, the number of addresses they had and the sum of their assets to determine a risk score. It deliberately avoided using protected grounds and tried to avoid "proxies".

According to the authors, "it was trained on a dataset encompassing 3 400 previous investigations. This led to a risk of embedding historical bias e.g. if human caseworkers had historically made higher rates of mistakes with a specific ethnic group the model could wrongly learn to predict this group commits fraud at higher rates".

Amsterdam officials adopted a definition of fairness based on equally distributing the burden of wrongful investigations across different demographic groups. It also engaged in extensive consultation. All stakeholder groups from the Amsterdam DPA to external consulting firms gave the project their approval, except the group representing those directly affected (benefits recipients).

Nonetheless the system was put into testing. The initial model was twice as likely to wrongly flag non-Dutch applicants and nearly twice as likely to flag an applicant with non-Western nationality than one with Western nationality. It was also 14% more likely to wrongly flag men for investigation.

Amsterdam city also tested the data collected from human caseworkers. In that process they discovered humans were more likely to wrongly flag Dutch nationals and women.

Because of the existence of bias, the team attempted to use training data re-weighting to remedy the problem. This meant that applicants with a non-Western nationality deemed to have made meaningful errors in their applications were given less weight in the data and those with a Western nationality given more. Once the model was reweighted, Dutch and non-Dutch nationals were equally likely to be wrongly flagged.

The problem with re-weighting the data was that although it might reduce fairness against people with a migration background it would not guarantee fairness across intersecting identities.

Nonetheless the system was rolled out on a limited basis to be used on real applicants. Its performance was to be measured on two key criteria: i) could it consider applicants without bias?; ii) could it detect welfare fraud better and more fairly than human caseworkers?

Instead of flagging fewer applicants for investigation it flagged more. And was no better than a human at identifying those who required extra scrutiny. Moreover, despite the re-weighting the system now wrongly flagged applicants with Dutch nationality and women. In addition, welfare applicants with children were also more likely to be flagged for investigation.

Ultimately the project was not continued.

The above is a summary of "Inside Amsterdam's high-stakes experiment to create fair welfare AI", 11 June 2025, MIT Technology Review, Lighthouse Reports and Trouw E. G., Geiger G. and Braun J-C. For more detailed information, see Lighthouse Reports 2025.

3.7. Assessing whether the evidence is sufficient to support a prima facie case of discrimination involving an AI or algorithmic system

- Review all the information and answers to the questions in step 3 to consider whether a prima facie case of discrimination has been made out. Use the indicators of discrimination as a guide.
- At this stage, assume there is no adequate explanation for the facts demonstrating a prima facie case (there may be; however, this would be relevant to assessing the respondent's defence (see 3.8 below)).
- Similarly, where there is a lack of evidence or a lack of transparency about a system, this should not prevent a case being brought or continued at this stage. Remember in step 1 it was identified that early striking out of claims where there is an informational imbalance was likely to be inappropriate: see 1.4 *Manjang v. Uber Eats UK Ltd & Others* (2021).

You may need to consider all or some of the following.

- Who is the victim and what protected grounds are engaged?
- Who is the appropriate comparator? Why has this comparator been chosen?
- Has direct or indirect discrimination occurred?
- Are there multiple or intersecting forms of discrimination?
- Have you established any proxy discrimination?
- Why has the discrimination occurred (causation)? Consider for example, whether the discrimination has occurred because of the aim of the system, the development of the system, the use of data within the system or because the system is not being used for its intended purpose or is being used incorrectly by the deployer.

For indirect discrimination also consider the following.

- What is the neutral provision, criterion or practice?
- How are the effects of the provision, criterion or practice significantly more negative in effect on a protected group?
- Has the complainant proved facts from which conclusions could be drawn that they have been treated less favourably owing to protected grounds?
- If the difference in treatment is not "directly" related to a protected characteristic, is it sufficiently linked? This will be particularly important when considering proxy discrimination.
- What was the context of the discrimination? Could the respondent successfully argue that the decision was taken for a reason other than prohibited discrimination?

Considering all the circumstances, has a prima facie case of discrimination been established?

If yes, continue with section 3.8.

If no, consider the following.

- Have there been any failures to comply with documentation, testing, monitoring or reporting obligations that may explain the discrimination or result in gaps in the evidence?
- Are there any pre-action steps that could be taken to fill any gaps in the evidence?
  - Consider making applications for disclosure of evidence based on transparency and access to justice considerations under Article 13 of the European Convention on Human Rights (right to an effective remedy before a national authority) and Article 47 of the Charter of Fundamental Rights of the European Union (right to an effective remedy and to a fair trial).
  - Note that in some circumstances where the respondent seeks to argue commercial confidentiality or the rights of third parties, confidential procedures may be available via the MSA, DPA or courts. Current case law suggests that there is a growing inclination to require this information to be made available; see Dun & Bradstreet (in the context of GDPR):

    > Where the controller takes the view that this information cannot be provided without disclosing third party details or trade secrets the data controller is

required to provide the allegedly protected information to the competent supervisory authority or court, which must balance the rights and interests at issue with a view to determining the extent of the data subject's right of access provided for in Article 15 of that regulation. (see also Confidentiality)

For the relevance of providing statistical information in establishing a prima facie case of discrimination, see step 3.6 about statistical data.

Transparency

A court may draw inferences from a failure to provide relevant statistical or other data. Inferences of discrimination may also be drawn from surrounding facts and circumstances such as a respondent's responses to questions or a failure to comply with a relevant code of practice. By not providing information, the respondent may in practice fail to discharge the burden of proof, leading the court to presume discrimination (see 3.8 for the circumstances where a legal burden to provide information arises).

- Inferences can often be drawn from an equivocal, inadequate or evasive response to a questionnaire or disclosure during the pre-action process or proceedings.
- Inferences may also be drawn from refusing to confirm or deny the existence of information.

Questions to consider

- Have there been any relevant failures to disclose information by the respondent that led to a lack of transparency? For example, was there an adequate response to any requests under the GDPR, any freedom of information requests, pre-action correspondence, requests made under the EU AI Act or otherwise?
- Can any inferences be drawn from the available evidence? For example, statistics, surrounding facts, known discrimination?
- Can any inferences be drawn from the lack of evidence? For example, a failure to provide answers to questions, failure to comply with guidance or codes of practice?
- In all the circumstances, do the surrounding facts and circumstances, including any failure to respond to questions or requests for information such as a DSAR request or to provide an explanation under Article 86 of the EU AI Act, provide for an inference of discrimination to be drawn?

Examples from the CJEU

- C-109/88, *Handels- og Kontorfunktionærernes Forbund I Danmark v. Danfoss*: the union brought a case on behalf of female workers in a company because they earned on average 7% less than their male colleagues in the same or similar job position. In this case the CJEU decided that as the pay system used was completely lacking in transparency, discrimination must be presumed, and the burden of proof must shift to the respondent/employer to show that there are objective and non-discriminatory reasons for the difference in paid wages.

- C-415/10 *Galina Meister v. Speech Design Carrier Systems GmbH*: the plaintiff claimed discrimination on grounds of gender, age and ethnic origin in the employment selection process, and requested the court to instruct the employer to make public the information on whether another candidate was employed at the end of the process. The CJEU considered that although the non-discrimination directives do not provide for the right of access to this type of information, the respondent's refusal to give any access to information to the plaintiff may be one of the factors that could be taken into account in the context of establishing the facts from which direct or indirect discrimination can be presumed to have occurred.

Examples of the consequences of lack of transparency from national case law

- **Netherlands case NL24.38560 (2025) (interlocutory judgment)**

  The court decided of its own motion to investigate the existence of a visa algorithm and instructed the relevant minister to:

  - provide information relevant to decision making;
  - conduct an HRIA;

  on the grounds of transparency in decision making and right to effective legal protection under both Article 13 of the European Convention on Human Rights and Article 47 of the Charter of Fundamental Rights of the European Union.

- **UK Tax Tribunal case (First tier):** Elsbury v. The Information Commissioner **(2025) UKFTT 915 (GRC) (2 August 2025)**

  HMRC's failure either to confirm or deny it holds the requested information reinforces the belief based on indicators in HMRC correspondence dealing with R&D claims that AI is being used by HMRC officers – perhaps in an unauthorised manner – thus undermining taxpayers' trust and confidence in HMRC's treatment of claims, in turn discouraging legitimate claimants from making claims thereby hindering the policy objectives of the R&D tax relief scheme itself.

- ***Filcams Cgil Bologna and Others v. Deliveroo Italia S.R.* (2020)**:

  The Court of Bologna found that the company had failed to discharge the burden of proof, as it neither demonstrated nor explained the concrete functioning of the algorithm and provided no evidence of its actual operation. It did not clarify which specific criteria were used to determine riders' statistics, and these were not disclosed on the platform, which only referred generically to "reliability" and "participation" as indicators for allocating future work opportunities. For further details of this case, see Purificato (2021).

3.8. Can the respondent show the difference in treatment is not discriminatory?

In practice, you will likely need to consider the same evidence and ask the same questions as set out above (3.1-3.8). However, it is possible that at this stage there will now be additional evidence to review or the respondent's explanation of the evidence or system will be more detailed. This will require review of the original material and analysis previously undertaken to ensure it remains valid in light of the new information.

Once the person alleging discrimination has established a prima facie case of discrimination, the burden then shifts to the respondent, who must show that the difference in treatment is not discriminatory. This can be done as follows.

- Showing that there is in fact no difference in treatment, because for example the comparator is wrongly chosen or the basis of the decision was not the protected ground, or the facts and circumstances of case are different from comparator.
- Proving that there was no causal link between the prohibited ground and the differential treatment.
- By demonstrating that although the differential treatment is related to the prohibited ground, it can be justified under one of the listed exceptions under EU law (such as genuine and determining occupational requirements).
- Proving that the adopted measure, law or practice is appropriate and necessary to achieve the relevant legitimate aim and any disadvantages caused were not disproportionate to the objectives pursued (reasonable and objective justification), pursuant to the European Convention on Human Rights for direct and indirect discrimination and EU law in cases of indirect discrimination.

If the respondent is unable to prove any of these, they will be liable for discrimination.

Accordingly, in the context of algorithmic or AI systems, once a prima facie case is shown, this would require the respondent to disclose relevant information about the system. This information could seek to demonstrate that any choices made were in compliance with objective and non-discriminatory criteria. For the relevance of providing statistical information in rebutting the burden of proof, see 3.6 approach to statistical data.

Table 7. Non-discrimination directives and the shift in burden of proof with examples of the approach taken by the CJEU to drawing inferences from failure to disclose evidence

Directive	Recitals/ article	Protected grounds	Scope	Example case showing the CJEU's approach to drawing inferences from a respondent's failure to disclose relevant or necessary information and/or any other requirements for transparency
2000/43/ EC (Racial Equality Directive)	Recitals 15 and 21 Article 8	Race and ethnic origin – not nationality and without prejudice to treatment arising from legal status of third-country nationals and stateless persons	Employment, vocational training, social protection, education, goods and services, including housing	Meister C-415/10: refusal to provide information (on recruitment criteria, for instance) may give rise to an inference of discrimination
Directive 2000/78/EC	Recital 31 Article 10	Religion or belief, disability, age, sexual orientation	Employment and occupation	Kelly C-104/10: no entitlement to data but failure to disclosure may allow courts to draw inferences
Directive 2006/54/ EC (Recast Gender Equality Directive)	Recital 30 Article 19	Sex (including pregnancy and maternity)	Employment and occupation (including social security schemes)	Danfoss C109/88: where the pay system is opaque, the burden shifts to employer Enderby C-127/92: justifications for pay differentials can be compelled to satisfy the objective justification test Kenny C-427/11: comparators pay data can be required to defeat prima facie case
Directive 2004/113/ EC (Gender, Goods and Services Directive)	Recital 22 Article 9	Sex	Goods and services	Test-Achats C-236/09 See also specific prohibition of use of sex as a factor in calculating insurance and related financial services premiums, consideration of actuarial factors in Article 5
2010/41/EU (Gender Self-Employment Directive)		Sex	Self-employed, spouses or life partners of self-employed	(Pending case) Loredas C-531/23: relating to legality of exemptions from keeping records of working time

Directive	Recitals/ article	Protected grounds	Scope	Example case showing the CJEU's approach to drawing inferences from a respondent's failure to disclose relevant or necessary information and/or any other requirements for transparency
2023/970/E Equal Pay Directive (transposition by June 2026)	Articles 5, 6 and 8-9		Employment	Provides a direct right to transparency. Chapter II provides a right to pay transparency (Article 5), pay setting and progression policy (Article 6), a right to information which must be accessible (Articles 8 and 9) and pay gap reporting (Articles 9 and 10)

Is there objective justification?

To show a difference in treatment is not discriminatory, in a case of indirect discrimination[57] a respondent could argue that there is an objective justification for the practice. This section highlights points to evaluate an objective justification put forward by a respondent.

To justify differential treatment, it must be shown that:

- the algorithmic system has a legitimate aim;
- the algorithmic system is suitable or appropriate to achieve that aim;
- the algorithmic system is necessary to achieve that aim;
- the algorithmic system is proportionate, that is, the algorithmic system is effective at achieving the aim, there are no other means of achieving the legitimate aim that would lead to smaller difference in treatment, and the legitimate aim is important enough to justify the difference in treatment.

Example CJEU case: C-167/97 Seymour-Smith

In circumstances where unfair dismissal claims were only possible after two years of employment and this was shown by statistics to indirectly discriminate against women, the member state responsible for the indirect discriminatory provision, criterion or practice was required to show that the rule reflects a legitimate aim of its social policy, that the aim is unrelated to any discrimination based on sex that it could reasonably consider that the means chosen were suitable for attaining that aim. The court in that case found "mere generalisations concerning the capacity of a specific measure to encourage recruitment are not enough to show

57. Under EU law justification is ordinarily not available in cases of direct discrimination, except for cases related to age/disability and genuine occupation cases.

that the aim of the disputed rule is unrelated to any discrimination based on sex or to provide evidence on the basis of which it could reasonably be considered that the means chosen were suitable for achieving that aim" (paragraphs 76-77). The court also noted that statistics subsequent to the adoption of the measure could be taken into account to provide an indicator of the measure's impact on women and men (paragraph 49).

Aim of the system

Arguing reasonable and objective justification starts with a legitimate aim. Here it can be helpful to note whether the respondent has mentioned different aims throughout different documents; see: 3.4 What is the algorithmic system intended to do?

Take note of different types of aims:

- lower-level aims (predicting fraud, determining if a student is in front of their computer, predicting probability of individual defaulting on loan);
- higher-level aims (minimising government spending on benefits to individuals who do not qualify for these, surveillance for online exams, minimising overarching default rate).

