

Targeted stakeholder consultation on classification of AI systems as high-risk

Fields marked with * are mandatory.

Targeted stakeholder consultation on the implementation of the AI Act's rules for high-risk AI systems

Disclaimer: This document is a working document of the AI Office for the purpose of consultation and does not prejudice the final decision that the Commission may take on the final guidelines. The responses to this consultation paper will provide important input to the Commission when preparing the guidelines.

This consultation is targeted to stakeholders of different categories. These categories include, but are not limited to, providers and deployers of (high-risk) AI systems, other industry organisations, as well as academia, other independent experts, civil society organisations, and public authorities.

The Artificial Intelligence Act (the 'AI Act')[1], which entered into force on 1 August 2024, creates a single market and harmonised rules for trustworthy and human-centric Artificial Intelligence (AI) in the EU.[2] It aims to promote innovation and uptake of AI, while ensuring a high level of protection of health, safety and fundamental rights, including democracy and the rule of law. The AI Act follows a risk-based approach classifying AI systems into different risk categories, one of which is the high-risk AI systems (Chapter III of the AI Act). The relevant obligations for those systems will be applicable two years after the entry into force of the AI Act, as from 2 August 2026.

The AI Act distinguishes between two categories of AI systems that are considered as 'high-risk' set out in Article 6(1) and 6(2) AI Act. Article 6(1) AI Act covers AI systems that are embedded as safety components in products or that themselves are products covered by Union legislation in Annex I, which could have an adverse impact on health and safety of persons. Article 6(2) AI Act covers AI systems that in view of their intended purpose are considered to pose a significant risk to health, safety or fundamental rights. The AI Act lists eight areas in which AI systems could pose such significant risk to health, safety or fundamental rights in Annex III and, within each area, lists specific use-cases that are to be classified as high-risk. Article 6(3) AI Act provides for exemptions for AI systems that are intended to be used for one of the cases listed in Annex III, but which do not pose significant risk since they fall under one of the exceptions listed in Article 6(3).

AI systems that classify as high-risk must be developed and designed to meet the requirements set out in Chapter III Section 2, in relation to data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security. Providers of high-risk AI systems must ensure that their high-risk AI system is compliant with these requirements and must themselves comply with a number of obligations set out in Chapter III Section 3, notably the obligation to put in place a quality management system and ensure that the high-risk AI system undergoes a conformity assessment prior to its being placed on the market or put into service. The AI Act also sets out obligations for deployers of high-risk AI systems, related to the correct use, human oversight, monitoring the operation of the high-risk AI system and, in certain cases, to transparency vis-à-vis affected persons.

Pursuant to Article 6(5) AI Act, the Commission is required to provide guidelines specifying the practical implementation of Article 6, which sets out the rules for high-risk classification, by 2 February 2026. It is further required that these guidelines should be accompanied with a comprehensive list of practical examples of use cases of AI systems that are high-risk and not high-risk. Moreover, pursuant to Article 96(1)(a) AI Act, the Commission is required to develop guidelines on the practical application of the requirements for high-risk AI systems and obligation for operators, including the responsibilities along the AI value chain set out in Article 25.

The purpose of the present targeted stakeholder consultation is to collect input from stakeholders on practical examples of AI systems and issues to be clarified in the Commission's **guidelines** on the classification of high-risk AI systems and future guidelines on high-risk requirements and obligations, as well as responsibilities along the AI value chain.

As not all questions may be relevant for all stakeholders, respondents may reply only to the section(s) and the questions they would like. Respondents are encouraged to provide **explanations and practical cases** as a part of their responses to support the practical usefulness of the guidelines.

The targeted consultation is available in English only and will be open for **6 weeks starting on 6 June until 18 July 2025**.

The questionnaire for this consultation is structured along 5 sections with several questions.

Regarding section 1 and 2, respondents will be asked to provide answers pursuant to the parts of the survey they expressed interest for in Question 13, whereas all participants are kindly asked to provide input for section 3, 4 and 5.

Section 1. Questions in relation to the classification rules of high-risk AI systems in Article 6(1) and the Annex I to the AI Act

- This section includes questions on the concept of a safety component and on each product category listed in Annex I of the AI Act.

Section 2. Questions in relation to the classification of high-risk AI systems in Article 6(2) and the Annex III of the AI Act. This category includes questions related to:

- AI systems in each use case under the 8 areas referred to in Annex III.
- The filter mechanism of Article 6(3) AI Act allowing to exempt certain AI systems from being classified as high-risk under certain conditions.
- If pertinent: Need for clarification of the distinction between the classification as a high-risk AI system and AI practices that are prohibited under Article 5 AI Act (and further specified in the Commission's guidelines on prohibited AI practices[3] from 3 February 2025) and interplay of the classification with other Union legislation.

Section 3. General questions for high-risk classification. This category includes questions related to:

- The notion of intended purpose, including its interplay with general purpose AI systems.
- Cases of potential overlaps within the AI Act classification system under Annex I and III.

Section 4. Questions in relation to requirements and obligations for high-risk AI systems and value chain obligations. This category includes questions related to:

- the requirements for high-risk AI systems and obligations of providers.
- the obligations of deployers of high-risk AI systems.
- the concept of substantial modification and the value chain obligations in Article 25 AI Act.

Section 5. Questions in relation to the need for amendment of the list of high-risk use cases in Annex III and of prohibited AI practices laid down in Article 5.

- Input for the mandatory annual assessment of the need for amendment of the list of high-risk use-cases set out in Annex III
- Input for the mandatory annual assessment of the list of prohibited AI practices laid down in Article 5

All contributions to this consultation may be made publicly available. Therefore, please do not share any confidential information in your contribution. Individuals can request to have their contribution anonymised. Personal data will be anonymised.

The AI Office will publish a summary of the results of the consultation. Results will be based on aggregated data and respondents will not be directly quoted.

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689).

[2] Article 1(1) AI Act.

Information about the respondent

* First name

Eva Deborah

* Surname

Kohner

* Email address

info@ENNHRI.org

* Do you represent an organisation (e.g., think tank or civil society/consumer organisation) or act in your personal capacity (e.g., independent expert or from a downstream provider)?

- ☒ Organisation
☐ In a personal capacity

* Name of the organisation

European Network of National Human Rights Institutions (ENNHRI)

* Type of organisation

Civil society organisation/association

* Is a representation of the organisation located in the EU?

- ☒ The organisation's headquarter is located in the EU
☐ A branch office, or any representation of the organisation is located in the EU
☐ None of the representations of the organisation is located in the EU

* Select the EU member state where the organisation's headquarter, or representation is located

BE - Belgium

* Select the size of the organisation

Small (10-49 employees)

* Sector(s) of activity

- ☐ Information technology ☐ Employment ☐ Transport

- | | | |
|--|---|--|
| ☐ Public administration | ☐ Education and training | ☐ Telecommunications |
| ☐ Law enforcement | ☐ Consumer services | ☐ Retail |
| ☐ Justice sector | ☐ Business services | ☐ E-commerce |
| ☐ Legal services sector | ☐ Banking and finances | ☐ Advertising |
| ☐ Cultural and creative sector, including media | ☐ Manufacturing | ☐ Consumer protection |
| ☐ Healthcare | ☐ Energy | ☒ Others |

* Please, specify

30 character(s) maximum

Human Rights, rule of law

* Describe the activities of your organisation or yourself

1300 character(s) maximum

ENNHRI is the European Network of National Human Rights Institutions. We bring together 50 National Human Rights Institutions (NHRIs) across Europe to enhance the promotion and protection of human rights in the region. Our network provides a platform for collaboration and solidarity in addressing human rights challenges and a common voice for NHRIs at the European level. NHRIs are state-mandated bodies, independent of government, with a broad constitutional or legal mandate to promote and protect human rights at the national level. They can take different forms, including ombuds institutions, human rights commissions and institutes. At ENNHRI, we work to: -Strengthen NHRIs by facilitating the exchange of information and good practices and organising capacity-building activities -Support NHRIs with their compliance with the UN Paris Principles during their establishment, accreditation and when they come under threat -Connect NHRIs to European institutions by facilitating their engagement with regional mechanisms, raising their visibility and intervening on regional legal and policy developments.

* All contributions to this consultation may be made publicly available. Therefore, please do not share any confidential information in your contribution. Your e-mail address will never be published. Should your contribution be anonymised in the instance that all contributions are made publicly available?

If you act in your personal capacity: All contributions to this consultation may be made publicly available. You can choose whether you would like your details to be made public or to remain anonymous. The type of respondent that you responded to this consultation as, your answer regarding residence, and your contribution may be published as received. Your name will not be published. Please do not include any personal data in the contribution itself.

If you represent one or more organisations: All contributions to this consultation may be made publicly available. You can choose whether you would like respondent details to be made public or to remain anonymous. Only organisation details may be published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its size, its presence in or outside the EU and your contribution may be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.

- ☒ Yes, please anonymise my contribution.
- ☐ No

* Do you agree that we may contact you in the event of follow-up questions or if we want to learn more about your responses?

- ☐ Yes
☒ No

☒ I acknowledge the attached privacy statement.

[Privacy_statement_high_risks.pdf](#)

* **On which part(s) of the public consultation are you interested to contribute to?** *Multiple answers are possible. Please note that selecting a particular answer will direct you to a set of questions specifically related to subject specified.*

- ☐ Questions in relation to **Annex I of the AI Act**. (Section 1)
☒ Questions in relation to **Annex III of the AI Act**. (Section 2)
☐ Questions on **horizontal aspects** of the high-risk classification. (Section 3)
☒ Questions in relation to **requirements and obligations for high-risk AI systems and value chain obligations**. (Section 4)
☒ Questions in relation to the **need for possible amendments of high-risk use cases in Annex III and of prohibited practices in Article 5**. (Section 5)

Section 2. Questions in relation to the classification rules of high-risk AI systems in Article 6(2) and (3) AI Act and Annex III to the AI Act

AI systems classified as high-risk by Article 6(2) AI Act are AI systems which pose a significant risk of harm to the health, safety or fundamental rights of natural persons, and which are intended to be used for specific use cases as explicitly specified in Annex III under each area (cf. Annex III):

- *Biometrics.*
- *Critical infrastructure.*
- *Education and vocational training.*
- *Employment, workers' management and access to self-employment.*
- *Access to and enjoyment of essential private services and essential public services and benefits.*
- *Law enforcement.*
- *Migration, asylum and border control management.*
- *Administration of justice and democratic processes.*

However, in certain cases the use of an AI system does not risk leading to a significant risk of harm to the health, safety or fundamental rights of natural persons, for example by not materially influencing the outcome of decision making. Therefore, even if the AI systems may be referred to in Annex III, paragraph 3 of article 6 AI Act envisages situations when such AI systems would not be classified as high-risk if one or more of the

following conditions are fulfilled:

- (a) the AI system is intended to perform a narrow procedural task;
- (b) the AI system is intended to improve the result of a previously completed human activity;
- (c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or
- (d) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.

However, this exception cannot be applied if the AI system performs profiling of natural persons.

A provider who considers that an AI system referred to in Annex III falls within one or more of the exceptions should document its assessment before that system is placed on the market or put into service and register it according to Article 49(2).

Questions in relation to **Annex III of the AI Act**. Multiple answers are possible

- ☒ Biometrics
- ☐ Critical infrastructure
- ☒ Education and vocational training
- ☐ Employment, workers' management and access to self-employment
- ☒ Access to and enjoyment of essential private services and essential public services and benefits
- ☒ Law enforcement
- ☒ Migration, asylum and border control management
- ☒ Administration of justice and democratic processes

2.A. Questions in relation to biometrics (Annex III, point 1)

The concepts of real-time remote biometric identification at publicly accessible places for law enforcement purposes, biometric categorisation and of emotion recognition are explained in the Guidelines on prohibited AI practices. The feedback given in this consultation should therefore be **strictly limited to the use of such systems that are not prohibited** pursuant to Article 5 AI Act or to questions regarding the delimitation between the prohibited use of such AI systems or their classification as high-risk.

Point 1 of Annex III to the AI Act distinguishes between three different types of biometrics use cases that are classified as high-risk. All three of them are based on biometric data, i.e. personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics, like the shape of the face, voice or gait:

- Point 1(a) of Annex III to the AI Act refers to the use of remote biometric identification systems. These systems aim at the remote (at a distance, without the active participation of the person in question) automated recognition of a natural person, for the purpose of establishing the identity of that person,

by comparing the biometric data of that individual to biometric data of individuals stored in a database. Verification and authentication, used for the confirmation of the identity of a natural person, are not considered to be high-risk AI systems performing biometric categorisation may fall under the scope of prohibited systems if they fulfil the cumulative conditions defined in Article 5(1)(g) AI Act which are further developed in Section 8 of the Commission Guidelines on prohibited AI practices.

- *Point 1(b) of Annex III to the AI Act refers to the use of biometric categorisation AI systems that are categorising natural persons according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics, unless the categorisation is ancillary to another commercial service and strictly necessary for objective technical reasons (Article 3(40) AI Act). According to recital 54, AI systems intended to be used for biometric categorisation according to sensitive attributes or characteristics are those attributes and characteristics protected under Article 9 (1) of Regulation (EU) 2016/679. AI systems performing biometric categorisation may fall under the scope of prohibited systems if they fulfil the cumulative conditions defined in Article 5(1)(g) which are further developed in Section 8 of the Commission Guidelines on prohibited AI practices.*
- *Point 1(c) of Annex III to the AI Act refers to the use of emotion recognition systems. These are AI systems for identifying or inferring emotions or intentions of natural persons on the basis of their biometric data. As clarified in recital 18 AI Act, emotion recognition includes for example emotions such as happiness, sadness, or anger. It explicitly excludes the recognition of physical states such as pain or fatigue. AI systems intended to perform emotion recognition may fall under the scope of prohibited systems if they fulfil conditions defined in Article 5(1)(f) AI Act, which are further developed in Section 7 of the Commission Guidelines on prohibited AI practices.*

Question 7. Please provide practical examples of AI systems that in your opinion may fall within the scope of high-risk AI systems related to biometrics.

Examples may include systems for which you have uncertainties or system that you consider should not be considered high-risk as they are outside the use cases listed in Annex III or they fulfil one or more of the conditions for the exceptions in Article 6(3) AI Act.

	Name and description of the system	Category of biometric system	The system is considered high-risk	Motivate your previous answer	The AI system performs profiling of natural person	The AI system meets at least one of the exception criteria of Article 6(3)	Motivate your previous answer and specify any exception criteria that it meets, if applicable
1	<i>Name/description</i> AI software to detect crimes, by company Oddity.ai (AI camera surveillance to detect ‘violent behaviour’ at platforms or other public spaces, software is used in multiple Dutch cities) Steden experimenteren met slimme camera's die alarm slaan bij geweld - https://www.rtl.nl/nieuws/tech/artikel/5452108/steden-experimenteren-met-slimme-cameras	<i>Category</i> Biometric categorisation (Point 1 (b))	<i>High-risk</i> Yes, completely	<i>Explain</i> Since Oddity.ai’s system uses camera surveillance to infer violent or aggressive behavior, presumably from body posture, gestures, and movement, it should be classified as a high-risk AI system under the AI Act because this constitutes behavioral biometric analysis, even if no facial recognition is used. This classification is required under Annex III 1(b) based on both functional use and the serious risks it poses to fundamental rights, as protected by the Charter of Fundamental Rights (CFR) and the General Data Protection Regulation (GDPR). For example, the use of this system carries a serious risk of interference with articles 7, 8, 11, 12 and 21 of the CFR. Its use could also potentially trigger obligations under the GDPR, especially Articles 6, 9, 13–14, 22, and 35. Further, use of this system could amount to mass, untargeted behavioural surveillance since it has the ability to monitor individuals in public spaces, analyse their behavior to detect “violent” acts without prior suspicion, and is deployed across multiple cities. Due to the risk to fundamental rights, this system requires strict oversight, transparency and robust safeguards. Based on information provided by the Dutch NHRI, ENNHRI submits that the classification of the system as high-risk is a minimum requirement and further restrictions or even prohibition could be warranted. As a reference, the EDPB-EDPS Joint Opinion 5/2021 recommended that AI systems for behavior analysis in public spaces should be considered incompatible with fundamental rights and called for their prohibition or strict regulation.	<i>Profiling</i> Yes	<i>Exception</i> No	<i>Explain</i> Oddity.ai’s system can be classified as performing profiling of a natural person because it automatically analyses individuals’ movements and behavior in public spaces to assess whether they are acting violently, presumably generating alerts based on these predictions. This constitutes an automated evaluation of personal traits and means that a natural person could be singled out or affected by the system’s output.
							<i>Explain</i> VSA has the potential to carry out profiling as it can automatically classify

2	<i>Name/description</i> Video surveillance cars (VSA) (with advanced Hikvision camera that has deep learning capabilities, focused on human and vehicle classification). (e.g. these cars are used by the police in the Netherlands) The Netherlands: Recording dissent: Camera surveillance at peaceful protests in the Netherlands - Amnesty International - https://www.amnesty.org/en/documents/eur35/8469/2024/en/	<i>Category</i> Remote biometric identification (Point 1 (a))	<i>High-risk</i> Yes, completely	<i>Explain</i> Based on information provided by the Dutch NHRI, ENNHRI submits that the use of Video Surveillance Cars (VSA) by Dutch police—equipped with Hikvision cameras featuring deep learning capabilities for human and vehicle classification—qualifies as a high-risk AI system under Annex III because it can use AI for real-time surveillance and classification of individuals in public spaces by law enforcement, which poses significant risks to fundamental rights, e.g. CFR art. 7, 8, 11, 12.	<i>Profiling</i> Yes	<i>Exception</i> No	individuals or vehicles using deep learning, track their behavior, movement, or presence in specific locations (e.g. protests), and use this data to support law enforcement decisions. Therefore, it is evaluating personal aspects such as identity, location, and behavior. Given its law enforcement context, scale, and fundamental rights impact, it does not meet the conditions for exemption under Annex 6 (3).
3	<i>Name/description</i> Matrice 300 Drone (for the purpose of public order, such as events and demonstrations, and supervision of water and roads) These drones are used by the Dutch police. The Netherlands: Recording dissent: Camera surveillance at peaceful protests in the Netherlands - Amnesty International - https://www.amnesty.org/en/documents/eur35/8469/2024/en/ DJI Mavic 2 Pro kopen? - https://droneland.nl/dji-mavic-2-pro DJI Matrice 300 RTK - https://droneland.nl/dji-matrice-300	<i>Category</i> Remote biometric identification (Point 1 (a))	<i>High-risk</i> Yes, completely	<i>Explain</i> Based on information provided by the Dutch NHRI, ENNHRI submits that the Matrice 300 Drone used by Dutch police for public order monitoring qualifies as a high-risk AI system, especially if equipped with AI functionalities such as real-time facial recognition, behavioral analysis, or movement tracking in publicly accessible spaces. If deployed without adequate transparency and safeguards, especially in contexts such as peaceful protests, it raises concerns under the CFR regarding the rights to privacy, data protection, freedom of assembly, and freedom of expression (art. 7, 8, 11, 12) and has already had a documented chilling effect on protest participation in the Netherlands – see linked Amnesty report.	<i>Profiling</i> Yes	<i>Exception</i> No	<i>Explain</i> The Matrice 300 drone, when used for AI-enabled surveillance of individuals in public spaces, performs profiling and must comply with the corresponding high-risk AI system obligations and data protection laws. Given its law enforcement context, scale, and fundamental rights impact, it does not meet

							the conditions for exemption under Annex 6 (3).
4	<i>Name/description</i> AFR Locate (facial recognition technology ('AFR') used by the South Wales Police Force on more than 60 occasions since May 2017 in various public settings - see Legal Challenge: Ed Bridges v South Wales Police - Liberty - https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/	<i>Category</i> Remote biometric identification (Point 1 (a))	<i>High-risk</i> Yes, completely	<i>Explain</i> Based on information provided by the British NHRI, ENNHRI submits this system to be high risk since the automated scanning of people's faces in a public setting without their consent has the potential for a violation of the right to privacy, the right to data-protection and the right to non-discrimination as protected under the GDPR and the Charter of Fundamental Rights. Moreover, it is likely that certain communities are more likely to be subject to this technology. This system could even be prohibited unless it meets strict necessity, proportionality, and legal authorisation under Article 5(1)(d) or (e) of the AI Act.	<i>Profiling</i> Yes	<i>Exception</i> No	<i>Explain</i> AFR Locate constitutes profiling under Article 3(52), as it involves automated biometric processing to identify individuals and evaluate personal aspects of their identity and movements in public spaces.
5	<i>Name/description</i> CCTV cameras in all schools in the Slovak Republic (for security purposes to collect biometric data, detect and identify faces of persons entering the school's property) Začalo sa testovanie bezpečnostných kamier na školách, Ministerstvo vnútra Slovenskej republiky - https://www.minv.sk/?tlacove-spravy&sprava=zacalo-sa-testovanie-bezpecnostnych-kamier-na-skolach	<i>Category</i> Remote biometric identification (Point 1 (a))	<i>High-risk</i> Yes, completely	<i>Explain</i> Based on information provided by the Slovakian NHRI, ENNHRI submits the system is high risk as it indiscriminately collects biometric data of all persons, including children, on the school's property via facial recognition, potentially violating rights to privacy, data protection and non-discrimination (art. 7.8 and 21 CFR), particularly given the absence of individual suspicion, consent, or proportional justification. Moreover, it may fall under Article 5(1)(d) or (h) as a prohibited practice, since such systems in educational settings pose serious risks to children's rights and freedoms. Under GDPR Articles 9(1) and 6(1)(e), processing special category biometric data for public interest requires strict necessity and appropriate safeguards, which are unlikely to be met in this context.	<i>Profiling</i> Yes	<i>Exception</i> No	<i>Explain</i> This system automatically processes biometric data to identify individuals and monitor their behavior and movements, thereby evaluating personal aspects and meeting the AI Act's definition of profiling of natural persons. It does not meet criteria for any exemptions under Article 6(3). In fact, as previously stated, it might fall under Article 5 unless an exception based on serious crime prevention,