It may also be necessary to consider the domestic legal framework under which the algorithmic system was deployed. See *Glukhin v. Russia*, Application No. 11519/20 (4 July 2023) (below).[58]

Suitability or appropriateness

The respondent should show that the algorithmic system can achieve the aim. This means that when the aim is improved efficiency of a decision-making process, the respondent should show that the algorithm has shortened processing time, decreased capacity required or otherwise increased efficiency. In case of a predictive system showing suitability could mean showing predictive accuracy of the system. Note that suitability claims should match the aim of the system. This should consider both broader and higher-level aims. A system can be inappropriate for not meeting one of the goals:

- lower-level aims, for example if the system is designed to optimise for something different than its intended use case. For example, was it optimised to predict errors, but now used to predict fraud;
- higher-level aims, for example if the aim is to reduce spending on fraudulent benefits, but the algorithm supported inspections are more expensive than the reduction in spending, then this algorithmic system is not suitable for this specific aim.

Necessity

- Aim cannot be achieved (as effectively) without the algorithm:
  - compared to the situation before the algorithm;
  - compared to non-algorithmic approaches.

58. See also *Beghal v. the United Kingdom* for further discussion of the requirements placed on domestic laws for an impugned measure to be regarded as "in accordance with the law".

- Aim cannot be achieved (as effectively) with another algorithmic system:
  - compared to algorithms using other inputs (for example excluding strongest proxies);
  - compared to other development dataset (with less historical inequalities or human biases included).

Example European Court of Human Rights case: *Glukhin v. Russia*, Application No. 11519/20 (4 July 2023)

The European Court of Human Rights considered the use of live facial recognition technology (LFR) to find and locate a protestor on the Russian metro under Article 8 (private life) and Article 10 (freedom of expression). While recognising the importance of modern scientific techniques of investigation and identification (paragraph 85) and having identified a lack of legal basis for the measures taken because of the lack of limitation in law of the use of LFR, the Court also assessed the "necessity in a democratic society" of the measures taken, particularly in light of their potential "chilling effect" on the right to freedom of expression and assembly (Article 10). The Court concluded:

> 90. In the light of all the above considerations, the Court concludes that the use of highly intrusive facial recognition technology in the context of the applicant's exercising his Convention right to freedom of expression is incompatible with the ideals and values of a democratic society governed by the rule of law, which the Convention was designed to maintain and promote. The processing of the applicant's personal data using facial recognition technology in the framework of administrative-offence proceedings – firstly, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him while he was travelling on the Moscow underground – cannot be regarded as "necessary in a democratic society".

Proportionality

In all cases the discrimination caused by the use of the system that the respondent is seeking to justify must be proportionate to the aim sought to be achieved. Overall, this requires a court to balance the seriousness of the harm against the other factors considered in this section.

Questions to consider

- Can the respondent prove they did not discriminate?
- Can the respondent prove they are not to be treated as having been discriminated against?
  - Does the human in the loop sufficiently resolve any residual discrimination?
  - Note that the discrimination could be as a result of human error rather than the algorithmic system.
- Could the respondent argue that the wrong comparator has been chosen?
- Can the respondent show that the complainant is not in a similar or comparable situation to their comparator?

- Is there a sustainable alternative explanation for the difference in treatment other than discrimination?
- What steps have been taken to avoid the discrimination (reasonable adjustments)?
- Where relevant, can the respondent show that the differential treatment is not based on the protected ground but other objective differences?
- Are those objective differences explicitly covered by the non-discrimination directives?
- Does the provision or practice in question pursue a legitimate goal?
- Review section 3.4 on what the AI system intends to do and how it does it – were the means chosen suitable?
- Are the means employed to achieve the goal suitable, necessary and proportionate to the aim that is seeking to be achieved?

Step 4
Remedies

Step 4 details the various remedies and courses of action available to equality bodies. Powers and mandates are likely to differ significantly by member state and this step has therefore been compiled specifically to look at the inter-relationship between the standards directives, which must be transposed by 19 June 2026, the AI Act, the GDPR and any other relevant Union law.

It will usually be necessary to consider more than one remedy depending on the issue or the case.

Figure 5. Step 4 – Remedies

STEP 4	Remedies	
4.1	Remedies for all algorithmic systems	**POSSIBLE ACTIONS** • Equality bodies' remedial powers • Initial assistance • Lodging a complaint to an MSA • GDPR remedies • Alternative dispute resolution • Litigation • Equality data collection and reporting
4.2	Additional remedies for high-risk AI systems	**POSSIBLE ACTIONS** • MSA response to serious incident • MSA investigation of serious risk to fundamental rights • Wrong AI classification • Compliant AI system posing a risk to fundamental rights
4.3	Serious risk to fundamental rights but AI is not high risk or a prohibited system	**POSSIBLE ACTIONS** • Seeking amendment to the AI Act • Seeking additions to Annex III of the AI Act

Section 4.1 deals with remedies for all algorithmic systems.

Section 4.2 provides additional remedies for high-risk systems.

Section 4.3 outlines what an EB should do in a case where a system or use case presents a risk to fundamental rights but is not classified as high-risk under the AI Act, including actions that an MSA may take that would or could require EB involvement.

Under the non-discrimination directives and standards directives, EBs are given broad powers to carry out activities to prevent discrimination and to promote equal treatment. These powers include awareness raising (Article 5), providing assistance to victims (Article 6), alternative dispute resolution (Article 7) conducting inquiries into a breach of the principle of equal treatment (Article 8), giving opinions and decisions, including a right to establish facts (Article 9) and acting in court proceedings, including a right to submit observations (Article 10).

Where discrimination has been identified in an algorithmic system, consideration should be given to the exercise of these powers to ensure:

- the respondent stops using the AI system in a discriminatory way, or, if this is not possible, the respondent stops using the AI system altogether;
- awareness of the algorithmic discrimination is appropriately communicated to affected groups and bodies;
- advice and assistance, including in respect of alternative dispute resolution (ADR) and litigation, is provided to individual victims;
- remedial action is taken, including through the provision of training, advice and support;
- a public debate on the issue of discrimination in algorithmic systems is undertaken and positive action and equality mainstreaming is promoted among public and private entities;
- communication with relevant stakeholders, including the social partners, and promotion of the exchange of good practices.

In carrying out such activities, equality bodies can take into consideration specific situations of disadvantage resulting from intersectional discrimination, which is understood as discrimination based on a combination of grounds protected under the non-discrimination directives.

EBs must take into consideration appropriate communication tools and formats for each target group. They shall focus in particular on groups whose access to information can be hindered, for example because of their precarious economic status, age, disability, level of literacy, nationality or residence status, or because of their lack of access to online tools.

Key resources

- "Strategic litigation handbook" (Equinet 2017)
- "How to use the Artificial Intelligence Act to investigate AI bias and discrimination: a guide for equality bodies" (Mittelstadt 2024)

4.1. Remedies for all algorithmic systems

Following the process at steps 2 and 3 should have helped to identify whether discrimination exists and what the cause of the discrimination may have been. EBs should use the information gathered during those phases to suggest remedial actions and adopt a plan for the removal or modification of contested practices, algorithms or systems. For example, the EB may have determined that the choice of fairness metrics was inappropriate for the use case or that the data were insufficiently representative.

Where the EB decides that the risk of discrimination or the discrimination identified is unlawful but can be remedied, consider action to achieve:

- the prohibition of the use of the system until the discrimination has been remedied;
- any remedial steps that should be taken.

Where the EB decides that the risk of discrimination is unlawful and cannot be remedied, action to achieve one of the following results should be considered:

- the prohibition of the use of the algorithmic system altogether;
- the prohibition of the use of the algorithmic system in a particular sector;
- the prohibition of the use of the algorithmic system for a particular purpose.

Such action could be achieved through the equality bodies exercising their own powers in respect of giving opinions, making recommendations and consultation, taken in conjunction with the MSA, either under the GPSR or the AI Act or through the courts.

4.1.1. Equality bodies' remedial powers

Equality bodies should first consider their remedial powers under national law, as above. These could include any or all of the remedies that are due to be formalised by the standards directives such as giving an opinion or recommendation or requiring a consultation or testing.

If the standards directives are transposed into national laws, EBs should be granted remedial powers. These will include Article 9 (issuing a binding or non-binding opinion, dependent on national context) and Article 15, consultation and recommendation powers.

Equality bodies should also be empowered to provide and document their assessment of the case, including establishing the facts and a reasoned conclusion on the existence of discrimination. In the case of algorithmic discrimination this could include through working in co-operation with the MSA.

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. EBs may need expert assistance in providing specific measures and if they do not have the expertise they may wish to consult with the

MSA. Appropriate mechanisms for the follow-up to non-binding opinions should be established, such as feedback obligations, and for the enforcement of binding decisions.

Consultations can be used to identify the existence of problems, to test the social and discriminatory impact of systems on affected or potentially affected communities and to gather evidence.

More generally, recommendations and consultations could be directed towards ensuring that the problems do not arise in future by, for example, recommending:

- data protection and equality impact assessments;
- community consultation and a community-led FRIA;
- use of sandboxes and real-world testing.

Further reading

- Crowley (2023), "Informing the policy agenda: equality bodies making recommendations"

4.1.2. Provide initial assistance to a victim

Article 6 of the standards directives provides that equality bodies shall provide initial assistance by informing victims of the following:

- the legal framework relating to discrimination and algorithmic systems, including advice targeted at 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, including;
  - under non-discrimination law;
  - under the AI Act – see for example the right to lodge a complaint with the MSA (Article 85 of the AI Act) and the right to an explanation (Article 86 of the AI Act);
  - under data-protection law – for example, lodging a complaint with the DPA (Article 77 of the GDPR) and the right to make a subject access request (Article 15 of the GDPR);[59]
- the applicable confidentiality rules and the protection of personal data (for example, the EBs' data-protection policies and, where relevant, any conflict between the EB obtaining evidence while exercising one part of their mandate and being able to provide that evidence for use in court by an individual);
- the possibility of obtaining psychological or other types of relevant support from other bodies or organisations.

59. A right to an explanation exists under both the GDPR (Articles 15 and 22) and the AI Act (Article 86). In step 2 and Appendices A and B, further explanation and templates for making the request are provided.

Equality bodies are to inform the complainant, within a reasonable time, about whether the complaint will be closed or whether there are grounds to pursue it further.

After providing initial assistance, the remedies available to an individual complainant may include:

- lodging a complaint with the MSA (Article 85 of the AI Act);
- considering alternative dispute resolution;
- litigating the discrimination in the national courts.

Any decision about the best course of action to take must be taken in conjunction with the affected person or group. If the EB does not have capacity, competence (such as data-protection claims) or resources to pursue the course of action sought by the affected person, the case should be referred to another competent legal service provider.

4.1.3. Assisting a legal or natural person to lodge a complaint with the MSA

Where the investigation under step 3 has identified compliance issues under the AI Act, a legal or natural person has the right to lodge a complaint with the MSA (Article 85 of EU AI Act). This means that the right extends to a body with a legal personality such as a corporation or organisation. The EB can assist the person making the complaint with evidence identified in step 3.

This right is without prejudice to and in addition to existing rights and remedies under EU and domestic law (Recital 170). It is not restricted to high-risk AI systems.

Any such complaint is "taken into account" for the purpose of conducting market surveillance activities under Regulation (EU) 2019/1020 on market surveillance and compliance of products. Time limits are most likely to be set out in national legislation (see Article 11 of Regulation (EU) 2019/1020).

Any AI system that is not high risk would fall under the General Product Safety Regulation (EU) 2023/988, Regulation (EU) 2023/988 and MSA Regulation (EU) 2019/1020.

> It is important that AI systems related to products that are not high-risk in accordance with this regulation and thus are not required to comply with the requirements set out for high-risk AI systems are nevertheless safe when placed on the market or put into service. To contribute to this objective, Regulation (EU) 2023/988 of the European Parliament and of the Council (53) would apply as a safety net. (Recital 166 of the AI Act)

The right to make a complaint is without prejudice to any other administrative or judicial remedies and therefore is a step that should be taken in conjunction with any other applicable remedies. Taken alone, this is unlikely to be the best remedy for an individual not least because there is no provision as to damages. However, it is an important accompanying measure and, as the MSA has very wide-ranging powers and remedies under Regulation (EU) 2019/1020, it will be worth considering in an appropriate case. A complaint to the MSA should trigger a more structural

investigation by the MSA and a broader remedy impacting the wider cohort of affected individuals than an individual discrimination claim. The MSA has extensive powers under both the AI Act and Regulation (EU)2019/1020 and can undertake documentary, physical and laboratory checks (see section 4.2).

If the complaint is successful, the MSA can require corrective action to be taken by an economic operator providing the action is appropriate and proportionate. If the corrective action is not taken or unsuccessful the MSA can prohibit or restrict the making available of a product on the market or order that the product is withdrawn or recalled. For products presenting a risk that have an impact beyond the MSA's own member state the MSA is required to immediately notify the European Commission and the other EU Member States of the measures taken. Regulation (EU)2019/1020 makes extensive provision for cross-border co-operation by different member states.

4.1.4. Remedies for a data subject under the GDPR or national data-protection regimes

Under the GDPR an individual data subject (a natural person) has the following data rights in addition to the right to an explanation.

- To object to automated processing of their personal data (Article 21).
- The tight to rectification of inaccurate personal data concerning her or him and to have incomplete personal data completed by means of providing a supplementary statement (Article 16).
- The right to erasure of their personal data without undue delay where one of the following applies:
  - consent is withdrawn and no other legal basis applies;
  - they have exercised their right to object under Article 21(1);
  - the personal data have been unlawfully processed.

These may be of relevance where an algorithmic system has resulted in discrimination. Any action taken may require the involvement of a data-protection expert or the data-protection authority.

Where states have adopted data-protection regimes in addition to the GDPR or in states not subject to the GDPR, it will be important to consider any national data-protection laws.

4.1.5. Offering alternative dispute resolution in accordance with law

Under the standards directives, Article 7, EBs shall be able to offer the parties the possibility of seeking an alternative resolution to their dispute. That process may be led by the equality body itself or by another competent entity in accordance with national law and practice, in which case the equality body may formulate observations to that entity. Such alternative dispute resolution may take different forms, such as mediation or conciliation, in accordance with national law and practice. The absence of a resolution shall not preclude the parties from exercising their right to act in court proceedings. Member states shall ensure that there is a sufficient

limitation period to guarantee that the parties to a dispute have access to court, for example by suspending the limitation period while the parties engage in an alternative dispute resolution process.