							with strict safeguards can be demonstrated which is highly unlikely in standard school security contexts.
6	<i>Name/description</i> Planned “Smart Policing” program - Greece Scanning systems to collect fingerprints and take photos and facial scans, to compare with national and international databases. Planned to be used by police and migration authorities during stop and searches. https://homodigitalis.gr/en/posts/5381/ (and the full text of the request to the Data Protection Authority here in Greek: https://homodigitalis.gr/wp-content/uploads/2020/03/HomoDigitalis_%CE%91%CE%AF%CF%84%CE%B7%CF%83%CE%B7%CE%93%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7%CF%82_%CE%91%CE%A0%CE%94%CE%A0%CE%A7_%CE%A3%CF%8D%CE%BC%CE%B2%CE%B1%CF%83%CE%B7%CE%95%CE%9B%CE%91%CE%A3_INTRACOM_19.03.2020.pdf) https://homodigitalis.gr/en/posts/134512/Briefing of political editors and foreign press correspondents General Secretariat for Communication and Information https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights	<i>Category</i> Remote biometric identification (Point 1 (a))	<i>High-risk</i> Yes, completely	<i>Explain</i> Based on information provided by the Greek NHRI, ENNHRI submits that the Biometric identification, as foreseen in the Planned “Smart Policing” program, even when conducted in a non-remote setting (i.e. systems used against individuals, not at a distance) , can have serious fundamental rights implications, potentially violating rights to privacy, data protection and non-discrimination (art. 7.8 and 21 CFR). These systems are intended to include hand-held facial image, fingerprint or palm scanners, voice or iris identification technology and, depending on the context of use, they could lead to discrimination, surveillance or coercion of the person the system is used against.	<i>Profiling</i> Yes	<i>Exception</i> No	<i>Explain</i> To ensure regulatory consistency with the GDPR, it is vital that certain AI systems which process biometric data are considered high risk. ENNHRI submits that the Greek “Smart Policing” program cannot be exempted under Annex VI(3) because it poses significant risks to fundamental rights, is intended for broad and systematic deployment, and there are concerns that it lacks publicly available safeguards or oversight mechanisms.
7	<i>Name/description</i>	<i>Category</i> ☒ Remote biometric identification (Point 1 (a)) ☒ Biometric categorisation (Point 1(b)) ☐	<i>High-risk</i> ☒ Yes, completely ☐ Partially ☐ No ☐ Unsure	<i>Explain</i>	<i>Profiling</i> ☒ Yes ☐ No ☐ Unsure	<i>Exception</i> ☐ Yes ☐ No ☐ Unsure	<i>Explain</i>

		Emotion recognition (Point 1(c))					
8	Name/description	<i>Category</i> ☐ Remote biometric identification (Point 1 (a)) ☐ Biometric categorisation (Point 1(b)) ☐ Emotion recognition (Point 1(c))	<i>High-risk</i> ☐ Yes, completely ☐ Partially ☐ No ☐ Unsure	<i>Explain</i>		<i>Profiling</i> ☐ Yes ☐ No ☐ Unsure	<i>Exception</i> ☐ Yes ☐ No ☐ Unsure <i>Explain</i>
9	Name/description	<i>Category</i> ☐ Remote biometric identification (Point 1 (a)) ☐ Biometric categorisation (Point 1(b)) ☐ Emotion recognition (Point 1(c))	<i>High-risk</i> ☐ Yes, completely ☐ Partially ☐ No ☐ Unsure	<i>Explain</i>		<i>Profiling</i> ☐ Yes ☐ No ☐ Unsure	<i>Exception</i> ☐ Yes ☐ No ☐ Unsure <i>Explain</i>
10	Name/description	<i>Category</i> ☐ Remote biometric identification (Point 1 (a)) ☐ Biometric categorisation (Point 1(b)) ☐ Emotion recognition (Point 1(c))	<i>High-risk</i> ☐ Yes, completely ☐ Partially ☐ No ☐ Unsure	<i>Explain</i>		<i>Profiling</i> ☐ Yes ☐ No ☐ Unsure	<i>Exception</i> ☐ Yes ☐ No ☐ Unsure <i>Explain</i>

Question 8. Do you have or know practical examples of AI systems related to biometrics where you need further clarification regarding the **distinction from prohibited AI systems**?

	Name and description of the system	Category of biometric system	Category of prohibited AI system with which there may be an interplay	Motivate your previous answer
1	<i>Name/description</i> Dialect Identification Assistance System – (DIAS) used in Germany ENNHRI Scoping paper on new technologies at the borders - https://ennhri.org/wp-content/uploads/2024/09/Technologies-migration-and-human-rights-the-role-of-European-NHRIs-an-ENNHRI-scoping-paper.pdf	<i>Category</i> Biometric categorisation (Point 1 (b))	<i>Category</i> Biometric categorisation system (Art. 5(1)(g))	<i>Explain</i> Based on information by the German NHRI, DIAS is used by the German Federal Office for Migration and Refugees to determine countries or regions of origin, in cases where the individual concerned does not have identification documents. The tool records speech and relies on open source linguistic data to produce a result providing a percentage breakdown of the dialect of the person concerned. The voice data qualifies as biometric data, and by assigning the person to a country of origin, can also infer ethnicity. An overreliance on results generated by DIAS and similar technologies can also contravene an individual's rights. Many voice recognition and dialect identification tools remain in the early stages of development. At the same time, the accuracy of these technologies is questionable. The determination of an individual's place of origin is complex and it is difficult for software to draw such conclusions based on dialect, a characteristic which can be altered based on an individuals' surroundings. While these technologies may be a support tool for authorities, they should not be the sole basis for a decision. In this regard, the GDPR forbids any authority to take decisions solely based on an automated decision-making algorithm, including those like DIAS.
2	<i>Name/description</i> Paris Olympics RBI	<i>Category</i> Remote biometric identification (Point 1 (a))	<i>Category</i> Real time remote biometric identification system (Art. 5(1)(h))	<i>Explain</i> Based on information provided by the French NHRI, since 2023, the government of France has been 'piloting' algorithmic video surveillance in ways which would likely be a contradiction of Articles 7 and 8 of the Charter of Fundamental Rights. These systems are harmful and infringe on people's fundamental rights to such an extent that it is not apparent which safeguards would prevent fundamental rights violations and make their use acceptable in a democratic, rule-of-law-respecting society.
		<i>Category</i> ☐ Remote biometric identification (Point 1 (a))	<i>Category</i> ☐ Real time remote biometric identification system (Art. 5(1)(h)) ☐	

3	<i>Name/description</i>	Biometric categorisation (Point 1(b)) ☐ Emotion recognition (Point 1(c))	Biometric categorisation system (Art. 5(1)(g)) ☐ Emotion inference system (Art. 5(1)(f)) ☐ Other ☐ Unsure	<i>Explain</i>
4	<i>Name/description</i>	<i>Category</i> ☐ Remote biometric identification (Point 1(a)) ☐ Biometric categorisation (Point 1(b)) ☐ Emotion recognition (Point 1(c))	<i>Category</i> ☐ Real time remote biometric identification system (Art. 5(1)(h)) ☐ Biometric categorisation system (Art. 5(1)(g)) ☐ Emotion inference system (Art. 5(1)(f)) ☐ Other ☐ Unsure	<i>Explain</i>
5	<i>Name/description</i>	<i>Category</i> ☐ Remote biometric identification (Point 1(a)) ☐ Biometric categorisation (Point 1(b)) ☐ Emotion recognition (Point 1(c))	<i>Category</i> ☐ Real time remote biometric identification system (Art. 5(1)(h)) ☐ Biometric categorisation system (Art. 5(1)(g)) ☐ Emotion inference system (Art. 5(1)(f)) ☐ Other ☐ Unsure	<i>Explain</i>

Question 9. If you see the need for clarification of the high-risk classification in Point 1 of Annex III to the AI Act and its **interplay with other Union or national legislation**, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay

1500 character(s) maximum

ENNHRI seeks clarification of the high-risk classification in Point 1 of Annex III to the AI Act, preferably in the form of guidelines, regarding the transparency obligations which arise from other legal frameworks. These include GDPR Articles 13 and 14, the Law Enforcement Directive (LED), and national Freedom of Information laws. Finally, clarification is sought on how high-risk systems under Annex III of the AI Act align with Articles 22 and 15(1)(h) GDPR, particularly following the CJEU's CK v Dun & Bradstreet Austria (C-203/22) ruling.

2.C. Questions in relation to education and vocational training (Annex III, point 3)

Point 3 of Annex III to the AI Act includes four use-cases for AI systems in the area of education and vocational training that are classified as high-risk. In more detail:

- *Point 3(a) of Annex III to the AI Act refers to AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels.*
- *Point 3(b) of Annex III to the AI Act refers to AI systems intended to be used to evaluate learning outcomes, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels.*
- *Point 3(c) of Annex III to the AI Act refers to AI systems intended to be used for the purpose of assessing the appropriate level of education that an individual will receive or will be able to access, in the context of or within educational and vocational training institutions at all levels.*
- *Point 3(d) of Annex III to the AI Act refers to AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels.*

Question 14. Please provide practical examples of AI systems that in your opinion may fall within the scope of high-risk AI systems related to education and vocational training.

Examples may include systems for which you have uncertainties or system that you consider should not be considered high-risk as they are outside the use cases listed in Annex III or they fulfil one or more of the conditions for the exceptions in Article 6(3).

Name/description

Proctorio (anti-cheating software system, using AI-based algorithm to automatically flag suspicious behaviour) 3e2a9e5b2fad237a3d35f36fa2c5f44552f2.pdf <https://oordelen.mensenrechten.nl/oordeel/2022-146> (interim verdict ruling a reasonable suspicion of discrimination) <https://oordelen.mensenrechten.nl/oordeel/2023-111> (final verdict ruling no discrimination in this specific case, but with a high risk of discrimination by the system)

Category

Monitoring test
behaviour (Point 3
(d))

High-risk

Yes, completely

Explain Based on information provided by the Dutch NHRI, ENNHRI submits that the classification of this system should be high-risk. This system demonstrated risks to Article 7 – the respect for privacy since it needed to be granted access to webcams, microphones and internet use. The student was required to use Google Chrome, which auto-filled many areas of the form, including those with ‘sensitive information’. There were risks to Article 8, the protection of personal data, in that the data the system gathered would be shared with the university. The potential was present for violations of Article 21, the right to non-discrimination, in that the requirement for facial recognition has a record of failing to register non-white faces and consequently failing to validate students’ identities.

Profiling

Yes

Exception

No

Explain Proctorio qualifies as profiling under the AI Act because it automatically processes students’ personal behavioral data to evaluate and flag their exam conduct. Proctorio cannot be exempted as it poses significant risks to students’ fundamental rights, including privacy, non-discrimination, and data protection.

Name/description

Category

- ☒ Access
/admission to
education (Point
3(a))
- ☒ Evaluating
learning
outcomes (Point
3(b))
- ☐

High-risk

- ☒ Yes, completely
- ☐ Partially
- ☐ No
- ☐ Unsure

Explain

Profiling

- ☐ Yes
- ☐ No
- ☐ Unsure

Exception

- ☐ Yes
- ☐ No
- ☐ Unsure

Explain

Name/description	Category	High-risk	Explain
Assessing education levels (Point 3(c))			
Monitoring test behaviour (Point 3(d))			
	Access /admission to education (Point 3(a))		
	Evaluating learning outcomes (Point 3(b))	Yes, completely	
		Partially	
		No	
	Assessing education levels (Point 3(c))	Unsure	
	Monitoring test behaviour (Point 3(d))		
	Category		
	Access /admission to education (Point 3(a))		
	Evaluating learning outcomes (Point 3(b))	High-risk	
		Yes, completely	
		Partially	
		No	

<i>Profiling</i> ☐ Yes ☐ No ☐ Unsure	<i>Exception</i> ☐ Yes ☐ No ☐ Unsure	<i>Explain</i>
<i>Profiling</i> ☐ Yes ☐ No ☐ Unsure	<i>Exception</i> ☐ Yes ☐ No ☐ Unsure	<i>Explain</i>

Name/description

Assessing education levels (Point 3(c))

Monitoring test behaviour (Point 3(d))

Category

Access /admission to education (Point 3(a))

Evaluating learning outcomes (Point 3(b))

Assessing education levels (Point 3(c))

Monitoring test behaviour (Point 3(d))

High-risk

Yes, completely

Partially

No

Unsure

Explain

Name/description

Category

Access /admission to education (Point 3(a))

Evaluating learning outcomes (Point 3(b))

High-risk

Yes, completely

Partially

No

Explain

Profiling

Yes

No

Unsure

Exception

Yes

No

Unsure

Explain

Profiling

Yes

No

Unsure

Exception

Yes

No

Unsure

Explain

19

Name/description

Name/description

Assessing education levels (Point 3(c))	☐ Unsure	
☐ Monitoring test behaviour (Point 3(d))		
Category		
☐ Access /admission to education (Point 3(a))		
☐ Evaluating learning outcomes (Point 3(b))	High-risk	Explain
☐ Assessing education levels (Point 3(c))	☐ Yes, completely	
☐ Monitoring test behaviour (Point 3(d))	☐ Partially	
	☐ No	
	☐ Unsure	
Category		
☐ Access /admission to education (Point 3(a))		
☐ Evaluating learning outcomes (Point 3(b))	High-risk	Explain
☐	☐ Yes, completely	
	☐ Partially	
	☐ No	

Profiling	Exception	Explain
☐ Yes	☐ Yes	
☐ No	☐ No	
☐ Unsure	☐ Unsure	
Profiling	Exception	Explain
☐ Yes	☐ Yes	
☐ No	☐ No	
☐ Unsure	☐ Unsure	

Name/description

Name/description

Assessing education levels (Point 3(c))	☐ Unsure	
☐ Monitoring test behaviour (Point 3(d))		
Category		
☐ Access /admission to education (Point 3(a))		
☐ Evaluating learning outcomes (Point 3(b))	High-risk	Explain
☐ Assessing education levels (Point 3(c))	☐ Yes, completely	
☐ Monitoring test behaviour (Point 3(d))	☐ Partially	
	☐ No	
	☐ Unsure	
Category		
☐ Access /admission to education (Point 3(a))		
☐ Evaluating learning outcomes (Point 3(b))	High-risk	Explain
☐	☐ Yes, completely	
	☐ Partially	
	☐ No	

Profiling	Exception	Explain
☐ Yes	☐ Yes	
☐ No	☐ No	
☐ Unsure	☐ Unsure	
Profiling	Exception	Explain
☐ Yes	☐ Yes	
☐ No	☐ No	
☐ Unsure	☐ Unsure	

- ☐ Assessing education levels (Point 3(c))
- ☒ Monitoring test behaviour (Point 3(d))
- ☐ Unsure

Question 15. If you have or know practical examples of AI systems related to education and vocational training for which you need further clarification regarding the **distinction from prohibited AI systems**, please specify which category of AI system is concerned.

1500 character(s) maximum

Question 16. If you see the need for clarification of the high-risk classification in *Point 3 of Annex III to the AI Act* and its **interplay with other Union or national legislation**, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay

1500 character(s) maximum

2.E. Questions in relation to the access to and enjoyment of essential private services and essential public services and benefits (Annex III, point 5)

The classification of AI systems as high-risk under Annex III point 5 AI Act targets AI systems which are intended to be used in different contexts of access to and enjoyment of essential private services and essential public services and benefits. According to recital 58, these are generally services necessary for people to fully participate in society or to improve one's standard of living. In particular, natural persons applying for or receiving essential public assistance benefits and services from public authorities namely healthcare services, social security benefits, social services providing protection in cases such as maternity, illness, industrial accidents, dependency or old age and loss of employment and social and housing assistance, are typically dependent on those benefits and services and in a vulnerable position in relation to the responsible authorities.

Point 5 of Annex III to the AI Act distinguishes between four different types of use cases that are classified as high-risk in the area of the access to and enjoyment of services and benefits.

Point 5(a) of Annex III to the AI Act refers to AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services.

Point 5(b) of Annex III to the AI Act refers to AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud. According to recital 58, AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under the AI Act. Point 5(b) of Annex III therefore contains two distinct use cases:

1. *AI systems intended to be used to evaluate the creditworthiness of natural persons.*
2. *AI systems intended to be used to establish their credit score.*

Point 5(c) of Annex III to the AI Act refers to AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance. According to recital 58, AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under the AI Act.

Point 5(d) of Annex III to the AI Act refers to AI systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of, emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems. Point 5(d) of Annex III therefore contains four distinct use cases:

1. *AI systems intended to evaluate and classify emergency calls by natural persons.*
2. *AI systems intended to be used to dispatch emergency first response services, including by police, firefighters and medical aid.*
3. *AI systems intended to be used to establish priority in the dispatching of emergency first response services, including by police, firefighters and medical aid.*
4. *AI systems intended to be used as emergency healthcare patient triage systems*

Question 20. Please provide practical examples of AI systems that in your opinion may fall within the scope of high-risk AI systems related to essential private services and essential public services and benefits.

Examples may include systems for which you have uncertainties or system that you consider should not be considered high-risk as they are outside the use cases listed in Annex III or they fulfil one or more of the conditions for the exceptions in Article 6(3) AI Act.

	Name and description of the system	Category of AI system	The system is considered high-risk	Motivate your previous answer	The AI system performs profiling of natural person	The AI system meets at least one of the exception criteria of Article 6(3)	Motivate your previous answer and specify any exception criteria that it meets, if applicable
1	<i>Name/description</i> Childcare benefits scandal in the Netherlands (tax authorities using data and algorithms to assess applications for childcare allowance for potential inaccuracies and possible fraud, using nationality as a criterium) Amnesty International rapport "Xenophobic machines - https://www.amnesty.nl/wat-we-doen/tech-en-mensenrechten/algorithmes-big-data-overheid	<i>Category</i> Evaluation of eligibility for public assistance benefits and services (Point 5(a))	<i>High-risk</i> No	<i>Explain</i> The Dutch childcare benefits assessment system is a set of algorithms that cannot strictly speaking be classified as an AI system. Based on information supplied by the Dutch NHRI, ENNHRI submits that, it is, however, a strong example of what can go wrong in the large scale automation of welfare systems. Since it automates access to essential social services using discriminatory criteria, it poses significant risks to fundamental rights. It uses sensitive personal data, including nationality, raising serious discrimination and fundamental rights concerns. The automated fraud detection impacts rights to non-discrimination (Article 21, EU Charter), social security (Article 34), and good administration (Article 41).	<i>Profiling</i> Yes	<i>Exception</i> No	<i>Explain</i> The childcare benefits system profiles individuals by automatically analysing their personal data, including nationality, to assess eligibility and detect potential fraud. The system cannot strictly be classified as an AI-system, however, similar assessment systems that could be classed in such a manner could not be exempted because of high risks to transparency and significant risks to fundamental rights, including discrimination and unfair denial of essential social services.
2	<i>Name/description</i> SCHUFA in Germany (private company collecting data of financial history and uses this to calculate the SCHUFA score, companies check this score when one applies for a new phone, credit card, internet contract, or when renting an apartment) AlgorithmWatch onderzoek OpenSCHUFA - https://algorithmwatch.org/en/openschufa-shedding-light-on-germanys-opaque-credit-scoring-2/	<i>Category</i> Evaluation of creditworthiness/ credit score of natural persons (Point 5(b))	<i>High-risk</i> Yes, completely	<i>Explain</i> Based on information provided by the German NHRI, ENNHRI submits that SCHUFA's credit scoring system is a high-risk AI system because it automatically assesses individuals' financial reliability, affecting access to essential private services like credit, housing, and utilities, which directly impact fundamental rights.	<i>Profiling</i> Yes	<i>Exception</i> No	<i>Explain</i> The system profiles natural persons as it assesses personal aspects such as reliability, risk, and financial behavior and automatically processes their personal financial and behavioral data to evaluate individuals' creditworthiness. It cannot be exempted due to its significant impact on fundamental rights and the sensitive nature of the data processed.
		<i>Category</i> ☒ Evaluation of eligibility for public					

3	Name/description	assistance benefits and services (Point 5 (a)) ☐ Evaluation of creditworthiness/ credit score of natural persons (Point 5(b)) ☐ Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) ☐ Evaluation and classification of emergency calls (Point 5(d))	High-risk ☐ Yes, completely ☐ Partially ☐ No ☐ Unsure
---	------------------	--	--

		relation to natural persons for life /health insurance (Point 5(c)) ☐ Evaluation and classification of emergency calls (Point 5(d))						
5	Name/description	Category ☐ Evaluation of eligibility for public assistance benefits and services (Point 5(a)) ☐ Evaluation of creditworthiness/ credit score of natural persons (Point 5(b)) ☐ Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) ☐ Evaluation and classification of emergency calls (Point 5(d))	High-risk ☐ Yes, completely ☐ Partially ☐ No ☐ Unsure	Explain		Profiling ☐ Yes ☐ No ☐ Unsure	Exception ☐ Yes ☐ No ☐ Unsure	Explain
		Category ☐						