4.1.6. Non-discrimination and human rights litigation

Equality bodies should have the right to act in court proceedings in civil and administrative matters, including the right to submit observations relating to the non-discrimination directives in accordance with national law and practice. This will vary by individual state.

Under Article 10 of the standards directives, the right of the equality body to act in court proceedings shall also 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;
- the right to initiate court proceedings in its own name, to defend the public interest.

This will include enforcement decisions in respect of binding opinions issued by the EB under Article 9 (see below). When considering whether to bring strategic litigation, equality bodies are referred to the detailed considerations in Equinet's "Strategic litigation handbook" (Equinet 2017: 17).

There is likely to be significant opportunity to engage in strategic litigation in respect of AI systems because both the technology and the law is relatively new. Strategic litigation will not necessarily be the best approach in every case. For example, it may take too long to obtain a result for an affected person, the information required to bring a successful claim may be missing, it may be more effective to enter into testing and negotiation processes and various other factors that will need to be considered on a case-by-case basis.

4.1.7. Data collection, access to equality data and reporting

Access to equality data is key to establish discrimination by AI and ADM systems. Equality bodies can leverage the new powers to collect data on the occurrence of algorithmic discrimination more broadly. Recommendations on the types of information to record have been made throughout this methodology, which may assist EBs in compiling equality data relating to algorithmic systems. Collected statistics might be helpful when establishing a case of prima facie discrimination in court, for instance. If the EB notes that there are frequent requests for assistance in relation to a particular sector or use case of an algorithmic system, it may require further investigation or prioritisation.

The collection of equality data is insufficient in many countries, not least because it is often legally restricted because EBs are often unable to process sensitive categories of personal data for bias measurement and mitigation purposes under

Article 9(2)(g) of the GDPR and Article 10(5) of the AI Act. EBs could recommend reforming data-collection rules and practices to improve existing knowledge on algorithmic discrimination (see Council of Europe 2025b).

Identifying structural issues and reporting on these on an annual basis

Data collection should enable the EB to identify and report on structural inequality in algorithmic systems. Where the EB uses a database to record details of cases and advice given, a new category of case should be added to enable the EB to track the actual or suspected discriminatory use of AI systems. In the longer term this methodology could be used to design specific fields for the database to enable the collection and analysis of data on these cases.

For inspiration, throughout step 3 of the methodology, indicators of the type of information that could be recorded in a database are identified at the end of each section and a suggested worksheet provided in Appendix K.

Structural issues may include:

- evidence of discrimination arising in a particular type of algorithmic system or technology;
- evidence of discrimination arising when algorithmic systems are used in particular sectors;
- evidence of suspicion that discrimination is arising in a sector or type of algorithmic system;
- evidence of groups being disproportionately affected by the adoption of algorithmic systems across multiple sectors;
- AI systems or use cases that should, but are not currently:
  - prohibited;
  - designated as high risk;
  - general-purpose models with systemic risk;
  - listed under any of these categories but nevertheless present an unacceptable risk of discrimination;
- systemic failures to comply with relevant parts of the AI Act relevant to discrimination, such as inadequate bias or fairness testing and inadequate data-collection practices.

4.2. Additional remedies for high-risk AI systems

4.2.1. Actions taken by the MSA in co-operation with the EB

In addition to the powers given to EBs under Article 77 of the AI Act in their own right, the MSA has obligations to work with an EB as an Article 77 authority when dealing with a "serious incident" (Article 73 of the AI Act), when AI systems present risks (Article 79 of the AI Act) and when investigating a compliant system that poses a risk to fundamental rights (Article 82 of the AI Act). An MSA may also

need to consult with an EB when considering an AI system wrongly classified by a provider as non-high risk (Article 80 of the AI Act). These processes are discussed in more detail below.

An EB may wish to refer a system to the MSA with evidence obtained under this methodology to report a serious incident, to conduct testing, to carry out an evaluation or to exercise powers under either the AI Act or MSA Regulation to require corrective action, suspension or withdrawal of the product from the market or other actions.

MSA responding to a notification of a serious incident (Article 73 of the AI Act)

The MSA has significant powers and responsibilities under Regulation (EU) 2019/1020 when dealing with a serious incident.

The MSA must inform the Article 77 body when it is notified by a provider of a serious incident (Article 73(3) of the AI Act). A serious incident is defined as an incident or malfunctioning of an AI system that for example directly or indirectly leads to the infringement of obligations under Union law intended to protect fundamental rights, including the right to non-discrimination (Article 3(49)(c) of the AI Act). Guidance will be issued by the Commission in due course.

In such cases, consider the following.

- Did the serious incident include a risk of discrimination?
  - If yes, should the affected persons be entitled to a remedy?
  - If yes, consider the most effective remedy (consider for example ADR, litigation or an inquiry).
  - If the affected persons are entitled to monetary compensation, ensure the remedy chosen does not preclude this. Take care to respect any relevant time limits.
- Is this likely to have additional and ongoing impacts for other individuals? For example, is the system used by banks to determine creditworthiness?
- Take immediate steps to raise awareness of the issue (Article 5 of the standards directives or via the MSA relying on product safety regulations).
- Consider whether the AI system interacts with other devices/software and raise awareness in respect of any similarly affected system.

Record the type of technology and sector in which the issue arose for use in EB reporting and equality data analysis.

The corrective action required will depend on the problems identified. However, the information, steps and approaches outlined in step 3 should assist the EB in identifying potential remedies.

MSA investigation under Article 79(3) of the AI Act: product presenting a serious risk to fundamental rights, including discrimination

Where the MSA (alone or in co-operation with an Article 77 body) finds that the AI system does not comply with the requirements laid down in the regulation, it shall require, without undue delay:

- appropriate corrective actions to bring the AI system into compliance;
- informing the Commission and other member states about the results of the evaluation and the action the provider is to take;
- withdrawing the AI system from the market (Article 79(5) of the AI Act);
- a recall within a period the MSA may prescribe, within 15 working days or as provided for in Union legislation (this will require a check on relevant legislation at this point);
- that the MSA informs the relevant notified body.

MSA procedure for dealing with AI systems classified by the provider as non-high risk in application of Annex III (Articles 6(4) and 80 of the AI Act)

If considering whether an AI system has been wrongly classified under the self-assessment opt-out procedure (Article 6(4) and the procedure in Article 80), the MSA must carry out an evaluation to determine whether Article 6(3) applies.

In this case it is possible that there is no fundamental risk assessment relevant and no consideration of discrimination. The issues being considered are whether the AI system:

- performs a narrow procedural task;
- improves the result of previously completed human activity;
- detects decision-making patterns or deviations from prior decision-making patterns;
- fulfils a preparatory task to an assessment.

However, it is possible that even these systems may pose risks to fundamental rights and non-discrimination. EBs can refer a system to the MSA to consider whether the AI system has been wrongly classified and provide the evidence on which they base that referral.

High-risk AI Act-compliant systems that pose a risk to the health or safety of persons, to fundamental rights or to other aspects of public-interest protection (Article 82 of the AI Act)

The MSA has powers in respect of a compliant system that presents a risk under Article 82 of the AI Act. Before taking these steps the MSA must have both:

- performed an evaluation under Article 79 of the AI Act;
- consulted the relevant Article 77 body.

The operator will be required to take "all appropriate measures to ensure that the AI system concerned, when placed on the market or put into service, no longer presents that risk".

Although not explicitly stated in the AI Act, the EB should be consulted at least when the MSA seeks to determine whether the risks to fundamental rights and/or equality have been successfully removed.

4.3. What to do when a system or use case poses a risk to fundamental rights but is not designated "high risk" or "prohibited"

This situation can arise when:

- a provider has self-assessed their algorithmic system as not an AI system according to the definition in Article 3 and is therefore beyond the scope of the act altogether;
- an algorithmic system that should be prohibited because of the risk it poses is not included in the list of prohibited systems in Article 5 of the AI Act;
- an algorithmic system that should be classed as high risk is not included in Annex III of the AI Act because either the sector or the use case is not included;
- a provider has applied the derogation in Article 6(3) to an AI system that would otherwise be classified as high risk.

Note: deployers have an obligation to monitor their high-risk systems and notify the MSA where they have reason to consider that the use of the AI system in accordance with the instructions may result in that system presenting a serious risk to fundamental rights (Article 26 in conjunction with Article 79 of the AI Act).

Note: if an AI system is a "product presenting a risk" as defined in Article 3 of point 19 of Regulation (EU) 2019/1020, the MSA is required to evaluate the system and, where risks to fundamental rights are identified, to co-operate with the relevant Article 77 authorities. Remedies for such a product under the AI Act are limited to compliant high-risk systems. Alternative remedies under the MSA Regulation and the General Product Safety Legislation, contract or tort law, non-discrimination legislation or human rights legislation may be available.

For individuals or affected groups, the fact that a system is not designated high risk or prohibited does not mean it cannot cause discrimination or result in or be used in a manner that breaches fundamental rights. EBs have all of the usual remedies for discrimination available to them under the non-discrimination directives and national law.

4.3.1. Seeking amendment to the AI Act

If the EB finds an AI practice to fundamentally contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights as enshrined in the Charter, representations should be made to the MSA and

the Commission to amend the AI Act. The AI Act sets out a procedure by which amendments can be made to the AI Act in various different circumstances.

Article 112 requires the Commission to assess the need for amendment of the list in Annex III (high risk) and Article 5 (prohibited systems) on a yearly basis and present the findings of their assessment to the European Parliament. It is therefore important to raise any concerns about AI systems that should be prohibited or AI systems that present high risk in areas or use cases missing from Annex III to the Commission under the procedures set out in the AI Act.

For the first five years of the EU AI Act (to 1 August 2029 and automatically extended thereafter unless opposed), the Commission has the power to adopt delegated acts in the following circumstances.[60]

Article 6(6)	To add or modify or delete conditions for self-assessing as non-high risk
Article 7	To amend Annex III by adding or modifying use cases (but not areas) and removing systems from the list
Article 11(3)	To amend technical documentation required by Annex IV (particularly in light of technical progress)
Article 47(5)	To update the content of the EU declaration of conformity in Annex V

Although the Commission does not have the power to adopt a delegated act to amend area headings in Annex III, it is required to assess the need for any such amendments by 2 August 2028 to existing area headings or adding new area headings in Annex III, amendments to lists of systems requiring additional transparency and amendments to enhance the effectiveness of the supervision/governance system. The Commission is then required to submit its assessment to the European Parliament and Council.

The AI Office will be developing a methodology for the evaluation of these criteria.

4.3.2. System used in a high-risk sector with a use case not registered in Annex III of the AI Act

If a particular "use case" is not in Annex III of the AI Act, the Commission has the power under section 7 to amend by adding or modifying use cases where:

- the system is intended to be used in an Annex III area; and
- the adverse impact on fundamental rights (including discrimination) is equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk systems already in Annex III.

Therefore, if a use case meeting these criteria is found by the EB to have an adverse impact on fundamental rights but is not in the lists in Annex III, consider reporting the use case to the Commission for it to be added to the list under Article 7 of the AI Act.

60. The Commission has delegated powers in respect of GPAI, but this is out of scope.

The factors to be considered by the Commission are set out in Article 7(2) of the AI Act and should be addressed when making a report:

- the intended purpose of the AI system;
- the extent to which an AI system has been used or is likely to be used;
- the nature and amount of the data processed and used by the AI system, in particular whether special categories of personal data are processed;
- the extent to which the AI system acts autonomously and the possibility for a human to override a decision or recommendations that may lead to potential harm;
- the extent to which the use of an AI system has already caused harm to health and safety, has had an adverse impact on fundamental rights or has given rise to significant concerns in relation to the likelihood of such harm or adverse impact, as demonstrated, for example, by reports or documented allegations submitted to national competent authorities or by other reports, as appropriate;
- the potential extent of such harm or such adverse impact, in particular in terms of its intensity and its ability to affect multiple persons or to disproportionately affect a particular group of persons;
- the extent to which persons who are potentially harmed or suffer an adverse impact are dependent on the outcome produced with an AI system, in particular because for practical or legal reasons it is not reasonably possible to opt out from that outcome;
- the extent to which there is an imbalance of power, or 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;
- the extent to which the outcome produced involving an AI system is easily corrigible or reversible, taking into account the technical solutions available to correct or reverse it, whereby outcomes having an adverse impact on health, safety or fundamental rights shall not be considered to be easily corrigible or reversible;
- the magnitude and likelihood of benefit of the deployment of the AI system for individuals, groups, or society at large, including possible improvements in product safety;
- the extent to which existing Union law provides for:
  - effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages;
  - effective measures to prevent or substantially minimise those risks.

References

Literature

Adams-Prassl J., Binns R. and Kelly-Lyth A. (2022), "Directly discriminatory algorithms", *The Modern Law Review*, 86(1), pp. 144-175. Available at: https://doi.org/10.1111/1468-2230.12759 (accessed 17 October 25).

Ahmed M. (2020), "UK passport photo checker shows bias against dark-skinned women", BBC News. Available at: www.bbc.co.uk/news/technology-54349538.amp (accessed 13 October 2025).

Allen R. and Masters D. (2019), "Artificial intelligence: the right to protection from discrimination caused by algorithms, machine learning and automated decision-making", *Journal of the Academy of European Law*. Available at: DOI: 10.1007/s12027-019-00582-w (accessed 19 June 2025).

Allen R. and Masters D. (2020), "Regulating for an equal AI: a new role for equality bodies", Equinet. Available at: https://equineteurope.org/publications/regulating-for-an-equal-ai-a-new-role-for-equality-bodies/?__cf_chl_f_tk=3KwuXAuyY1rQSy6K-Kjf6WQaiw8Fzq0tVZpxUk2K39Qs-1782916549-1.0.1.1-nTAmM4flODMeHv8UOjuY-4hye5_yL66T80oAESRgxorA (accessed 20 October 2025).

Algorithm Audit (2024a), "Preventing prejudice". Available at: https://algorithmaudit.eu/algoprudence/cases/aa202401_preventing-prejudice/ (accessed 11 October 2025).

Algorithm Audit (2024b), "Addendum to preventing prejudice". Available at: https://algorithmaudit.eu/algoprudence/cases/aa202402_preventing-prejudice_addendum/ (accessed 1 October 2025)

Algorithm Watch (2022), "Automated decision-making systems and discrimination: a guidebook for anti-discrimination counselling". Available at: https://algorithmwatch.org/en/autocheck/ (accessed 29 September 2025).

Amnesty International (2021), "Xenophobic machines: discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal". Available at: https://www.amnesty.org/en/documents/eur35/4686/2021/en/ (accessed 13 October 2025).

Article 29 Data Protection Working Party (2017a), "Guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679". Available at: https://ec.europa.eu/newsroom/article29/items/611236/en (accessed 8 November 2025).

Article 29 Data Protection Working Party (2017b), "Opinion on some key issues of the law enforcement directive (EU 2016/680) – wp258", European Commission. Available at: https://ec.europa.eu/newsroom/article29/items/610178/en (accessed 17 October 2025).

Article 29 Data Protection Working Party (2018a), "Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01, 17/EN)", European Commission. Available at: https://ec.europa.eu/newsroom/article29/items/612053/en (accessed 10 November 2025).

Article 29 Data Protection Working Party (2018b), "Guidelines on transparency under Regulation 2016/679 (WP260, 17/EN)", European Commission. Available at: www.edpb.europa.eu/our-work-tools/our-documents/article-29-working-party-guidelines-transparency-under-regulation_en (accessed 10 November 2025).

Autoriteit Persoonsgegevens (2024), Final recommendation on supervision of AI: sector and centrally coordinated. Available at: www.autoriteitpersoonsgegevens.nl/en/current/final-recommendation-on-supervision-of-ai-sector-and-centrally-coordinated (accessed 1 October 2025).

Barocas S., Hardt M. and Narayanan A. (2023), *Fairness and machine learning: limitations and opportunities*, MIT Press, Cambridge, MA.

Barros Vale S. and Zanfir-Fortuna G. (2022), "Automated decision-making under the GDPR: practical cases from courts and data protection authorities", Future of Privacy Forum. Available at: https://fpf.org/blog/fpf-report-automated-decision-making-under-the-gdpr-a-comprehensive-case-law-analysis/ (accessed 1 October 2025).

Big Brother Watch (2025), "Suspicion by design". Available at: https://bigbrotherwatch.org.uk/campaigns/welfare-data-watch/ (accessed 10 November 2025).

Bird K. A., Castleman B. L. and Song Y. (2024), "Are algorithms biased in education? Exploring racial bias in predicting community college student success", *Journal of Policy Analysis and Management*, Vol. 44 (2). Available at: https://onlinelibrary.wiley.com/doi/full/10.1002/pam.22569 (accessed 17 October 2025).

Boscarol F. (2022), "Costly birthplace: discriminating insurance practice", Algorithm Watch. Available at: https://algorithmwatch.org/en/discriminating-insurance/ (accessed 13 October 2025).

Ceross A. (2025), *Understanding artificial intelligence: concepts, limitations, and risks*, Equinet. Available at: https://equineteurope.org/publications/understanding-artificial-intelligence-concepts-limitations-and-risks/ (accessed 1 October 2025).

College voor de Rechten van de Mens (2023), "Oordeelnummer 2023-111". Available at: https://oordelen.mensenrechten.nl/oordeel/2023-111#kop (accessed 14 October 2025).

College voor de Rechten van de Mens (CRM) (2025), "Toetsingskader risicoprofilering". Available at: www.mensenrechten.nl/actueel/nieuws/2025/01/28/nieuw-toetsingskader-tegen-discriminatie-door-risicoprofilering (accessed 29 September 2025).

Council of Europe and European Union Agency for Fundamental Rights (2018), *Handbook on European non-discrimination law*, 2nd edn, Publications Office of the European Union. ISBN: 978-92-871-9851-8.

Council of Europe (2025a), "Legal protection against algorithmic discrimination in Europe: current frameworks and remaining gaps". Available at: https://rm.coe.int/legal-protection-eng-web/48802a38d7 (accessed 4 June 2026).

Council of Europe (2025b), "European policy guidelines on AI and algorithm-driven discrimination for equality bodies and other national human rights structures". Available at: https://rm.coe.int/policy-guidelines-eng-web/48802a38a5 (accessed 4 June 2026).

Council of Europe (2025c), "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)". Available at: https://rm.coe.int/prems-002726-gbr-2006-huderia-texte-web-a4/48802ba7b1 (accessed 19 June 2025).

Council of Europe (2026), "Model 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)". Available at: https://rm.coe.int/prems-002726-gbr-2006-huderia-texte-web-a4/48802ba7b1 (accessed 19 June 2025).

Crenshaw K. (1991), "Mapping the margins: intersectionality, identity politics, and violence against women of color", *Stanford Law Review*, 43(6), pp. 1241-1299. Available at: www.jstor.org/stable/1229039 (accessed 1 October 2025).

Crenshaw K. (2015), "Why intersectionality can't wait", *The Washington Post*. Available at: www.washingtonpost.com/news/in-theory/wp/2015/09/24/why-intersectionality-cant-wait/ (accessed 1 October 2025).

Crowley N. (2023), *Informing the policy agenda: equality bodies making recommendations*, Equinet. Available at: https://equineteurope.org/informing-the-policy-agenda-equality-bodies-making-recommendations/ (accessed 1 October 2025).

Dastin J. (2018), "Amazon scraps secret AI recruiting tool that showed bias against women", *Reuters*. Available at: www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-airecruiting-tool that-showed-bias-against-women-idUSKCN1MK08G (accessed 10 November 2025).

Dimitrova D. and De Hert P. (2024), "The LED's right of access to one's data: loopholes on proper access, legality review and data protection authority accountability", *New Journal of European Criminal Law*, 15(1), pp. 12-32. Available at: https://doi.org/10.1177/20322844231214484 (accessed 17 October 2025).

Equinet (2017), *Strategic litigation handbook*. Available at: https://equineteurope.org/publications/strategic-litigation-handbook/ (accessed 29 September 2025).

Equinet (2022), *Equality Bodies working on cases without an identifiable victim: Actio popularis.* Available at: https://equineteurope.org/equality-bodies-working-on-cases-without-an-identifiable-victim-actio-popularis/ (accessed 29 September 2025).

Equinet (2025), Webinar series: equality by design, deliberation and oversight. Available at: https://equineteurope.org/webinar-series-equality-by-design-empowering-equality-bodies-and-civil-society-on-the-interface-between-technical-standards-and-legal-requirements/ (accessed 1 October 2025).

Erdogan I. (2023), "Transparency in the face of new technologies: information rights under the law enforcement directive", *Jean Monnet Network on EU Law Enforcement Working Paper Series*. Available at: https://jmn-eulen.nl/papers/events-on-ai/ (accessed 17 October 2025).

Erdogan I. (2024), "Diving into the iceberg: establishing transparency in AI for law enforcement", *European Papers*, 9(3), pp. 956-977. Available at: www.europeanpapers.eu/e-journal/diving-into-iceberg-establishing-transparency-ai-for-law-enforcement (accessed 17 October 2025).

Eticas Foundation (2024), Automating (in)justice? An adversarial audit of riscanvi. Available at: https://www.eticasfoundation.org/automating-injustice-an-adversarial-audit-of-riscanvi/ (accessed 13 October 2025).

European Center for Not-for-Profit Law and Danish Institute for Human Rights (2025), A guide to fundamental rights impact assessments (FRIA). Available at: https://ecnl.org/publications/guide-fundamental-rights-impact-assessments-fria (accessed 31 April 2026).

European Commission (2019), *Equality law review: European network of legal experts in gender equality and non-discrimination*, Publications Office of the European Union. Available at: https://op.europa.eu/s/AiAN (accessed 19 June 2026).

European Commission (2021), *Guidelines on improving the collection and use of equality data*, Publications Office of the European Union. Available at: https://data.europa.eu/doi/10.2838/9725 (accessed 17 October 2025).

European Commission (2025), "Supporting the implementation of the AI ACT with clear guidelines". Available at: https://digital-strategy.ec.europa.eu/en/news/supporting-implementation-ai-act-clear-guidelines (accessed 1 May 2025).

European Court of Human Rights (2025), "Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention". Available at: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_14_art_1_protocol_12_eng (accessed 10 November 2025).

Farkas L. and O'Farrell O. (2015), *Reversing the burden of proof: practical dilemmas at the European and national level*, Publications Office of the European Union. Available at: https://op.europa.eu/en/publication-detail/-/publication/a763ee82-b93c-4df9-ab8c-626a660c9da8/language-en (accessed 10 November 2025).

FRA (2018), Handbook on European non-discrimination law – 2018 edition. Available at: https://fra.europa.eu/en/publication/2018/handbook-european-non-discrimination-law-2018-edition# (accessed 1 July 2026).

FRA (2025), "Assessing high-risk artificial intelligence: fundamental rights risks". Available at: Assessing High-risk Artificial Intelligence: Fundamental Rights Risks – European Union Agency for Fundamental Rights (accessed 4 June 2026).

Fredman S. (2016), *Intersectional discrimination in EU gender equality and non-discrimination law*, European Equality Law Network, Publications Office of the European Union. Available at: https://op.europa.eu/en/publication-detail/-/publication/d73a9221-b7c3-40f6-8414-8a48a2157a2f/language-en (accessed 17 October 2025).

González Fuster G. (2020), "Artificial intelligence and law enforcement. Impact on fundamental rights". European Parliament. Available at: https://op.europa.eu/s/AiyD (accessed 12 November 2025).

Howard E. (2024), "Intersectional discrimination and EU law: time to revisit Parris", *Sage Journals*. Available at: https://journals.sagepub.com/doi/10.1177/13582291241285336 (accessed 1 May 2026).

Ilieva S. (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 29 September 2025).

Information Commissioner's Office and Equality and Human Rights Commission (2023), Memorandum of understanding between the Information Commissioner and the Equality and Human Rights Commission. Available at: https://ico.org.uk/about-the-ico/our-information/working-with-other-bodies/ (accessed 1 October 2025).

JuLIA Project (2024), *Handbook: artificial intelligence, judicial decision-making and fundamental rights*, JuLIA 101046631, European Commission (DG JUST – JUST-2021-JTRA). Available at: https://www.julia-project.eu/resources accessed 1 October 2025).

Lighthouse Reports (2025), "How we investigated Amsterdam's attempt to build a 'fair' fraud detection model". Available at: www.lighthousereports.com/methodology/amsterdam-fairness/ (accessed 19 June 2026).

Lighthouse Reports (2024), "How we investigated Sweden's suspicion machine". Available at: www.lighthousereports.com/methodology/sweden-ai-methodology/ (accessed 20 October 2025).

Lighthouse Reports (2023), "How we investigated France's mass profiling machine". Available at www.lighthousereports.com/methodology/how-we-investigated-frances-mass-profiling-machine/ (accessed 19 October 2025).

Mahieu R. L., Asghari H. and van Eeten M. (2018), "Collectively exercising the right of access: individual effort, societal effect", *Internet Policy Review*, 7(3). Available at: https://doi.org/10.14763/2018.3.927 (accessed 10 November 2025).

Makkonen T. (2007), *Measuring discrimination: data collection and EU equality law*, Publications Office of the European Union. Available at: https://op.europa.eu/en/publication-detail/-/publication/7d20295d-212c-4acb-bd9f-6f67f4c7ce67 (accessed 10 November 2025).

Makkonen T. (2016), *European handbook on equality data: 2016 revision*, Publications Office of the European Union. Available at: https://ec.europa.eu/newsroom/just/document.cfm%3Faction%3Ddisplay%26doc_id%3D43205&ved=2ahUKEwiysrmm-eeQAxXiwAIHHUBOH9MQFnoECBgQAQ&usg=AOvVaw1aG86yvlJ51QDEGbA_FR7L (accessed 10 November 2025).

Mantelero A. (2024), "The fundamental rights impact assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template", *Computer Law & Security Review*, 54, p. 106020. Available at: www.sciencedirect.com/science/article/pii/S0267364924000864 (accessed 10 November 2025).

Mittelstadt B. (2024), "How to use the Artificial Intelligence Act to investigate AI bias and discrimination: a guide for equality bodies", Equinet. 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 1 October 2025).

Mittelstadt B., Wachter S. and Russell C. (2023), "The unfairness of fair machine learning: levelling down and strict egalitarianism by default". Available at: https://arxiv.org/abs/2302.02404 (accessed 17 July 2026).

Norwegian Data Protection Authority (2023), "Evaluation of the Norwegian Data Protection Authority's regulatory sandbox for artificial intelligence". Available at: https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/the-sandbox-has-been-evaluated/ (accessed 17 October 2025).

Parviainen H. (2024), "Challenges of direct discrimination in algorithmic recruitment: insuperable or not?*", *International Journal of Comparative Labour Law and Industrial Relations*, 40, 4 December 2024, pp. 437-466. Available at: https://doi.org/10.54648/ijcl2024017 (accessed 17 October 2025).

Purificato I. (2021), "Behind the scenes of Deliveroo's algorithm: in the blindness of 'frank' its discriminatory potential", *Italian Labour Law e-Journal*, 14(1), pp. 169-194. Available at: doi:10.6092/issn.1561-8048/12990 (accessed 22 June 2026).

PWC (2024), *Onderzoek misbruik uitwonendenbeurs*. Available at: www.tweedekamer.nl/kamerstukken/detail?id=2024D07564&did=2024D07564 (accessed 12 November 2025).

Research Institute – Digital Human Rights Center (2025), "Enlightenment 4.0 – human understanding of AI decision-making: report on the theoretical basis of the right to explanation of individual decision-making under Article 86 AI Act", Federal Ministry of Labour and Social Affairs, Health Care and Consumer Protection Republic of Austria. Available at: https://researchinstitute.at/en/enlightenment-4-0-project-results-published-in-english/; Website of the Ministry of Social Affairs (accessed 29 September 2025).

Schot E. and Davidson D. (2025), "*Onbetrouwbaar algoritme bestempelt jongeren als toekomstig crimineel*, Follow the money". Available at: www.ftm.nl/artikelen/algoritme-bestempelt-jongeren-onterecht-als-toekomstig-crimineel?share=UommUbfeHZLpB371b2sHbWwyodKB4uUhl7QNw2Jm6lIWXJmeq7VOeP7i73ixLPA%3D (accessed 13 October 2025).

Skiotytė G. and Sadauskaitė A. (2026), "A Digital Omnibus: identifying interlinks and possible overlaps between different legal acts in the field of digital legislation to streamline tech rules", European Parliament, Policy Department for Economy and Growth, Brussels. Available at: https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU(2026)772641 (accessed 31 April 2026).

Smith E. and Vogell H. (2022), "How your shadow credit score could decide whether you get an apartment", ProPublica. Available at: www.propublica.org/article/how-your-shadow-credit-score-could-decide-whether-you-get-an-apartment (accessed 17 October 2025).