6	Name/description	Evaluation of eligibility for public assistance benefits and services (Point 5 (a)) ☐ Evaluation of creditworthiness/ credit score of natural persons (Point 5(b)) ☐ Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) ☐ Evaluation and classification of emergency calls (Point 5(d))	High-risk ☐ Yes, completely ☐ Partially ☐ No ☐ Unsure
---	------------------	--	--

		☐ Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) ☐ Evaluation and classification of emergency calls (Point 5(d))	☐ No ☐ Unsure			☐ No ☐ Unsure	☐ No ☐ Unsure	
8	Name/description	Category ☐ Evaluation of eligibility for public assistance benefits and services (Point 5 (a)) ☐ Evaluation of creditworthiness/ credit score of natural persons (Point 5(b)) ☐ Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) ☐ Evaluation and classification of emergency calls (Point 5(d))	High-risk ☐ Yes, completely ☐ Partially ☐ No ☐ Unsure					

9	Name/description	Category ☐ Evaluation of eligibility for public assistance benefits and services (Point 5(a)) ☐ Evaluation of creditworthiness/ credit score of natural persons (Point 5(b)) ☐ Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) ☐ Evaluation and classification of emergency calls (Point 5(d))	High-risk ☐ Yes, completely ☐ Partially ☐ No ☐ Unsure	Explain	Profiling ☐ Yes ☐ No ☐ Unsure	Exception ☐ Yes ☐ No ☐ Unsure	Explain
		Category ☐ Evaluation of eligibility for public assistance benefits and services (Point 5(a)) ☐ Evaluation of creditworthiness/	High-risk				

10	Name/description	credit score of natural persons (Point 5(b)) ☐ Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) ☐ Evaluation and classification of emergency calls (Point 5(d))	☐ Yes, completely ☐ Partially ☐ No ☐ Unsure	Explain		Profiling ☐ Yes ☐ No ☐ Unsure	Exception ☐ Yes ☐ No ☐ Unsure	Explain
----	------------------	--	--	---------	--	--	--	---------

Question 21. If you have or know practical examples of AI systems related to essential private services and essential public services and benefits where you need further clarification regarding the **distinction from prohibited AI systems**, in particular Art. 5(1)(c) AI Act, please specify

ENNHRI seeks clarification of the distinction between the above mentioned high risk AI systems and prohibited AI systems under Art. 5 (1)(c). There is a lot of evidence demonstrating that AI systems used in the context of access to and enjoyment of essential services, including public benefits and services often leads to discrimination, surveillance and further marginalisation of beneficiaries of those services. Prominent cases in the EU include the Dutch child benefits risk-profiling system (<https://shorturl.at/zwyl4>). As highlighted in the examples above, AI Act guidelines should reflect the state of play in Europe and clarify that risk of profiling and fraud detection systems, could be seen as amounting to social scoring <https://tinyurl.com/yn36vb4r> which would make them prohibited systems. Given this, AI systems influencing decisions on people's access to essential services and benefits should be considered under the social scoring ban, unless, by case-by-case assessment, deployers can prove that their systems do not lead to social scoring and meaningful safeguards guaranteeing the right to non-discrimination, equality, privacy, data protection, social protection and other socio-economic rights are in place.

Question 22. Do you see the need for clarification of one of the various use cases of high-risk classification in *Point 5 of Annex III to the AI Act* and its **interplay with other Union or national legislation**, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay
1500 character(s) maximum

In terms of Union legislation, the assessment should consider EU equality, data protection, and consumer rights law, which are underpinned by the Charter of Fundamental Rights. While AI Act guidelines should clarify that certain AI systems in the context of access to and enjoyment of essential services and benefits might amount to social scoring, some of these have already been challenged on the ground of non-discrimination law.

Question 23. Do you have or know practical examples of AI systems that could fall under the **exception** mentioned in *Point 5 of Annex III to the AI Act* and *recital 58 AI Act*?

	Name and description of the system	Category of exception	Please motivate your answer
1	Name/description	<i>Category</i> ☐ Exception of being intended for the purpose of detecting financial fraud (Point 5(b)) ☐ Exception of being intended for the purpose of detecting fraud in the offering of financial services or for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements (recital 58)	<i>Explain</i>
2	Name/description	<i>Category</i> ☐ Exception of being intended for the purpose of detecting financial fraud (Point 5(b)) ☐ Exception of being intended for the purpose of detecting fraud in the offering of financial services or for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements (recital 58)	<i>Explain</i>
3	Name/description	<i>Category</i> ☐ Exception of being intended for the purpose of detecting financial fraud (Point 5(b)) ☐ Exception of being intended for the purpose of detecting fraud in the offering of financial services or for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements (recital 58)	<i>Explain</i>
4	Name/description	<i>Category</i> ☐ Exception of being intended for the purpose of detecting financial fraud (Point 5(b)) ☐ Exception of being intended for the purpose of detecting fraud in the offering of financial services or for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements (recital 58)	<i>Explain</i>
5	Name/description	<i>Category</i> ☐ Exception of being intended for the purpose of detecting financial fraud (Point 5(b)) ☐ Exception of being intended for the purpose of detecting fraud in the offering of financial services or for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements (recital 58)	<i>Explain</i>

2.F Questions in relation to law enforcement (Annex III, point 6)

The classification of AI systems as high-risk under Annex III point 6 AI Act targets AI systems which are intended to be used in law enforcement (as defined in Art. 3(46) AI Act), in so far as their use is permitted under relevant Union or national law.

Point 6 of Annex III to the AI Act provides five use cases in the context of law enforcement in which AI systems are classified as high-risk.

- *Point 6(a) of Annex III to the AI Act refers to AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf to assess the risk of a natural person becoming the victim of criminal offences.*
- *Point 6(b) of Annex III to the AI Act refers to AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities as polygraphs or similar tools.*
- *Point 6(c) of Annex III to the AI Act refers to AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies, in support of law enforcement authorities to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences.*
- *Point 6(d) of Annex III to the AI Act classifies as high-risk AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies, in support of law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 (profiling is defined as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements), or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups. By contrast, AI systems based solely on profiling and assessment of personality traits and characteristics are prohibited under article 5(1)(d) AI Act.*

- *Point 6(e) of Annex III to the AI Act refers to AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 (defined as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements) in the course of the detection, investigation or prosecution of criminal offences.*

Question 24. Please provide practical examples of AI systems that in your opinion may fall within the scope of high-risk AI systems listed in the area of law enforcement in Annex III.

Examples may include systems for which you have uncertainties or system that you consider should not be considered high-risk as they are outside the use cases listed in Annex III or they fulfil one or more of the conditions for the exceptions in Article 6(3) AI Act.

Name/description

Criminaliteits Anticipatie Systeem (CAS) (location-based predictive policing, algorithm uses historical crime data and specific characteristics of a neighbourhood to produce a digital map that shows area's that have an increased risk of high impact crimes) Criminaliteits Anticipatie Systeem (CAS) - Politie - <https://algoritmes.overheid.nl/nl/algoritme/oorg10264/81228922/criminaliteits-anticipatie-systeem-cas> Algoritmes getoetst | Rapport | Algemene Rekenkamer - <https://www.rekenkamer.nl/publicaties/rapporten/2022/05/18/algoritmes-getoetst>

Category

Assessing re-offending risk in law enforcements (Point 6(d))

High-risk

Yes, completely

Explain Based on information provided by the Dutch NHRI, ENNHRI submits that CAS is a high risk system as it influences police resource allocation and interventions, raising concerns about discriminatory impacts, over-policing, and bias based on historical data patterns. Further, it may indirectly affect individuals' rights through increased surveillance or policing of specific communities, especially when tied to socioeconomic or demographic patterns.

Profiling

Unsure

Exception

No

Explain While CAS does not explicitly profile natural persons, its use in law enforcement targeting based on location-linked patterns could result in indirect profiling. ENNHRI believes that the CAS cannot be exempted since it is used by law enforcement to anticipate crime locations, which affects policing strategies and resource allocation i.e. areas with higher predicted crime may face more surveillance or interventions. This creates serious risks of discrimination, bias, and stigmatisation, especially for marginalised communities, based on historical and potentially biased crime data. This creates serious risks to fundamental rights, including to privacy, equality, and non-discrimination (CFR, Articles 7, 8, and 21).

Name/description

Top400 crime prevention programme (identifying and disciplining the 400 most at risk youth for criminality in the city through a ProKid+ algorithm) <https://openresearch.amsterdam/nl/page/93293/meerjarenplan-aanpak-top600-en-top400-2023-2026> <https://piip.nu/dossier/top400/>, <https://www.bitsoffreedom.nl/2022/11/14/mensenrechten-in-het-gedrang-door-de-top400/> <https://controlealtdedelete.nl/articles/top400-aanpak-is-discriminerend#gsc.tab=0>

Category

Assessing re-offending risk in law enforcements (Point 6(d))

High-risk

Unsure

Explain Based on information provided by the Dutch NHRI, ENNHRI submits that the Top400 programme could be potentially classified as a high-risk AI system as it uses predictive algorithms for individual risk assessments by law enforcement, posing serious risks to fundamental rights including privacy, non-discrimination, and due process – e.g. risks to privacy, non-discrimination, presumption of innocence, and child protection under Articles 7, 8, 21, 48, and 24 CFR. However, it is unclear to what extent the Prokid+ algorithm is an AI system or not.

Profiling

Yes

Exception

No

Explain The ProKid+ algorithm processes personal data (e.g., school attendance, family history, police contacts) to predict a child's future risk of criminality. This constitutes automated analysis of behaviour and personal characteristics, meaning it conducts profiling. The system (if classified as an AI-system) cannot be exempted because it poses significant risks to fundamental rights and is used in a broad,

Name/description

Sensing-project (mass surveillance using cameras and other sensors to monitor people driving around, movement patterns and information about vehicles. This data is processed into an algorithmic model that calculates a risk score for each vehicle. www.amnesty.nl/actueel/nederland-maak-een-einde-aan-gevaarlijke-politie-experimenten-met-massasurveillance

Category

Assessing re-offending risk in law enforcements (Point 6(d))

High-risk

Yes, completely

Explain Based on information provided by the Dutch NHRI, ENNHRI submits that the Sensing-project is a high-risk AI system as it evaluates the trustworthiness of individuals based on behavioural data and risk scores through monitoring and analysing movement patterns and information about vehicles. This raises serious fundamental rights concerns, including Art. 7 (Respect for private life), Art. 8 (Protection of personal data), Art. 21 (Non-discrimination) and potentially Art. 22 (Right to freedom of movement) under the Charter.

Profiling

Yes

Exception

No

systematic manner that directly impacts individuals, particularly children.

Explain The Sensing-project is likely profiling because it systematically collects and analyses data on individual movements and behaviours to assign a risk score, which constitutes automated processing to evaluate personal aspects such as behaviour, likely intentions, or trustworthiness. It should not be exempted because it involves systematic, widespread surveillance and behavioural risk assessment by public authorities, posing significant fundamental rights risks apparently without clear safeguards or narrowly tailored exceptions.