Soler Garrido J., De Nigris S., Bassani E., Sanchez I., Tatjana E., Antoine-Alexandre A. and Boulangé T. (2024), *Harmonised standards for the European AI Act*, Joint Research Centre, European Commission Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC139430 (accessed 17 October 2025).

The Guardian (2021), "What happened when a 'wildly irrational' algorithm made crucial healthcare decisions". Available at: www.theguardian.com/us-news/2021/jul/02/algorithm-crucial-healthcare-decisions (accessed 17 October 2025).

United Nations (2011), "Guiding principles on business and human rights: implementing the United Nations 'protect, respect and remedy' framework", United Nations, New York and Geneva. Available at: https://digitallibrary.un.org/record/720245?v=pdf (accessed 1 October 2025).

Vogiatzoglou P. and Marquiene T. (2022), Assessment of the implementation of the Law Enforcement Directive, European Parliament. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740209 (accessed 17 October 2025).

Wachter S., Mittelstadt B. and Russell C. (2020), "Why fairness cannot be automated: bridging the gap between EU non-discrimination law and AI", *Computer Law & Security Review*, Volume 41, July 2021. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364921000406 (accessed 1 July 2026).

Weerts H., Xenidis R., Tarissan F., Olsen H. P. and Pechenizkiy M. (2023), "Algorithmic unfairness through the lens of EU non-discrimination law: or why the law is not a decision tree", *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, pp. 805-816.

Weerts H., Kelly-Lyth A., Binns R. and Adams-Prassl J. (2024), "Unlawful proxy discrimination: a framework for challenging inherently discriminatory algorithms", *The 2024 ACM Conference on Fairness, Accountability, and Transparency*, pp. 1850-1860. doi:10.1145/3630106.3659010.

Xenidis R. (2021), "Tuning EU equality law to algorithmic discrimination: three pathways to resilience", *Maastricht Journal of European and Comparative Law*, 27(6), pp. 736-758.

Zuiderveen Borgesius F. (2018), "Discrimination, artificial intelligence and algorithmic decision making", Directorate General of Democracy, Council of Europe. Available at: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73 (accessed 10 November 2025).

Legislation

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), *Official Journal of the European Union*, L 205.

Council Directive 76/207/EEC of 9 February 1976 on the implementation of the principle of equal treatment for men and women as regards access to employment, vocational training and promotion, and working conditions, *Official Journal of the European Communities*, OJ, L 39, 14 February 1976, pp. 40-42.

Council Directive 97/80/EC of 15 December 1997 on the burden of proof in cases of discrimination based on sex, *Official Journal of the European Communities*, OJ, L 014, 20 January 1998, pp. 6-8.

Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, *Official Journal of the European Communities*, OJ, L 180, 19 July 2000, pp. 22-26.

Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, *Official Journal of the European Communities*, OJ, L 303, 2 December 2000, pp. 16-22.

Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services, *Official Journal of the European Union*, OJ, L 373, 21 December 2004, pp. 37-43.

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, *Official Journal of the European Union*, OJ L, 2024/1499, 2024/1500, 29 May 2024.

Council of Europe (1950), European Convention on Human Rights, Rome, 4 November 1950, European Treaty Series No. 5.

Council of Europe (2000), Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 2000, European Treaty Series No. 177.

Council of Europe (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Vilnius, 5 September 2024, Council of Europe Treaty Series No. 225.

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. Official Journal of the European Union, OJ, L 204, 26 July 2006, pp. 23-36.

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 (Text with EEA relevance), OJ L 132, 17 May 2023, pp. 21-44.

Directive (EU) 2024/1385 on combating violence against women and domestic violence, OJ L, 2024/1385, 24 May 2024.

Directive (EU) 2024/1500 of the European Parliament and of the Council of 14 May 2024 on standards for equality bodies, *Official Journal of the European Union*, OJ, L, 2024/1500, 29 May 2024.

European Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) C(2025) 5052 final, 29 July 2025.

Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). Available at: https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng, accessed 24 July 2026.

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 (General Data Protection Regulation, GDPR), *Official Journal of the European Union*, OJ, L 119, 4 May 2016, pp. 1-88.

Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM/2025/837 final, EUR-Lex - 52025PC0837 - EN - EUR-Lex.

European Parliament legislative resolution of 16 June 2026 on the proposal for a regulation of the European Parliament and of the Council as regards the simplification of the implementation of harmonised rules on artificial intelligence. Available at: https://www.europarl.europa.eu/doceo/document/TA-10-2026-0198_EN.html#title2, accessed 25 June 2026.

Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products, *Official Journal of the European Union*, OJ, L 169, 25 June 2019, pp. 1-44.

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No. 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA relevance), *Official Journal of the European Union*, OJ L 135, 23 May 2023, pp. 1-51.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), *Official Journal of the European Union*, OJ, L 2024/1689, 12 July 2024.

Regulation (EC) 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), *Official Journal of the European Union*, OJ, L 218, 13 August 2008, pp. 60-81.

Regulation (EU) No. 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of "Eurodac" for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a

third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), *Official Journal of the European Union*, OJ, L 180, 29 June 2013, pp. 1-30.

Swedish Discrimination Act, 2008: 567.

Jurisprudence/case law

Andersen v. Region Syddanmark, (2010), European Court of Justice, Case C-499/08. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2010_346_R_0007_01 (accessed 1 July 2026)

Assessment of creditworthiness, authority, direct multiple discrimination, gender, language, age, place of residence, financial reasons, conditional fine (2018), National Non- Discrimination and Equality Tribunal of Finland, Plenary Session (voting), 216/2017. Available at: https://www.yvtltk.fi/en/decisions/multiple-discrimination-in-the-assessment-of-creditworthiness/ (accessed 13 October 2025).

Association Belge des Consommateurs Test-Achats ASBL and Others v. Conseil des ministres (2011) European Court of Justice, Case C-236/09; ECLI:EU:C:2011:100. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62009CJ0236 (accessed 12 November 2025).

Beghal v. the United Kingdom, Application No. 4755/16 (22 August 2016), European Court of Human Rights, for further discussion of the requirements placed on domestic laws for an impugned measure to be regarded as "in accordance with the law", available at: https://hudoc.echr.coe.int/eng/?i=001-166724.

CHEZ Razpredelenie Bulgaria AD v. Komisia za zashtita ot diskriminatsia (2015), European Court of Justice, Case C-83/14; ECLI:EU:C:2015:480. Available at: https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:62014CJ0083 (accessed 10 November 2025).

CK v. Dun & Bradstreet Austria GmbH and Magistradt der Stadt Wien (2025), European Court of Justice, Case C-203/22; ECLI:EU:C:2025:117. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-203/22 (accessed 7 October 2025).

David L. Parris v. Trinity College Dublin and Others (2016), European Court of Justice, Case C-232/09; ECLI:C:2010:674. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62015CJ0443 (accessed 1 May 2026).

Dekker v. Stichting Vormingscentrum voor Jong Volwassenen (VJV-Centrum) Plus (1990), European Court of Justice, Case C-177/88;ECLI:EU:C:1990:383. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61988CJ0177 (accessed 7 October 2025).

D.H. and Others v. The Czech Republic (2007), European Court of Human Rights, Application No. 57325/00. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-72317%22]} (accessed 1 October 2025).

Dita Danosa v. LKB Līzings SIA (2010), European Court of Justice, Case C-232/09; ECLI:EU:C:2010:674. Available at: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62009CJ0232 (accessed 20 October 2025).

Enderby v. Frenchay Health Authority and Secretary of State for Health (1993), European Court of Justice, Case C-127/92;ECLI:EU:C:1993:313. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-127/92 (accessed 1 October 2025).

Filcams Cgil Bologna and Others v. (…) S.R.L. (2020), Tribunal of Bologna, Order No. 2949/2019. Available at: https://apps.eurofound.europa.eu/platformeconomydb/italian-court-rules-that-the-deliveroo-algorithm-discriminates-workers-106121.

Frédéric Hay v. Crédit Agricole mutuel de Charente Maritime et des Deux-Sèvres (2012), European Court of Justice, Case C-267-12; ECLI:EU:C:2013:823. Available at: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62012CJ0267 (accessed 12 November 2025).

Galina Meister v. Speech Design Carrier Systems GmbH (2012), European Court of Justice, Case C-415/10; ECLI:EU:C:2012:217. Available at: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62010CJ0415 (accessed 12 November 2025).

Glukhin v. Russia (2023), European Court of Human Rights, Application No. 11519/20. Available at: https://hudoc.echr.coe.int/eng?i=001-225655 (accessed 7 October 2025).

Handels- og Kontorfunktionærernes Forbund I Danmark v. Dansk Arbejdsgiverforening, acting on behalf of Danfoss (1989), European Court of Justice, Case C109/99; ECLI:EU:C:1989:383. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61988CJ0109 (accessed 12 November 2025).

Helga Nimz v. Freie und Hansestadt Hamburg (1991), European Court of Justice, Case C-184/89; ECLI:EU:C:1991:50. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:61989CJ0184 (accessed 12 November 2025).

Hoogendijk v. The Netherlands (2005), European Court of Human Rights, Application No. 58641/00. Available at: https://hudoc.echr.coe.int/eng?i=001-68064 (accessed 1 October 2025).

Inge Nolte v. Landesversicherungsanstalt Hannover (1995), European Court of Justice, Case C-317-93; ECLI:EU:C:1995:438. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61993CJ0317 (accessed 12 November 2025).

Ingeniørforeningen i Danmark v. Region Syddanmark (2010), European Court of Justice, Case C-499/08; ECLI:EU:C:2010:600. Available at: https://curia.europa.eu/juris/documents.jsf?critereEcli=ECLI:EU:C:2010:600 (accessed 1 October 2025).

Ingrid Rinner-Kühn v. FWW Spezial-Gebäudereinigung GmbH & Co. KG (1989), European Court of Justice, Case C-171/88; ECLI:EU:C:1989:328. Available at: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A61988CJ0171 (accessed 12 November 2025).

IX v. Wabe eV and MH Müller Handels GmbH v MJ (2021), European Court of Justice, Cases C-804/18 and C-341/19; ECLI:EU:C:2021:144. Available at: https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:62019CC0341 (accessed 7 October 2025).

James v. Eastleigh Borough Council (1990), House of Lords, 2 AC 751. Available at: https://www.bailii.org/uk/cases/UKHL/1990/6.html (accessed 12 November 2025).

Jyske Finans v. Ligebehanlingsnævnet (2017), European Court of Justice, C-668/15; ECLI:EU:C:2017:278. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-668/15 (accessed 10 November 2025).

Kelly v. National University of Ireland (University College, Dublin) (2011), European Court of Justice, Case C-104/10; ECLI:EU:C:2011:506. Available at: https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:62010CJ0104 (accessed 10 November 2025).

La Quadrature du Net and Others v. Premier ministre and Ministère de La Culture (2024), European Court of Justice, Case C-470/21; ECLI:EU:C:2024:370. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0470 (accessed 14 November 2025).

(Loredas) HJ v. US and MU (2024), European Court of Justice, Case C-531-23; ECLI:EU:C:2024:1050. Available at: https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:62023CJ0531 (accessed 12 November 2025).

M. A. De Weerd, née Roks, and others v. Bestuur van de Bedrijfsvereniging voor de Gezondheid, Geestelijke en Maatschappelijke Belangen and others (1994), European Court of Justice, Case C-343/92; ECLI:EU:C:1994:71. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:61992CJ0343 (accessed 12 November 2025).

Manjang v. Uber Eats UK Ltd and others (2021), Employment Tribunal, Case No. 3206212/2021. Available at: www.gov.uk/employment-tribunal-decisions/mr-p-e-manjang-v-uber-eats-uk-ltd-and-others-3206212-slash-2021 (accessed 7 October 2025).

Maria Kowalska v. Freie und Hansestadt Hamburg (1990), European Court of Justice, C-33-89; ECLI:EU:C:1990:265. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61989CJ0033 (accessed 12 November 2025).

Minoo Schuch-Ghannadan v. Medizinische Universität Wien (2019), European Court of Justice, C-274/18; ECLI:EU:C:2019:828. Available at: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62018CJ0274 (accessed 10 November 2025).

N.B. v. Slovakia (2010), European Court of Human Rights, Application No. 29518/10, Judgment of 12 June 2012. Available at: https://hudoc.echr.coe.int/eng?i=001-111427 (accessed 12 November 2025).

Oršuš and others v. Croatia (2010), European Court of Human rights, Application No. 15766/03, Judgment of 16 March 2010. Available at: https://hudoc.echr.coe.int/eng?i=001-97689 (accessed 12 November 2025).

PublicResourceOrg, Inc. and Right to Know CLG v European Commission (2024), European Court of Justice Case C-588/21; ECLI:EU:C:2024:201. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0588 (accessed 17 October 2025).

R (on the application of Bridges) v. Chief Constable of South Wales Police (2020), Court of Appeal, Case EWCA Civ 1058. Available at: www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html (accessed 1 October 2025).

R v. Secretary of State for Employment, ex parte Seymour-Smith and Perez (1999), European Court of Justice, Case C-167/97;ECLI:EU:C:1999:60. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61997CJ0167 (accessed 1 October 2025).

Rechtbank Overijssel (2024) Indirecte discriminatie door DUO bij selectie van uitwonende studenten voor controle. Het verkregen bewijs wordt uitgesloten, Case: ECLI:NL:RBOVE:2024:5627. Available at: ECLI:NL:RBOVE:2024:5627, Rechtbank Overijssel, ak_23_1340 en ak_23_1341 (accessed 1 July 2026).

(SCHUFA Holding) OQ v. Land Hessen (2023), European Court of Justice, Case C-634/21; ECLI:EU:C:2023:957. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-634/21 (accessed 7 October 2025).

(Opinion of AG Pikamäe in SCHUFA Holding) Opinion of Advocate General Pikamäe OQ v. Land Hessen (2023), European Court of Justice, Case C-634/21; ECLI:EU:C:2023:220. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-634/21 (accessed 7 October 2025).

S and Marper v. United Kingdom, [GC] (2008), European Court of Human Rights, Application Nos. 30562/04 and 30566/04, Judgment of 4 December 2008. Available at: https://hudoc.echr.coe.int/fre?i=001-90051 (accessed 12 November 2025).

Sylvie Beghal v. United Kingdom (2016), European Court of Human Rights, Application No. 4755/16, Decision of 14 January 2016. Available at: https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-166724%22]} (accessed 12 November 2025).

Tadao Maruko v. Versorgungsanstalt der deutschen Bühnen (2008), European Court of Justice, C-267/06; ECLI:EU:C:2008:179. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-267/06 (accessed 12 November 2025).