Name/description

CATCH (Centrale Automatische TeChnologie voor Herkenning van personen), a facial recognition technology used by the Dutch police. In English, CATCH stands for Central Automatic Technology for Recognition of Persons and the system is used in the Center for Biometrics in Zoetermeer. There is a database with criminal law images – photos that police officers take of arrested suspects and convicts – and one for images of foreigners. If bystanders or victims have taken images of, for example, scammers at the door or a street assault, these can be compared with the photos in CATCH.) Fors meer gezichtsvergelijkingen voor opsporing in 2023 | politie.nl - <https://www.politie.nl/nieuws/2024/november/19/fors-meer-succesvolle-gezichtsvergelijkingen-voor-opsporing-in-2023.html>

Category

Profiling individuals in criminal investigations (Point 6(e))

High-risk

Yes, completely

Explain Based on information provided by the Dutch NHRI, ENNHRI submits that the use of facial recognition technology by law enforcement Decision-making by AI system interferes with fundamental rights (art. 6, 7, 8), therefore requires oversight and strict safety and ethical standards. Further it has the potential to violate data protection rights under GDPR.

Profiling

Yes

Exception

No

Explain This system has the clear potential for breaching fundamental rights and can be used for profiling natural persons. Therefore, it does not meet the criteria for exemption under Annex 3 since an AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons.

Name/description

Facial recognition System “Gesichtserkennungssystem (GES)” used by the German Federal Criminal Police Office (BKA) GES is a central system that searches the BKA’s electronic police information system, INPOL, for matches to facial images. The GES aims to solve crimes and verify the identity of asylum seekers by comparing images from various sources, including police identification procedures, cell phone photos, and video camera recordings. <https://digit.site36.net/2018/08/15/g20-in-hamburg-data-protection-commissioner-considers-face-recognition-illegal/> <https://www.heise.de/en/news/Gesichtserkennung-BKA-nutzte-Millionen-Polizeifotos-fuer-Test-9714197.html> <https://digit.site36.net/2024/12/16/new-police-technology-in-germany-unleashed-facial-recognition-takes-off/>

Category

Profiling individuals in criminal investigations (Point 6(e))

High-risk

Yes, completely

Explain Based on information provided by the German NHRI, ENNHRI submits that GES is a high-risk system as it is used by German federal police (BKA), to process biometric facial data from multiple sources (e.g. CCTV, phones) to match individuals against criminal databases (INPOL), supporting post-event investigations like G20 Hamburg and involving automated evaluation of identity, behavior, and movement—constituting profiling under Article 3(52) of the AI Act. Further, given its use, it could also be classified under Annex III, Point 1(a) – for remote biometric identification in public spaces. The system presents significant risks to fundamental rights, including Article 7 CFR privacy, Article 8 CFR data protection and Art 21 Non-discrimination, as well as to Art. 9 GDPR – Biometric data as a special category and Art. 22 GDPR – Automated decision-making and profiling.

Profiling

Yes

Exception

No

Explain This system has the clear potential for breaching fundamental rights and can be used for profiling natural persons. Therefore, it does not meet the criteria for exemption under Annex 3 since an AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons.

Name/description

Category

☐ Assessing victim
risk in law
enforcement
(Point 6(a))

☐ Polygraph use in
law enforcement
(Point 6(b))

☐ Evaluating of
evidence
reliability in
investigations
(Point 6(c))

☐ Assessing re-
offending risk in
law
enforcements
(Point 6(d))

☐ Profiling
individuals in
criminal
investigations
(Point 6(e))

Category

☐ Assessing victim
risk in law
enforcement
(Point 6(a))

☐ Polygraph use in
law enforcement
(Point 6(b))

High-risk

- ☐ Yes, completely
- ☐ Partially
- ☐ No
- ☐ Unsure

Explain

Profiling

- ☐ Yes
- ☐ No
- ☐ Unsure

Exception

- ☐ Yes
- ☐ No
- ☐ Unsure

Explain

Name/description

- ☐ Evaluating of evidence reliability in investigations (Point 6(c))
- ☐ Assessing re-offending risk in law enforcements (Point 6(d))
- ☐ Profiling individuals in criminal investigations (Point 6(e))
- High-risk

☐ Yes, completely

☐ Partially

☐ No

☐ Unsure

Explain

Category

- ☐ Assessing victim risk in law enforcement (Point 6(a))
- ☐ Polygraph use in law enforcement (Point 6(b))
- ☐ Evaluating of evidence reliability in investigations (Point 6(c))
- ☐ Assessing re-offending risk in law

- High-risk

☐ Yes, completely

☐ Partially

☐ No

☐ Unsure

Explain

Profiling

- ☐ Yes
- ☐ No
- ☐ Unsure

Exception

- ☐ Yes
- ☐ No
- ☐ Unsure

Explain

Name/description

Profiling

- ☐ Yes
- ☐ No
- ☐ Unsure

Exception

- ☐ Yes
- ☐ No
- ☐ Unsure

Explain

Name/description

enforcements
(Point 6(d))

☐ Profiling
individuals in
criminal
investigations
(Point 6(e))

Category

☐ Assessing victim
risk in law
enforcement
(Point 6(a))

☐ Polygraph use in
law enforcement
(Point 6(b))

☐ Evaluating of
evidence
reliability in
investigations
(Point 6(c))

☐ Assessing re-
offending risk in
law
enforcements
(Point 6(d))

☐ Profiling
individuals in
criminal
investigations
(Point 6(e))

Category

High-risk

☐ Yes, completely

☐ Partially

☐ No

☐ Unsure

Explain

Profiling

☐ Yes

☐ No

☐ Unsure

Exception

☐ Yes

☐ No

☐ Unsure

Explain

Name/description

- ☐ Assessing victim risk in law enforcement (Point 6(a))
- ☐ Polygraph use in law enforcement (Point 6(b))
- ☐ Evaluating of evidence reliability in investigations (Point 6(c))
- ☐ Assessing re-offending risk in law enforcements (Point 6(d))
- ☐ Profiling individuals in criminal investigations (Point 6(e))

High-risk

- ☐ Yes, completely
- ☐ Partially
- ☐ No
- ☐ Unsure

Explain

Profiling

- ☐ Yes
- ☐ No
- ☐ Unsure

Exception

- ☐ Yes
- ☐ No
- ☐ Unsure

Explain

Question 25. Do you have or know practical examples of AI systems listed in the area of law enforcement in Annex III where you need further clarification regarding the **distinction from prohibited AI systems**?

	Name and description of the system	Category of AI system	Category of prohibited AI system with which there may be an interplay	Please motivate your answer
1	<i>Name/description</i>	<i>Category</i> ☐ Assessing re-offending risk in law enforcements (Point 6(d)) ☐ Profiling individuals in criminal investigations (Point 6(e))	<i>Category</i> ☐ Predicting criminal behaviour (Art. 5(1)(d)) ☐ Other	<i>Explain</i>
2	<i>Name/description</i>	<i>Category</i> ☐ Assessing re-offending risk in law enforcements (Point 6(d)) ☐ Profiling individuals in criminal investigations (Point 6(e))	<i>Category</i> ☐ Predicting criminal behaviour (Art. 5(1)(d)) ☐ Other	<i>Explain</i>
3	<i>Name/description</i>	<i>Category</i> ☐ Assessing re-offending risk in law enforcements (Point 6(d)) ☐ Profiling individuals in criminal investigations (Point 6(e))	<i>Category</i> ☐ Predicting criminal behaviour (Art. 5(1)(d)) ☐ Other	<i>Explain</i>
4	<i>Name/description</i>	<i>Category</i> ☐ Assessing re-offending risk in law enforcements (Point 6(d)) ☐ Profiling individuals in criminal investigations (Point 6(e))	<i>Category</i> ☐ Predicting criminal behaviour (Art. 5(1)(d)) ☐ Other	<i>Explain</i>
5	<i>Name/description</i>	<i>Category</i> ☐ Assessing re-offending risk in law enforcements (Point 6(d)) ☐ Profiling individuals in criminal investigations (Point 6(e))	<i>Category</i> ☐ Predicting criminal behaviour (Art. 5(1)(d)) ☐ Other	<i>Explain</i>

Question 26. If you see the need for clarification of one of the various use-cases in *Point 6 of Annex III to the AI Act* and its **interplay with other Union or national legislation**, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay

1500 character(s) maximum

2.G. Questions in relation to migration, asylum and border control management (Annex III, point 7)

The classification of AI systems as high-risk under Annex III point 7 AI Act targets AI systems which are intended to be used in different contexts of migration, asylum, and border control management.

Point 7 of Annex III to the AI Act provides four use cases in the context of migration, asylum and border control management in which AI systems are classified as high-risk.

- *Point 7(a) of Annex III to the AI Act refers to AI systems intended to be used by or on behalf of competent public authorities, or by Union institutions, bodies, offices or agencies as polygraphs or similar tools.*
- *Point 7(b) of Annex III to the AI Act refers to AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assess a risk, including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State.*
- *Point 7(c) of Annex III to the AI Act refers to AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assist competent public authorities for the examination of applications for asylum, visa or residence permits and for associated complaints with regard to the eligibility of the natural persons applying for a status, including related assessments of the reliability of evidence.*
- *Point 7(d) of Annex III to the AI Act refers to AI systems intended to be used by or on behalf of competent public authorities, or by Union institutions, bodies, offices or agencies, in the context of migration, asylum or border control management, for the purpose of detecting, recognising or identifying natural persons, in the context of migration, asylum or border control management, with the exception of the verification of travel documents.*

Question 27. Annex III point 7 applies only when the AI system is “intended to be used by or on behalf of competent public authorities, or by Union institutions, bodies, offices or agencies”. If you need **further clarification** on the scope of these actors, please specify the practical elements and the issues for which you need further clarification; please provide practical examples

1500 character(s) maximum

Given the expanding number of actors involved in migration, asylum and border control, it should be clarified and made explicit what actors would be considered as “acting on behalf of competent public authorities” and in what context this applies. It should be made clear that Annex III point 7 applies to Frontex, Europol and actors commissioned by Europol to carry out activities on their behalf. This point should also apply to private actors, including private companies, private security actors and international organisations to whom border management is outsourced. It should also be clarified that Annex II point 7 applies to actors outside of EU territory, that are implementing EU policies or multilateral agreements.

Question 28. Please provide practical examples of AI systems that in your opinion may fall within the scope of high-risk AI systems listed in point (7) of Annex III, related to migration, asylum and border control management.

Examples may include systems for which you have uncertainties or system that you consider should not be considered high-risk as they are outside the use cases listed in Annex III or they fulfil one or more of the conditions for the exceptions in Article 6(3) AI Act.

Name/description

Visa Streaming Algorithm in the UK (Algorithm used to assess who receives a visa. The system took information provided by visa applicants and automatically processed it, giving each person a code based on a “traffic light system – green, amber or red) <https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them/> <https://www.theguardian.com/uk-news/2020/aug/04/home-office-to-scrap-racist-algorithm-for-uk-visa-applicants> <https://migrantsrights.org.uk/wp-content/uploads/2025/02/AI-under-watch-English.pdf>.