Verli Hariev Belov v. CHEZ Elektro Balgaria AD and Others (2013), European Court of Justice, Case C-394/11; ECLI:EU:C:2013:48. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62011CJ0394 (accessed 17 October 2025).

VL v. Szpital Kliniczny im. dra J. Babińskiego Samodzielny Publiczny Zakład Opieki Zdrowotnej w Krakowie (2021), European Court of Justice, Case C-16/19;ECLI:EU:C:2021:64, para. 48. Available at: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62019CJ0016 (accessed 7 October 2025).

Appendix A

Template for data subject access request (DSAR)

Note: a DSAR may be drafted either in broad terms or in a more narrowly defined manner, each approach having its own benefits and risks.

Specific requests may increase the likelihood of receiving the precise information sought, reducing the need for follow-up correspondence and speeding up the process. Still, in practice, queried organisations often provide an individualised response only after a follow-up request. Narrowly defined requests at an early stage may burden the data subject, who may not know the relevant processing activities or terminology, increasing the risk of missing information and enabling restrictive interpretations by data controllers.

Under the Digital Omnibus regulation proposal[61] this will be formalised. It states that DSARs should be "as specific as possible", while "overly broad and undifferentiated requests should also be regarded as excessive", suggesting that general and undifferentiated requests may be rejected as excessive.

This template serves as an example only and should be adapted to the specific case.

Name, address of the data subject]
[optional: telephone number and e-mail address of data subject]

[Date of the request]

[Details of data controller – Company address][62]

Data subject access request under Article 15 of the GDPR

To whom it may concern,

61. Recital 35, Article 3, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)
62. Send to the data controller: their contact details are usually found in the organisation's privacy policy or legal notice on its website. In cases involving an AI system, the data controller will be typically the deployer of the system (the organisation that uses it, that is, the entity the data subject interacted with during the relevant process, such as a bank, insurer, university or employer) The non-profit organisation Datenanfragen.de e.V., which runs the website datarequests.org (available also in various other languages) maintains a company database with the relevant contact information for privacy-related requests for many companies.

I am hereby exercising my rights under **Article 15 of the General Data Protection Regulation (GDPR)** and request confirmation as to whether or not you are processing personal data concerning me.

If you are processing my personal data, please provide me with the following information in accordance with Article 15 of the GDPR.

1. Access to my personal data for X purposes

- A copy of all personal data concerning me that have been used or considered for the following purposes:

  [Insert purposes central to your case here; for example, opening or managing a bank account in my name/entering into, renewing or extending my mobile phone contract/processing or evaluating my eligibility for [insert specific benefit]/processing or evaluating my job application/determining my access to online accounts, apps or digital subscriptions/allocating rides or delivery orders to me on the platform, etc.]

2. Information on additional processing purposes

- Information about any other purposes for which my personal data have been or are being processed, beyond those listed above.
- A description of the categories of personal data concerned.

3. Disclosures to third parties

- The recipients or categories of recipients to whom my personal data have been disclosed, along with copies of the data shared and the purpose of the sharing, and the date(s) of disclosure

4. Automated decision making and profiling

- Information on whether automated decision making, referred to in Article 22(1) and (4) of the GDPR, has been carried out in relation to my personal data.
- If so, please provide meaningful information about the logic involved, including the categories of personal data, the procedures and principles used for obtaining a specific result as well as the envisaged consequences of such processing for me.

5. Profiling details

- Information on whether any profiling was conducted using my personal data.
- If so, please provide me with the content of this profile and explain how it was created.

If you are transferring my personal data to a third country or an international organisation, I request to be informed about the appropriate safeguards according to Article 46 of the GDPR concerning the transfer.

Please make the personal data concerning me, which I have requested, available to me in a structured, commonly used and machine-readable format as laid down in Article 20(1) of the GDPR.

My request explicitly includes any other services and companies for which you are the controller as defined by Article 4(7) of the GDPR.

As laid down in Article 12(3) of the GDPR, you must provide the requested information to me without undue delay and in any event within one month of receipt of the request. If an extension of up to two further months is necessary, please inform me accordingly.

According to Article 15(3) of the GDPR, you must answer this request without cost to me.

[As proof of my identity, I enclose a copy of my passport/driving licence, etc.] or

[Enter your identification data here. This often includes information like your name, your date of birth, your address, your e-mail address and so on.]

If you do not answer my request within the stated period, I reserve the right to take legal action against you and to lodge a complaint with the responsible supervisory authority.

Thank you in advance.

Yours sincerely,

[Enter your name here]

Appendix B

Template for requesting an explanation pursuant to Article 86 of the AI Act

The following template incorporates a version developed by Research Institute – Digital Human Rights Center (2025b), as published on the website of the Austrian Ministry of Social Affairs.

[Name, address of the person affected]
[optional: telephone number and e-mail address of the person affected]
[Date of the request]
[Details of the deployer of the AI systems[63]]

Request for an explanation pursuant to Article 86 of the AI Act

To whom it may concern,

I refer to the decision concerning me [description of the decision, for example the rejection of a loan application, received risk assessment, assignment of a credit score], which I received on [date of receipt of the decision].

This decision [ ] produces legal effects for me, as it [briefly explain the impact of the decision, for example the rejection of a loan application, denial of access to certain services, increase in insurance prices, etc.].

[or] affects me significantly and adversely, as it [give reasons for the impairment, such as discrimination on the basis of differentiating criteria, targeting of sports betting adverts at people with a gambling addiction].

I hereby assert my right to an explanation pursuant to Article 86 of Regulation (EU) 2024/1689 (AI Act) and request a clear and meaningful explanation of the role of the AI system in the decision-making process and the main elements of the decision taken.

To this end, I request the following information.

63. Send to the deployer of the AI system: the organisation that uses it – that is, the entity the data subject interacted with during the relevant process, such as a bank, insurer, university or employer. If it is a public authority – or an entity acting on their behalf – find their contact details in Part C of the EU database. In any other case, look for deployer's contact details in the AI system interface, the organisation's privacy policy or legal notice on its website.
If a deployer is not explicitly stated, use the contact details of the data controller, who will typically be also the deployer of the system.

1. Role of the AI system in the decision-making process

- To what extent and in what way did the AI system used contribute to the decision-making process?

2. Main elements of the decision taken

- What were the main reasons for the decision, including key influencing criteria, input data and preliminary decisions that influenced the decision made?
- What other implications does the decision have for me, and how were these effects assessed?
- How were the criteria that influenced the decision weighted and why?

3. Human review and basis [not obligatory]

- Was the decision made by the AI system in a fully automated way, or was it reviewed by a human decision maker? If the latter is the case, what exactly did this review look like and who/which department was responsible?
- [optional if applicable] On which contractual or legal basis is the decision based?

[As proof of my identity, I enclose a copy of my passport/driving licence, etc.] or

[Enter your identification data here. These often include information like your name, your date of birth, your address, your e-mail address and so on.]

I formally request that you provide me with the requested information within [x month/s] [in writing], free of charge and in a comprehensible form. If you have any questions, please do not hesitate to contact me [for paper submissions, use the contact details provided above].

Thank you in advance for processing my request and I look forward to receiving your prompt reply.

Yours sincerely,

[Name of the person concerned]

Appendix C

Examples of the use of algorithms and AI

This appendix includes examples where algorithms and AI systems are commonly used. It is ordered per sector, so that one can easily ascertain likely algorithmic involvement. For this list, we made use of Allen and Masters (2020) and Algorithm Watch (2022), more details of which can be found in the references list.

Sector	Example
Banking	Credit scoring
	Automation in the client acceptance procedure
	Fraud or anti-money-laundering detection
Child and youth welfare services	Predicting the future need for welfare services for a child
Education	Admission
	Automation in the allocation of students among schools, universities or programmes
	Automated proctoring
	Predicting or detecting truancy and early school leaving
	Detecting learning problems
Employment	Job application selection or CV selection
	(Un)employment agencies predicting the likelihood of finding employment
	Allocating job offers to job seekers
	Allocating job seekers to training or coaching
	Analysing (exit) interviews
Healthcare	Predicting the chances of disease
	Diagnostic systems
	Predicting the number of elderly people needing extra care
Housing	Automated vetting of potential tenants
	Online forms
	Credit checking

Sector	Example
	Apartment ads on online platforms: which ads are displayed to whom? (Automated placement)
Immigration and border management	Facial recognition of people on a watchlist
	Automation in the visa application acceptance
	Automated travel document review
Insurance	Online forms
	Pricing algorithms
	Automation in the client acceptance procedure
	Automatic claim handling
	Fraud detection
Judicial process	Assisting in drafting laws
Justice	Suggested sentencing based on data
Police	Predicting the occurrence of crimes in certain neighbourhoods or areas (geographic predictive policing)
	Predicting disorderly or violent behaviour
	Risk-assessment or profiling tools used for predicting individuals' future risk of committing crime, including recidivism or more generally identifying "dangerous" or "relevant" people (individual predictive policing)
	Assessing or estimating the likelihood of a person being the perpetrator of an existing crime (individual predictive policing)
	Camera surveillance detecting criminal activity
Social benefits	Online forms
	Predicting fraud or mistakes
	Automation in benefit processing
Taxes	Predicting fraud or mistakes

Appendix D

Examples of algorithmic discrimination or risk of discrimination

Sector or technology	Description algorithm	Description of discriminatory practice	Source
Banking	"Scoring" or assessing creditworthiness	The ADM system had rules in place that led it to decide that a "40-year-old woman" was not creditworthy.	Algorithm Watch (2022) (p. 6) (Similar case in Finland, available here)
Education	Course or degree completion predicting algorithm	Under-represented minority groups were consistently assigned higher risk, along with a lower accuracy score.	Bird, Castleman and Song (2024)
Facial recognition technology	Technology that can identify or match facial images	There are differences in accuracy between different demographics, such as age, gender and skin colour. These differences might lead to cases of discrimination. The Dutch equality body stated the need for organisations to prove their technology does not discriminate, reversing the burden of proof.	College voor de Rechten van de Mens (2023)
Healthcare	Algorithm allocating "care needed" for patients	Arbitrary points system, leading to different allocation of hours in similar cases.	The Guardian (2021)
Housing	Tenant screening algorithms, assigning risk score	Tenant screening based on characteristics that were not proven to be linked to risk.	Smith and Vogell (2022)
Insurance	Pricing algorithm	Direct discrimination as citizenship/nationality impacted the price of car insurance in otherwise identical profiles.	Boscarol (2022)

Sector or technology	Description algorithm	Description of discriminatory practice	Source
Immigration and border control management	Travel document review, facial recognition technology	Direct discrimination as the technology gave a wrongful outcome more often for darker-skinned pictures than lighter-skinned images.	Ahmed (2020)
Judicial system/child and youth welfare	Risk assessment of recidivism	Certain nationalities led to a higher risk score, increasing the chance of prosecution.	Schot and Davidson (2025)
Police/law enforcement	Risk assessment recidivism	The AI system had no transparency, explainability and robustness. Inconsistent and higher risk scores for those without "social stability factors", mostly younger individuals.	Eticas Foundation (2024)
Social benefits	Detecting incorrect or fraudulent applications for childcare benefits	Racial profiling, where applications from non-Dutch nationals were consistently assigned higher risk scores.	Amnesty International (2021)
Social benefits	Social assistance system exacerbating exclusion	Indirect discrimination through a seemingly neutral criterion that put protected demographics at a disadvantage.	Amnesty International (2023)
Welfare fraud detection	Fraud risk scoring system used to identify social benefit recipients for further review	The model disproportionately flagged women, migrants, low-income earners and people without a university education as suspicious.	Lighthouse Reports (2024)
Welfare fraud detection	Fraud risk scoring system used to identify social benefit recipients for further review (CNAF)	The system was contested for generating direct and indirect discriminatory effects for women, people with disabilities and people living in poverty.	La Quadrature du Net (2024) Lighthouse Reports (2023)

Appendix E
Proxies

From a data science/data analysis perspective, proxy variables substitute other variables, for example, if those cannot be observed or measured directly. Proxy variables allow conclusions about certain characteristics without recording those characteristics directly. For example, "30 years of work experience" indicates that the person must be at least in their mid-40s (Algorithm Watch 2022).

In the context of non-discrimination law and algorithmic/AI systems, "proxies" refer to characteristics, features or combinations thereof that are not themselves listed among the explicitly prohibited grounds of discrimination under the relevant legal framework, but that correlate with those grounds in a way that their use can lead to unlawful discrimination.

Two types of proxies can be identified in this regard.

a. Statistical proxies: characteristics (or combinations thereof) that correlate with legally protected grounds and whose use may disproportionately disadvantage persons belonging to a protected group. Such proxies are typically associated with indirect discrimination. For example, in most European countries there is a correlation between educational degree and race or ethnic origin.
b. Inextricably linked proxies: a characteristic (or combinations thereof) that are inextricably linked to a protected attribute, such that their use reflects an inherently discriminatory practice. These proxies are typically associated with direct discrimination. For example, pregnancy has been considered inextricably linked to sex (see Table 8 below).

Although it remains unsettled how close the correspondence between a proxy and a protected group must be to constitute direct discrimination, an inextricable link does not require full (100%) correspondence (Parviainen 2024). Adams-Prassl, Binns and Kelly-Lyth have deemed that a "sufficient degree of correspondence" is required (2023), whereas Weerts et al. (2024) have proposed that the proxy and the protected ground must be "at least highly associated and possibly even deterministically related". Weerts et al. note the relevance of the "but for" question: a claimant in a country with a sex-based retirement age could reasonably argue that he would have reached the retirement age but for his sex; a same-sex couple who live in a country which prohibits same-sex marriage could readily say that they would be married but for their sexual orientation; a woman could reasonably argue that she would not be pregnant but for her sex; and a Muslim woman could argue that she would not wear a headscarf but for her religion.

Whether an inextricable link exists in a given case requires a case-by-case judicial assessment, in which contextual criteria – rather than precise statistical thresholds – shall be given particular weight, in line with the CJEU's approach in discrimination cases (see, for example, *IX v. WABE eV* and *MH Müller Handels GmbH v. MJ*, paragraph 78, where weight was given to the type of signs involved). See the table below for examples of different types of proxies for protected characteristics.

Table 8. Examples of known proxies (as mentioned in, among others, CRM 2025, Weerts et al. 2024, Algorithm Watch 2022)

Characteristic	Proxy for	Type of proxy
30 years of work experience (Algorithm Watch 2022)	Individual is over 45 years old	Inextricably linked
Pregnancy (*Dekker v. Stichting voor Jong Volwassenen (VJV-Centrum) Plus*, 1990)	Sex	Inextricably linked
Marital status (*Tadao Maruko v. Versorgungsanstalt der deutschen Bühnen*, 2008; *Frédéric Hay v Crédit Agricole mutuel de Charente Maritime et des Deux-Sèvres*, 2012)	Sexual orientation, in countries that do not permit same-sex marriage	Inextricably linked, in countries that do not permit same-sex marriage
Sex-based retirement age (*James v. Eastleigh Borough Council*, 1990, §10)	Sex	Inextricably linked
Language or language skill level	Race	Statistical proxy or inextricably linked
Literacy	Race (depending on the country this could also be a proxy for age and sex)	Statistical proxy
Level of education	Race ethnic origin	Statistical proxy
Postcode or neighbourhood	Race (though segregated neighbourhoods)	Statistical proxy
Income	Race, sex	Statistical proxy
Number of persons in household or immediate family	Race (sex)	Statistical proxy
Place of birth	Race	Statistical proxy
Receiving of essential financial benefits	Race	Statistical proxy
Religion	Race	Statistical proxy
Names including, ending or starting with specific letter combination	Race	Statistical proxy

Characteristic	Proxy for	Type of proxy
Absence from work/late cancellations/reduced work availability (*Filcams Cgil Bologna and Others v. Deliveroo Italia S.R.L*, 2020)	Belief (trade union membership), gender or state of health	Statistical proxy
Clothing items and head coverings (such as the wearing of a headscarf) (*IX v. WABE and MH Müller Handels*, 2021)	Religion and belief	Statistical proxy (referring to any signs of political, philosophical or religious belief, for example) or inextricably linked (referring explicitly to conspicuous, large-sized signs, for instance)

Appendix F

List of AI and algorithm registries in Europe

Geographic scope	Title	Scope	Link	Date of update
Belgium	BoSA AI Observatory	List of all known AI applications and projects used by federal institutions and agencies	https://bosa.belgium.be/fr/themes/administration-numerique/cooperation-et-partage-des-connaissances/cooperation-nationale-5	
EU databased for high-risk AI systems – forthcoming		High-risk AI systems		
Each EU country – forthcoming		High-risk AI systems related to critical infrastructure		
EU	Selected AI cases in the public sector	AI in the public sector	Joint Research Centre Data Catalogue – Selected AI cases in the public sector (JRC129301), European Commission	31 December 2021
EU	Public Sector Tech Watch	Observatory dedicated to monitoring, analysing and disseminating the use of emerging technologies	https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch	

Geographic scope	Title	Scope	Link	Date of update
Germany			Use Case Platform – Applied AI Institute	
Helsinki	The City of Helsinki's artificial intelligence systems	AI in the public sector	Tekoälyrekisteri – Helsingin kaupungin tekoälyrekisteri	Rolling updates
Netherlands	The Algorithm Register of the Dutch Government	Algorithmic systems in the public sector	The Algorithm Register of the Dutch Government	Rolling updates
UK	Algorithmic transparency standards recording hub	UK Government (voluntary standard)	Find out how algorithmic tools are used in public organisations – GOV.UK	Rolling
UK	Non-governmental register: Public Law Project Tracking Automated Government (TAG) Register		TAG Register	Rolling

Appendix G

Non-discrimination directives, protected grounds and scope

Directive	Protected grounds	Scope	Standards directive
2000/43/EC (Racial Equality Directive)	Race and ethnic origin – not nationality and without prejudice to treatment arising from legal status of third-country nationals and stateless persons	Employment, vocational training, social protection, education, goods and services, including housing	2024/1499
Directive 2000/78/EC	Religion or belief, disability, age, sexual orientation	Employment and occupation	2024/1499
Directive 2004/113/EC (Gender Goods and Services Directive)	Sex	Goods and services	2024/1499
Directive 2006/54// EC (Recast Gender Equality Directive)	Sex (including pregnancy and maternity)	Employment and occupation (including social security schemes)	2024/1500
2010/41/EU (Gender Self-Employment Directive)	Sex	Self-employed, spouses or life partners of self-employed	2024/1500
2023/970/ EU Equal Pay Directive (transposition by June 2026)		Employment	2024/1500 (but note that without prejudice to more specific provisions set out in the directive itself)

Appendix H

Other potentially relevant regulations and guidelines

Council of Europe

Non-discrimination

Recommendation CM/Rec(2019)1 of the Committee of Ministers to member States on preventing and combating sexism: https://search.coe.int/cm?i=090000168093b26a.

Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies): https://search.coe.int/cm?i=09000016809e1154.

Recommendation CM/Rec(2026)1 of the Committee of Ministers on equality and artificial intelligence, GEC/ADI-AI, under the GEC and CDADI: https://search.coe.int/cm?i=09125948802acd7f.

Studies

Report on preventing discrimination caused by the use of artificial intelligence – Parliamentary Assembly of the Council of Europe, Committee on Equality and Non-discrimination; rapporteur: Mr Christophe Lacroix, (Belgium, SOC), 29 September 2020: https://pace.coe.int/en/files/28807.

Shrishak K. and Pénicaud S. (2025), "Legal protection against algorithmic discrimination in Europe: current frameworks and remaining gaps", Council of Europe. (also in French, Dutch, Portuguese, Finnish, Swedish). Available at: https://rm.coe.int/legal-protection-eng-web/48802a38d7 (accessed 4 August 2026).

Study on discrimination, artificial intelligence and algorithmic decision making – ECRI, November 2018: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.

Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination – GEC/CDADI, August 2023: https://rm.coe.int/prems-112923-gbr-2530-etude-sur-l-impact-de-ai-web-a5-1-2788-3289-7544/1680ac7936.

Xenidis R. (2025), "European policy guidelines on AI and algorithm-driven discrimination for equality bodies and other national human rights structures (also in French, D utch, Portuguese, Finnish, Swedish)", Council of Europe. Available at: https://rm.coe.int/policy-guidelines-eng-web/48802a38a5 (accessed 4 August 2026).

Gender

Recommendation CM/Rec(2026)2 of the Committee of Ministers on accountability for technology-facilitated violence against women and girls: https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209125948802acd83%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}.

Justice and enforcement

Assessment tool for the operationalisation of the European Ethical Charter on the use of artificial intelligence in judicial systems and their environment – CEPEJ(2023)16Final: https://rm.coe.int/cepej-2023-16final-operationalisation-ai-ethical-charter-en/1680adcc9c.

European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment – CEPEJ(2018)14: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

Guidelines on facial recognition, Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data, Convention 108, 28 January 2021: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

Welfare and social safety net

Decl(17/03/2021)2 – Declaration by the Committee of Ministers on the risks of computer-assisted or artificial-intelligence-enabled decision making in the field of the social safety net (adopted by the Committee of Ministers on 17 March 2021 at the 1399th meeting of the Ministers' Deputies): https://search.coe.int/cm?i=0900001680a1cb98.

Education

Havinga, Beth, Holmes, Wayne and Persson Jen (2024), "Regulating the use of artificial intelligence systems in education: preparatory study on the development of a legal instrument". Available at: https://www.coe.int/en/web/education/-/regulating-the-use-of-artificial-intelligence-systems-in-education.

Recommendation on the impact of artificial intelligence (AI) on the education sector, adopted by the Conference of International Non-Governmental Organisations – CONF-AG(2023)REC4. Available at: https://rm.coe.int/conf-ag-2023-rec4-draft-recommendation-on-the-impact-of-artificial-int/1680ac8e25.

Migration, immigration and asylum

Recommendation CM/Rec(2022)17of the Committee of Ministers to member States on protecting the rights of migrant, refugee and asylum-seeking women and girls (paragraphs 5-8 and 22-25 in particular): https://rm.coe.int/prems-092222-gbr-2573-recommandation-cm-rec-2022-17-a5-bat-web-1-/1680a6ef9a.

See also: IT Flows policy brief: https://bura.brunel.ac.uk/handle/2438/27982.

Appendix I

High-risk AI practices

High-risk area	Use case
1. Biometrics	Remote biometric identification systems, not including verification
	Biometric categorisation of sensitive or protected attributes, or inference of characteristics based on those attributes
	Emotion recognition
2. Critical infrastructure	Safety components in management and operation of critical infrastructure
3. Education and vocational training	Determining access or admission, or assigning individuals to educational level
	Evaluating learning outcomes and/or steering the learning process in educational or vocational training
	Assessing the appropriate level of education
	Monitoring or detecting prohibited behaviour of students during tests
4. Employment, worker management and access to self-employment	Recruitment or selection of natural persons, targeted job advertisements or evaluating candidates/job applications
	Decision making regarding work-related relationships (such as a promotion), allocation of tasks, and monitoring or evaluating performance
5. Access to essential services	Evaluating eligibility for public benefits and services
	Evaluating creditworthiness or establishing credit score, financial fraud excluded
	Risk assessment and pricing in life and health insurance
	Evaluating and/or classifying emergency calls for dispatch, or establishing priority in dispatching of emergency first response or healthcare triage
6. Law enforcement	Assessing the risk of being a victim of a criminal offence
	Polygraph or similar tools
	Evaluating reliability of evidence
	Assessing risk of (re-)offending, or assessing personality traits or criminal behaviour

High-risk area	Use case
	Assisting in detection, investigation or prosecution of criminal offences
7. Migration, asylum and border control management	Polygraph or similar tools
	Assessing risk on the matters of security, irregular migration or health posed by entrance into the territory of a member state
	Examining applications for asylum, visa, residence permit or complaints regarding eligibility applying for status
	Detecting, recognising or identifying natural persons, exception applies for verification (of travel documents)
8. Administration of justice and democratic processes	Assisting judicial authority in researching and interpreting facts and the law, and applying the law to concrete facts
	Systems intended to influence voting behaviour in elections and/or referendums

Note: the Commission has published draft guidelines on the classification of high-risk AI systems, which are in consultation until June 2026.[64]

64. See more here: Commission seeks feedback on the draft guidelines for the classification of high-risk artificial intelligence systems, Shaping Europe's digital future, accessed on 5 June 2026.

Appendix J

Prohibited AI practices

Table 9. List of prohibited practices regarding the use of AI systems

Prohibited practice	Article	Recital
Purposefully manipulating or deceiving, materially distorting behaviour or impairing the ability to make an informed decision, reasonably likely to cause significant harm, including the generation of non-consensual sexual and intimate content or child sexual abuse material (CSAM).	5(1)(a); 5(1)(ba) & (bb), 5(1a) and (1b)	Recital 29
Exploiting any vulnerability due to age, disability or socio-economic status, with the objective or effect of materially distorting behaviour, reasonably likely to cause significant harm.	5(1)(b)	Recital 29
Classifying or evaluating natural person(s) over a certain period of time based on their social behaviour or personal(ity) characteristics with a social score leading to detrimental or unfavourable treatment in either: ▸ an unrelated context than originally collected; ▸ an unjustified or disproportionate manner.	5(1)(c)	Recital 31
Risk assessment or prediction of committing a criminal offence, based solely on the profiling of a natural person.	5(1)(d)	Recital 42
Untargeted scraping of facial images from CCTV or the internet, to expand or create a facial recognition database.	5(1)(e)	Recital 43
Emotion recognition in the workplace, exceptions apply for medical and safety reasons.	5(1)(f)	Recital 44
Biometric categorisation of individual persons to deduce race, political opinion, trade union membership, religious or philosophical beliefs, sex life or sexual orientation.	5(1)(g)	Recital 30
“Real-time” remote biometric identification in publicly accessible places for the purposes of law enforcement, exceptions apply.	5(1)(h)	Recitals 32, 33, 38, 39, 40 and 41

Table 10. Prohibited AI practices can be related to high-risk AI

High-risk AI systems (Article 6(2), Annex III)	Prohibited practice Article 5	Examples of prohibited and potentially prohibited use cases and explanation
1. Biometrics 1a) Remote biometric identification (RBI) systems	(h) "Real-time" remote biometric identification in public spaces for law enforcement, unless used for: i. a search for a victim of abduction; ii. preventing a specific, substantial and imminent threat; iii. identifying a person for specific crimes (specified in Annex II).	**Key elements: the use of RBI in:** **i. "real time"** **ii. public spaces** **iii. by, or on behalf of, law enforcement.** Recital 32 states that the use of real-time RBI systems "evoke a feeling of constant surveillance and indirectly dissuade the exercise of freedom of assembly and other fundamental rights" **Example: police using live facial recognition CCTV to identify and arrest a person of interest.** After identifying a peaceful protestor, police in Moscow (*Glukhin v. Russia*, 2024) used CCTV footage to identify and locate an individual using "real-time" biometric identification
1a) Remote biometric identification (RBI) systems	(e) Untargeted scraping of facial images for creating or expanding a database	**Key elements: the method of creating or expanding a recognition database by untargeted scraping rather than identifying itself.** It is prohibited as untargeted scraping operates like a "vacuum cleaner", as stated in Article 5(1)(e), indiscriminately collecting facial images without targeting specific individuals. Recital 43 adds to the justification based on the "feeling of mass surveillance" and possibility of violating fundamental rights. **Example: border authorities building a facial recognition database through mass scraping**

High-risk AI systems (Article 6(2), Annex III)	Prohibited practice Article 5	Examples of prohibited and potentially prohibited use cases and explanation
		There could be a possibility where border authorities scrape facial images from social media, news articles and CCTV footage without specific targeting of individuals. If these are then added to a database for biometric identification, it would be prohibited under Article 5(1)(e).
1b) Biometric categorisation on protected characteristics (or inference thereof)	(g) Biometric categorisation which infer race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation	**Key elements: the specific purpose of inferring the protected characteristics listed (race, political opinions, trade union membership, religion, sex life or sexual orientation) based on biometric data.** Biometric categorisation is already immediately considered high risk, with Article 5(1) (g) absolutely prohibiting the use of biometric data to infer these specific attributes. **Example: an AI system that analyses a person's social media pictures to infer their sexual orientation from their biometric data to send them targeted advertising.**
1c) Emotion recognition	(f) Emotion recognition in the workplace and educational institution (exception: medical and safety purposes)	**Key elements: inferring emotions or intentions in the context of a workplace and education where the exemptions of medical or safety justification do not apply.** Article 5(1)(f) prohibits the use of the high-risk emotion recognition practice in these specific contexts. Recital 44 further highlights concern about the scientific basis for such AI systems that, especially combined with power imbalances in a work or educational context, could have detrimental effects.