Category

Assessing risks for individuals entering a Member State (Point 7(b))

High-risk

Yes, completely

Explain

Based on information from the British NHRI, the system was revealed to be discriminatory while the algorithm discriminated on the basis of nationality by design. The algorithm entrenched inaccurate and unfair decision-making, and subjected visa applications of people from certain countries to extra scrutiny. While this specific decision-making algorithm was scrapped, new streaming algorithms have been implemented in a broader and more complex system with no scrutiny or transparency which infringes on article 21, non-discrimination CFR.

Profiling

Yes

Exception

No

Explain The Visa Streaming Algorithm performs profiling because it automatically processes personal data of visa applicants to evaluate and classify them into categories (green, amber, red). It should not be exempted because it involves systematic, high-risk automated decision-making in public administration that significantly impacts fundamental rights without sufficient safeguards or narrowly defined exceptions.

Name/description

iBorderCtrl system use of automatic deception detection system (ADDS, computer software that observes facial (micro) gestures of the participant to detect deceptive behaviour) iBorderCtrl? No! | iBorderCtrl.no - <https://iborderctrl.no/start> Full article: The politics of deceptive borders: ‘biomarkers of deceit’ and the case of iBorderCtrl - <https://www.tandfonline.com/doi/full/10.1080/1369118X.2020.1792530> ENNHRI’s scoping paper on new technologies at the border - <https://ennhri.org/wp-content/uploads/2024/09/Technologies-migration-and-human-rights-the-role-of-European-NHRIs-an-ENNHRI-scoping-paper.pdf>

Category

Polygraph use by public authorities (Point 7(a))

High-risk

Yes, completely

Explain

Given that iBorderCtrl’s automatic deception detection is deployed during migrant interrogations at EU borders, it is a high-risk system due to its direct impact on fundamental rights such as the right to asylum, non-discrimination (Article 21 CFR), and privacy/data protection (Articles 7 and 8 CFR).

Profiling

Yes

Exception

No

Explain iBorderCtrl performs profiling because it automatically processes biometric data (facial micro-gestures) to evaluate personal behavioral traits related to deception, which involves assessing and categorising individuals based on their personal characteristics. It cannot be exempted as it is used for border control and migration management, a core high-risk area explicitly listed in Annex III(7). Also, it has significant impacts on fundamental rights like privacy, freedom of movement, and non-discrimination and affects vulnerable populations.

Name/description

High-risk

Explain

This system processes biometric and linguistic data to assess applicants’ country of origin, directly impacting fundamental rights including the right to asylum, non-discrimination (Article 21 CFR),

Profiling

Exception

Explain The system performs profiling as it automatically processes personal and linguistic data to evaluate personal characteristics therefore classifying individuals based on sensitive personal attributes. It should not be

EU Asylum Agency (EUAA) dialect recognition LADO (common European Platform to identify the country of origin of applicants through language assessment https://euaa.europa.eu/sites/default/files/publications/2023-10/2023_EUAA-Strategy-on-Digital-Innovation-in-Asylum-Procedures-and-Reception-Systems_EN.pdf <https://blogs.sussex.ac.uk/sussex-centre-for-migration-research/2025/01/10/european-language-detection-software/>.

Identifying individuals in migration and border control (Point 7(d))

Yes, completely

privacy and data protection (Articles 7 and 8 CFR), and the right to an effective remedy (Article 47 CFR). Its use in critical asylum procedures should require strict regulation as a high-risk system.

Yes

No

exempted as it processes sensitive data for migration and asylum decisions which risks impacting fundamental rights.

Name/description

ROBORDER project (autonomous border surveillance by mobile robots to detect capabilities for illegal activities and incidents) autonomous swarm of heterogeneous RObots for BORDER surveillance | ROBORDER | Projekt | Fact Sheet | H2020 | CORDIS | European Commission - <https://cordis.europa.eu/project/id/740593>

Category

Identifying individuals in migration and border control (Point 7(d))

High-risk

Yes, completely

Explain It is a high risk system because it involves autonomous surveillance at borders with potential significant impacts on fundamental rights such as privacy, freedom of movement, and non-discrimination.

Profiling

Yes

Exception

No

Explain The system potentially performs profiling as it automatically processes data collected through autonomous surveillance to detect and evaluate individuals' behaviors and potential involvement in illegal activities, thereby assessing personal characteristics and classifying people based on that data. It should not be exempted as it processes sensitive data which risks impacting fundamental rights

Name/description

Category

- ☐ Polygraph use by public authorities (Point 7(a))
- ☐ Assessing risks for individuals entering a Member State (Point 7(b))
- ☒ Assisting with asylum and visa applications (Point 7(c))
- ☐ Identifying individuals in

High-risk

- ☐ Yes, completely
- ☐ Partially
- ☐ No
- ☐ Unsure

Explain

Profiling

- ☐ Yes
- ☐ No
- ☐ Unsure

Exception

- ☐ Yes
- ☐ No
- ☐ Unsure

Explain

Name/description

migration and
border control
(Point 7(d))

Category

☐ Polygraph use by
public authorities
(Point 7(a))

☐ Assessing risks
for individuals
entering a
Member State
(Point 7(b))

☐ Assisting with
asylum and visa
applications
(Point 7(c))

☐ Identifying
individuals in
migration and
border control
(Point 7(d))

High-risk

☐ Yes, completely

☐ Partially

☐ No

☐ Unsure

Explain

Name/description

Category

☐ Polygraph use by
public authorities
(Point 7(a))

☐ Assessing risks
for individuals
entering a
Member State
(Point 7(b))

☐

High-risk

☐ Yes, completely

☐ Partially

Explain

Profiling

☐ Yes

☐ No

☐ Unsure

Exception

☐ Yes

☐ No

☐ Unsure

Explain

Profiling

☐ Yes

Exception

☐ Yes

Explain

Name/description

Assisting with
asylum and visa
applications
(Point 7(c))
☐ Identifying
individuals in
migration and
border control
(Point 7(d))

Category

☐ Polygraph use by
public authorities
(Point 7(a))

☐ Assessing risks
for individuals
entering a
Member State
(Point 7(b))

☐ Assisting with
asylum and visa
applications
(Point 7(c))

☐ Identifying
individuals in
migration and
border control
(Point 7(d))

Category

☐ Polygraph use by
public authorities
(Point 7(a))

High-risk

☐ Yes, completely
☐ Partially
☐ No
☐ Unsure

Explain

☐ No
☐ Unsure

☐ No
☐ Unsure

Profiling

☐ Yes
☐ No
☐ Unsure

Exception

☐ Yes
☐ No
☐ Unsure

Explain

Name/description

☐ Assessing risks
for individuals
entering a
Member State
(Point 7(b))

High-risk

☐ Yes, completely

☐ Partially

☐ No

☐ Unsure

Explain

☐ Assisting with
asylum and visa
applications
(Point 7(c))

☐ Identifying
individuals in
migration and
border control
(Point 7(d))

Category

☐ Polygraph use by
public authorities
(Point 7(a))

☐ Assessing risks
for individuals
entering a
Member State
(Point 7(b))

High-risk

☐ Yes, completely

☐ Partially

☐ No

☐ Unsure

Explain

☐ Assisting with
asylum and visa
applications
(Point 7(c))

☐ Identifying
individuals in

Name/description

Profiling

☐ Yes

☐ No

☐ Unsure

Exception

☐ Yes

☐ No

☐ Unsure

Explain

Profiling

☐ Yes

☐ No

☐ Unsure

Exception

☐ Yes

☐ No

☐ Unsure

Explain

migration and
border control
(Point 7(d))

Question 29. Do you have or know practical examples of AI systems listed in the area of migration, asylum and border control management in Annex III where you need further clarification regarding the **distinction from prohibited AI systems**?

	Name and description of the system	Category of AI system	Category of prohibited AI system with which there may be an interplay	Please motivate your answer
1	<i>Name/description</i> Netherlands Visa Risk Scoring - social scoring related to the trustworthiness of a visa applicant to not overstay the visa https://www.nrc.nl/nieuws/2023/04/23/beslisambtenarenblijven-profileren-met-risicoscores-a4162837 https://www.lighthousereports.com/investigation/ethnic-profiling/	<i>Category</i> ☐ Assessing risks for individuals entering a Member State (Point 7 (b))	<i>Category</i> ☐ Social scoring (Art. 5(1) (c))	<i>Explain</i> Based on information from the Dutch NHRI, ENNHRI submits that the evaluation is based on personal characteristics (nationality) that lead to indirect discrimination, as nationality can be a proxy for race. Applicants from Morocco and Suriname were consistently ranked as 'high-risk', and were automatically moved to an "intensive track" subject to extensive investigation and delay. The risk profiles were also based on data from third parties to see if a group of individuals from the same nationalities attempted to apply for asylum, leading to classification as 'high score' individuals deemed as at risk of applying for asylum.
2	<i>Name/description</i>	<i>Category</i> ☐ Assessing risks for individuals entering a Member State (Point 7(b)) ☐ Assisting with asylum and visa applications (Point 7 (c)) ☐ Identifying individuals in migration and border control (Point 7(d))	<i>Category</i> ☐ Social scoring (Art. 5 (1)(c)) ☐ Predicting criminal behaviour (Art. 5(1) (d)) ☐ Real time remote biometric identification system (Art. 5(1)(h)) ☐ Other	<i>Explain</i>
		<i>Category</i> ☐	<i>Category</i> ☐	

3	Name/description	Assessing risks for individuals entering a Member State (Point 7(b)) - Assisting with asylum and visa applications (Point 7(c)) - Identifying individuals in migration and border control (Point 7(d))	Social scoring (Art. 5(1)(c)) - Predicting criminal behaviour (Art. 5(1)(d)) - Real time remote biometric identification system (Art. 5(1)(h)) - Other	Explain
4	Name/description	<i>Category</i> - Assessing risks for individuals entering a Member State (Point 7(b)) - Assisting with asylum and visa applications (Point 7(c)) - Identifying individuals in migration and border control (Point 7(d))	<i>Category</i> - Social scoring (Art. 5(1)(c)) - Predicting criminal behaviour (Art. 5(1)(d)) - Real time remote biometric identification system (Art. 5(1)(h)) - Other	Explain
		<i>Category</i> - Assessing risks for individuals entering a Member State (Point 7(b))	<i>Category</i> - Social scoring (Art. 5(1)(c))	

5	<i>Name/description</i>	Assisting with asylum and visa applications (Point 7 (c)) ☐ Identifying individuals in migration and border control (Point 7(d))	Predicting criminal behaviour (Art. 5(1) (d)) ☐ Real time remote biometric identification system (Art. 5(1)(h)) ☐ Other	<i>Explain</i>
---	-------------------------	--	--	----------------

Question 30. Do you see the need for clarification of one of the various use cases of high-risk classification in Point 7 of Annex III to the AI Act and its **interplay with other Union or national legislation**, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay

1500 character(s) maximum

2.H. Questions in relation to administration of justice and democratic processes (Annex III, point 8)

The classification of AI systems as high-risk under Annex III point 8 AI Act targets AI systems which are intended to be used in the administration of justice and democratic processes, since they have a potentially significant impact on democracy, the rule of law, individual freedoms as well as the right to an effective remedy and to a fair trial.