High-risk AI systems (Article 6(2), Annex III)	Prohibited practice Article 5	Examples of prohibited and potentially prohibited use cases and explanation
		Note: recognising physical states, for example whether or not a bus driver is fatigued, is not prohibited here. **Example: an AI system that infers whether employees leave their workplace "happy", "angry" or "sad".** An employer trying to gauge the emotions of its restaurant employees from CCTV footage.
3) Educational and vocational training a) Determining access/admission	(a) Manipulation, deception or impairment of an informed decision, causing harm	**Key elements: the use of a manipulative or deceptive technique that materially distorts (or is reasonably likely to) the behaviour of an individual.** Article 5(1)(a) prohibits techniques that have the purpose or effect of distorting behaviour through techniques that impair informed decision making and cause significant harm. Note: intent is not necessary, the effect suffices. **Example: a university employing a chatbot in their determination of admission, with countdowns or fabricated messages.** A chatbot deploying techniques otherwise known as dark patterns, such as "Only 3 spots left!" would be prohibited under this article.

High-risk AI systems (Article 6(2), Annex III)	Prohibited practice Article 5	Examples of prohibited and potentially prohibited use cases and explanation
3) Educational and vocational training b) Evaluating the learning outcomes and steering the learning process c) Assessing (appropriate) education level d) Monitoring/ detecting prohibited behaviour of students	(f) Emotion recognition in workplace and educational institution (exception: medical and safety purposes)	**Key element: the inference of emotive states or intentions of students, and the influence of those on their learning process.** AI systems may be used for assessing students; however, recognising their emotions or intentions is prohibited. Recital 44 further highlights concern about the scientific basis of such AI systems that, especially combined with power imbalances in a work or educational context, could have detrimental effects. **Example: a university uses a personalised learning platform that takes into account students' emotions on their webcams during online lectures to steer the learning process.**
4) Employment and worker management a) Recruitment (targeted advertising) or selection (job application evaluation)	(a) Manipulation, deception or impairment of an informed decision, causing harm (b) Exploiting a vulnerability	**Key elements: the use of a manipulative or deceptive technique that materially distorts (or is reasonably likely to) the behaviour of an individual.** Article 5(1)(a) prohibits techniques that have the purpose or effect of distorting behaviour through techniques that impair informed decision making and cause significant harm. Note: intent is not necessary, the effect suffices. **Example: an AI recruitment platform with fabricated urgency and deceptive manipulation towards signing a contract.**

High-risk AI systems (Article 6(2), Annex III)	Prohibited practice Article 5	Examples of prohibited and potentially prohibited use cases and explanation
		A recruitment agency deploying an AI system with exaggerated salaries/benefits or urgency impairing an informed decision would be prohibited under this article.
4) Employment and worker management b) Decisions affecting work-related relationships, such as termination or task allocation	(a) Manipulation, deception or impairment of an informed decision, causing harm (b) Exploiting a vulnerability	**Key elements: the use of a manipulative or deceptive technique that materially distorts (or is reasonably likely to) the behaviour of an individual.** Article 5(1)(a) prohibits techniques that have the purpose or effect of distorting behaviour through techniques that impair informed decision making and cause significant harm. Note: intent is not necessary, the effect suffices. **Example: a logistics company deploying AI that allocates delivery tasks and monitors driver performance.** There is a feasible scenario where, through such a system, drivers' behaviour could be distorted into working longer than legal hours, impacting health and safety and causing significant harm. Such a system would therefore be prohibited.
4) Employment and worker management b) Decisions affecting work-related relationships, such as termination or task allocation	(f) Emotion and/or intention recognition in workplace and educational institution	**Key element: the inference of emotive states or intentions of employees, and the influence of these on their work.**

High-risk AI systems (Article 6(2), Annex III)	Prohibited practice Article 5	Examples of prohibited and potentially prohibited use cases and explanation
		AI systems may be used to assist decision making. However, basing any assistance on the use of emotion recognition is prohibited. Recital 44 further highlights concern about the scientific basis of such AI systems that, especially combined with power imbalances in a work or educational context, could have detrimental effects. **Example: a call centre deploying AI to monitor employees uses their emotional state for performance evaluation.** In the example, if an AI system were to infer emotive states of the employee based on voice recordings, and take this into account for the performance evaluation, it would be a prohibited practice.
5) Access to essential services and benefits a) Evaluating eligibility of a natural person	(c) Social scoring leading to unfavourable treatment: i) in a different context than the collected data and/or ii) unjustified or disproportional	**Key elements: unfavourable treatment based on their social behaviour from an unrelated context and/or disproportionate in its effect.** If an AI system is used for evaluating eligibility, it may not be the case that it takes data from a different context. **Example: public authorities deploy an AI system to allocate benefits that uses unrelated data.** It is important in these forbidden cases that the context in which the data are collected materially differs from the context they are used in.

High-risk AI systems (Article 6(2), Annex III)	Prohibited practice Article 5	Examples of prohibited and potentially prohibited use cases and explanation
5b) Evaluating creditworthiness	(c) Social scoring leading to unfavourable treatment: i) in a different context than the collected data and/or ii) unjustified or disproportional	**Key elements: unfavourable treatment based on their social behaviour from an unrelated context and/or disproportionate in its effect.** If an AI system is used for assessing a person's credit, it may do this based on financial history, but not other, unrelated contexts. **Example: financial institutions deploy an AI system to assess loans, but also access other, non-financial databases.** If a bank were to also analyse social media connections, or take into account the address of the person in deciding whether or not the applicant's loan should be approved, it might be prohibited under Article 5(1)(c).
5c) Risk assessment in regard to the pricing of health or life insurance	(c) Social scoring leading to unfavourable treatment: i) in a different context than the collected data and/or ii) unjustified or disproportional	**Key elements: unfavourable treatment based on their social behaviour from an unrelated context and/or disproportionate in its effect.** If an AI system is used for pricing life insurance it may do this based on medical history, but not other, unrelated contexts. **Example: an insurer deploys an AI system to assess pricing based on information from an unrelated context.** If an insurer were to analyse social media connections and behaviour, it might be prohibited under Article 5(1)(c).

High-risk AI systems (Article 6(2), Annex III)	Prohibited practice Article 5	Examples of prohibited and potentially prohibited use cases and explanation
6) Law enforcement a) Assessing risk of victimhood b) Polygraphs c) Evaluating reliability of evidence d) Assessing risk of (re)offending, or assessing characteristics e) Profiling during detection, investigation or prosecution	(d) Crime risk assessment solely based on profiling	**Key elements: assessment is based on personality traits and characteristics and no objective facts.** **Note: if a system supports a human decision, an exception may apply.** Article 5(1)(d) prohibits risk assessments for criminal offences based solely on the profiling of personality traits without objective verifiable facts linking to criminal activity. **Example: predictive policing system, profiling individuals on their demographic.** If the police department were to predict the likelihood of criminal activity based on characteristics such as age, nationality or neighbourhood, it would be a prohibited system under Article 5(1)(d). (AI Act, Recital 48. EP policy guidelines with examples p. 18)
6) Law enforcement e) Profiling during detection, investigation or prosecution	(h) Real-time remote biometric identification in public spaces for law enforcement, unless used for: i. a search for a victim of abduction' ii. preventing specific, substantial and imminent threat;	**Key elements: the use of RBI in:** **i. "real time"** **ii. public spaces** **iii. by, or on behalf of, law enforcement.**

High-risk AI systems (Article 6(2), Annex III)	Prohibited practice Article 5	Examples of prohibited and potentially prohibited use cases and explanation
	iii. identifying a person for specific crimes (specified in Annex II).	Recital 32 states that the use of real-time RBI systems "evoke a feeling of constant surveillance and indirectly dissuade the exercise of freedom of assembly and other fundamental rights". **Example: police using live facial recognition CCTV to identify and arrest a person of interest.** After identifying a peaceful protestor, police in Moscow (*Glukhin v. Russia*, 2024) used CCTV footage to identify and locate an individual using "real-time" biometric identification.
7) Migration, asylum and border control Risk assessment of security, irregularity or health Assessing asylum/ visa/permits, eligibility and complaints	(d) Crime risk assessment solely based on profiling	**Key elements: assessment is based on personality traits and no objective facts.** **Note: if a system supports a human decision, exceptions may apply.** Article 5(1)(d) prohibits risk assessments for criminal offences based solely on profiling of personality traits without objective verifiable facts linking to criminal activity. **Example: border authorities deploying an AI system that bases risk profiling of individuals on their demographic.** If border authorities were to predict the risk of offending based on characteristics such as nationality or region, it might be a prohibited system under Article 5(1)(d).

High-risk AI systems (Article 6(2), Annex III)	Prohibited practice Article 5	Examples of prohibited and potentially prohibited use cases and explanation
7) Migration, asylum and border control (b) Risk assessment of security, irregularity or health	(h) Real-time remote biometric identification in public spaces for law enforcement, unless used for: i. a search for a victim of abduction; ii. preventing specific, substantial and imminent threat; iii. identifying a person for specific crimes (specified in Annex II).	**Key elements: the use of RBI in:** **i. "real time"** **ii. public spaces** **iii. by, or on behalf of, law enforcement.** Recital 32 states that the use of real-time RBI systems "evoke a feeling of constant surveillance and indirectly dissuade the exercise of freedom of assembly and other fundamental rights". **Example: the use of live facial recognition CCTV at the border to identify persons of interest.**
7) Migration, asylum and border control (d) Detecting, recognising or identifying natural persons (exception for travel document verification)	(e) Untargeted scraping of facial images	**Key elements: the method of creating or expanding a recognition database by untargeted scraping rather than identifying itself.** It is prohibited as untargeted scraping operates like a "vacuum cleaner", as stated in Article 5(1)(e), indiscriminately collecting facial images without targeting specific individuals. Recital 43 adds to the justification based on the "feeling of mass surveillance" and possibility of violating fundamental rights. **Example: border authorities building a facial recognition database through mass scraping.** There could be a possibility where border authorities scrape facial images from social media, news articles and CCTV footage without specific targeting of individuals. If these were then to be added to a database for biometric identification at the border, it would be prohibited under Article 5(1)(e).

Appendix K

Record sheet for step 3

This sheet has been designed as an example of how a caseworker following the steps in section 3 could record their findings. The examples are fictional to give an idea of the types of information that could be recorded. It is anticipated that the actual recording will be significantly more detailed. The final column is to enable a review of the evidence following any disclosure by the respondent.

Step		Presumption of discrimination	Following respondent's disclosure
3.1 Known and suspected risk **3.1.1 Type of system**	Record whether the system is a high-risk system or whether it is intended for use in any of the sectors or areas identified as posing a risk of discrimination in the AI Act.	**Examples** **Sector:** **Use case:**	
3.1.2 Known risks of discrimination	Record the area in which there is a known risk, the type of technology and any other relevant information and evidence.	**Examples** **Sector:** law enforcement **Technology:** live facial recognition, biometrics **Source:** NGO or academic research, EU AI Act, Article 5 (prohibited systems), Article 6 (high risk) and Annex III.	
3.2 Protected characteristics and proxies	Record direct use of protected characteristics. Where are they used and how?	**Protected characteristics** **How used:** input data, for example	

Step		Presumption of discrimination	Following respondent's disclosure
Further investigate the technical design of the system and influence of the (suspected) proxies on the outcomes of the system. **The fact that a proxy is used as an input is by itself not enough as evidence for discrimination. The next step is to evaluate the evidence to understand if the use of these inputs leads to unequal treatment.**	Record any identified use of protected characteristics or proxies that are used to, or are believed to, impact the outcome of the system. Record also for each proxy why the EB considers these to be proxies.	**Examples** **Proxies:** for example, a postcode as a proxy for race, pregnancy as a proxy for gender. **Evidence and arguments**	
3.3 Risk assessments, including FRIA	Record any risks to discrimination identified by the provider or deployer and any measures identified to mitigate that risk.	**Examples** **Risk:** race discrimination owing to historical bias **Where identified:** risk assessment **Mitigation measure:** de-biasing technique	
	Consider and record whether there are any clear and obvious failures in the risk assessment, DPIA or FRIA.	Risk assessment refers to discrimination but not race. DPIA: does not consider race under special category data. FRIA: does not consider race discrimination and Article 14 of the European Convention on Human Rights.	

Step		Presumption of discrimination	Following respondent's disclosure
	Consider and record the existence and impact of any human in the loop. Who is the relevant person? Does the relevant person have the necessary competence, training and authority to override a decision made by an AI system? Has the relevant person been trained to understand and interpret the output of the system and recognise where bias may arise and intervention be required? Are there any guidelines or protocols issued to decision makers to help them understand how to use the AI system or interpret the output?	Contact person: Role: reviews decisions but does not review the data that led to the decision. Query whether this is sufficient?	
3.4 Aim of system	Record the purpose of the system and what it optimises for.	Purpose of the system: Designed to optimise for:	

Step		Presumption of discrimination	Following respondent's disclosure
	Record proxies and protected characteristics that influence the system output and, when available, metrics on their weight/influence on the output.	Protected characteristics that influence the system: Proxies that influence the system: Metrics on weight/ influence:	
3.5 Training, testing and validation data	Record any general data issues, including issues relating to data quality.	For example, the data sample is very small, old or relates to a different geographical area.	
	Data issues related to inequality and discrimination.		
	Issues relating to insufficient documentation.		
	Concerns about mitigation measures.		
	Argument for how data and mitigation issues would lead to unequal treatment in the current case.		
	Record any indicators of non-compliance with the AI Act provisions relevant to data.		
3.6 Testing and evaluation	Output or treatment gaps as revealed in the statistics.		
	Issues with the reported statistics (such as the wrong metric, or data issues).		
	Gaps in testing identified.		

Step		Presumption of discrimination	Following respondent's disclosure
Conclusion	Review the information and record the basis on which a case of prima facie discrimination can be argued or conclude that it cannot.		
	Review all the steps after further disclosure to determine whether the respondent has successfully rebutted the presumption or justified the discrimination.		

Artificial intelligence (AI) is reshaping our societies and affecting fundamental rights and equality. These systems can reinforce and create discrimination because they are often designed to differentiate among individuals: classifying, ranking or targeting them. In combination with historical inequalities and human biases embedded in the data, rules and design choices of algorithmic systems, discriminatory patterns may be reproduced and scaled unless they are proactively identified and mitigated.

This methodology provides step-by-step guidance to equality bodies and other human rights organisations in Europe to assess discrimination cases related to AI or algorithmic systems. It is meant for the case workers, advisers and lawyers of entities that investigate discrimination claims involving, or suspected of involving, AI or automated decision making.

The methodology relies on the European regulatory framework on AI, specifically on the EU AI Act and the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, and anti-discrimination law, and make references to other legislation, such as data protection, example cases and jurisprudence, where relevant.

PREMS 114926

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.

http://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

Co-funded by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Co-funded and implemented by the Council of Europe