Point 8 of Annex III to the AI Act provides two cases in the context of administration of justice and democratic processes in which AI systems are classified as high-risk.

Point 8(a) of Annex III to the AI Act refers to AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a practical set of facts, or to be used in a similar way in alternative dispute resolution. Point 8(a) of Annex III therefore contains two distinct use cases. For the second use case, it is specified in recital 61 that this applies when the outcomes of the alternative dispute resolution proceedings produce legal effects for the parties.

1. AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a practical set of facts.
2. AI systems intended to be used in a similar way to the use case above in alternative dispute resolution.

Point 8(b) of Annex III to the AI Act refers to AI systems intended to be used for influencing the outcome of an election or referendum. It is further specified in point 8(b) of Annex III that this does not include AI systems to the output of which natural persons are not directly exposed, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view.

Question 31. Please provide practical examples of AI systems that in your opinion may fall within the scope of high-risk AI systems listed in the area of administration of justice and democratic processes in point (8) of Annex III.

Examples may include systems for which you have uncertainties or system that you consider should not be considered high-risk as they are outside the use cases listed in Annex III or they fulfil one or more of the conditions for the exceptions in Article 6(3) AI Act.

Name/description

From Germany - Legal tech in administrative court asylum proceedings: The plan is to use the EMIL and TABEA prototypes to develop large language models (LLMs) similar to ChatGPT: EMIL, the 'knowledge assistant for asylum procedures,' is designed to help judges find relevant information in reports from sources such as the UNHCR or EASO on the situation in countries of origin. To this end, the available sources – regardless of their language – are made searchable in German with the help of a research bot, and a summary of the information sources is offered as a text suggestion that can be incorporated into a court decision if necessary. According to the project, no evaluation or weighting of the information is to be carried out. EMIL uses a meta database that is updated daily based on data sources prepared by other institutions, such as ecoi.net and RefWorld. These sources are then processed by an LLM. Judges can submit queries using natural language prompts via a web browser. TABEA, the 'factual assistant for asylum proceedings,' is intended to help 'penetrate' asylum case files. To this end, data such as nationality, asylum application, time and manner of entry, or date of birth are to be processed in a standardised manner. In addition, the application will provide an overview of the reasons for departure or the persecution alleged, summarise the BAMF's (Bundesamt für Migration und Flüchtlinge) hearing transcript and, based on the information in the file, suggest wording for the facts of the case. However, as this involves the processing of particularly sensitive personal data, only LLM technologies that can be operated in the justice system's own data centres are being tested. The large language models Mistral, Llama 3 and T5 Large are being tested, for example. While separate 'prompts' currently still need to be formulated for use, the 'best prompt' will later be stored and the task will only be initiated via a 'Create summary' or 'Draft facts' button.

Name/description

Category

Assisting judicial authorities or used in similar ways in alternative dispute resolution (Point 8 (a))

High-risk

Unsure

Explain Based on information provided by the German NHRI, ENNHRI submits that the proposed LLMs developed to assist in administrative court asylum proceedings could potentially be classified as high-risk AI systems. Although these LLMs are currently just considerations, and there is a discussion about whether or not they would definitely qualify as high-risk under the AI Act, they serve as a useful example of the significant risks that such systems could pose. The proposed LLMs are planned to be based on the two prototypes, EMIL and TABEA, which both likely qualify as high risk systems as their use engages key fundamental rights (e.g., right to asylum, fair trial, non-discrimination), and TABEA in particular processes sensitive personal data to generate legal summaries, which elevates the risk profile.

Profiling

Unsure

Exception

No

Explain These proposed LLMs would likely profile natural persons because they might be used to automatically process personal data to evaluate individuals and make decisions that affect their rights and freedoms. In such a case, they should not be exempted as they would pose serious threats to fundamental rights.

Category

- ☒ Assisting judicial authorities or used in similar ways in alternative dispute resolution (Point 8(a))
- ☐ Influencing election

High-risk

- ☐ Yes, completely
- ☐ Partially
- ☐ No
- ☐ Unsure

Explain

Profiling

- ☐ Yes
- ☐ No
- ☐ Unsure

Exception

- ☐ Yes
- ☐ No
- ☐ Unsure

Explain

Name/description

outcomes or
voting behaviour
(Point 8(b))

Category

☐ Assisting judicial
authorities or
used in similar
ways in
alternative
dispute
resolution (Point
8(a))

High-risk

☐ Yes, completely
☐ Partially
☐ No
☐ Unsure

Explain

Profiling

☐ Yes
☐ No
☐ Unsure

Exception

☐ Yes
☐ No
☐ Unsure

Explain

☐ Influencing
election
outcomes or
voting behaviour
(Point 8(b))

Category

☐ Assisting judicial
authorities or
used in similar
ways in
alternative
dispute
resolution (Point
8(a))

High-risk

☐ Yes, completely
☐ Partially
☐ No
☐ Unsure

Explain

Profiling

☐ Yes
☐ No
☐ Unsure

Exception

☐ Yes
☐ No
☐ Unsure

Explain

Name/description

outcomes or
voting behaviour
(Point 8(b))

Name/description

Category

- ☐ Assisting judicial
authorities or
used in similar
ways in
alternative
dispute
resolution (Point
8(a))
- ☐ Influencing
election
outcomes or
voting behaviour
(Point 8(b))

High-risk

- ☐ Yes, completely
- ☐ Partially
- ☐ No
- ☐ Unsure

Explain

Profiling

- ☐ Yes
- ☐ No
- ☐ Unsure

Exception

- ☐ Yes
- ☐ No
- ☐ Unsure

Explain

Name/description

Category

- ☐ Assisting judicial
authorities or
used in similar
ways in
alternative
dispute
resolution (Point
8(a))
- ☐ Influencing
election
outcomes or
voting behaviour
(Point 8(b))

High-risk

- ☐ Yes, completely
- ☐ Partially
- ☐ No
- ☐ Unsure

Explain

Profiling

- ☐ Yes
- ☐ No
- ☐ Unsure

Exception

- ☐ Yes
- ☐ No
- ☐ Unsure

Explain

Category

- ☐ Assisting judicial
authorities or

Name/description

used in similar
ways in
alternative
dispute
resolution (Point
8(a))
☒ Influencing
election
outcomes or
voting behaviour
(Point 8(b))

High-risk

- ☐ Yes, completely
- ☐ Partially
- ☐ No
- ☐ Unsure

Explain

Profiling

- ☐ Yes
- ☐ No
- ☐ Unsure

Exception

- ☐ Yes
- ☐ No
- ☐ Unsure

Explain

Name/description

☐ Assisting judicial
authorities or
used in similar
ways in
alternative
dispute
resolution (Point
8(a))
☒ Influencing
election
outcomes or
voting behaviour
(Point 8(b))

High-risk

- ☐ Yes, completely
- ☐ Partially
- ☐ No
- ☐ Unsure

Explain

Profiling

- ☐ Yes
- ☐ No
- ☐ Unsure

Exception

- ☐ Yes
- ☐ No
- ☐ Unsure

Explain

Category

☒ Assisting judicial
authorities or
used in similar
ways in
alternative

High-risk

Profiling

Exception

Name/description

dispute
resolution (Point
8(a))
☒ Influencing
election
outcomes or
voting behaviour
(Point 8(b))

- ☐ Yes, completely
☐ Partially
☐ No
☐ Unsure

Explain

- ☐ Yes
☐ No
☐ Unsure

- ☐ Yes
☐ No
☐ Unsure

Explain

Category

☒ Assisting judicial
authorities or
used in similar
ways in
alternative

High-risk

- ☐ Yes, completely
☐ Partially
☐ No
☐ Unsure

Explain

Profiling

- ☐ Yes
☐ No
☐ Unsure

Exception

- ☐ Yes
☐ No
☐ Unsure

Explain

Name/description

dispute
resolution (Point
8(a))
☒ Influencing
election
outcomes or
voting behaviour
(Point 8(b))

Question 32. If you see the need for clarification of the high-risk classification in *Point 8 of Annex III to the AI Act* and its **interplay with other Union or national legislation**, in particular Regulation (EU) 2024/900 on targeted political advertising, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay

1500 character(s) maximum

Section 4 – Questions in relation to requirements and obligations for high-risk AI systems and value chain obligations

A. Requirements for high-risk AI systems

The AI Act sets mandatory requirements for high-risk AI systems as regards risk management (Article 9), data and data governance (Article 10), technical documentation (Article 11) and record-keeping (Article 12), transparency and the provision of information to deployers (Article 13), human oversight (Article 14), and robustness, accuracy and cybersecurity (Article 15).

Providers are obliged to ensure that their high-risk AI system is compliant with those requirements before it is placed on the market. Harmonised standards will play a key role to provide technical solutions to providers that can voluntarily rely on them to ensure compliance and rely on a presumption of conformity. The Commission has requested the European standardisation organisations CEN and CENELEC to develop standards in support of the AI Act. This work is currently under preparation.

Question 35. Beyond the technical standards under preparation by the European Standardisation Organisations, are there further aspects related to the AI Act's requirements for high-risk AI systems in Articles 9-15 for which you would seek clarification, for example through guidelines?

If so, please elaborate on which specific questions you would seek further clarification.

3000 character(s) maximum

ENNHRI would welcome clarifications of the connection between Article 9 and Article 27 AI Act in situations where the provider and deployer are the same organisation. Specifically, in circumstances where the provider and deployer might overlap, it should be clarified whether implementing a risk management process that identifies and mitigates fundamental rights risks as per art 9 would be sufficient to meet the fundamental rights impact assessment obligation under art (27). Additionally, ENNHRI believes further guidance on the practical functioning of the process described in Article 10(5) can be of use, due to its technical complexity and possible importance for minimising the risk of discrimination based on avoidable biases in the test and training data. Facilitating developers to make use of this scheme through accessible and clear guidance could enhance take up and/or avoid misinterpretation. Article 9 is only concerned with risks “which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information.” However, Article 52(1) of the EU Charter of Fundamental Rights states that “[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms” and that “[s]ubject to the principle of proportionality, limitations may be

made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.” Accordingly, it is possible that fundamental rights harms cannot be considered a risk under Article 9 if they may not be mitigated or eliminated through technical means. This is especially the case because there may not be an acceptable residual risk to fundamental rights. ENNHRI would welcome clarification to what extent harm to fundamental rights are within the scope of Article 9 considering the references to acceptable residual risk and risks that can be addressed through technical means.

Question 36. Are there aspects related to the requirements for high-risk AI systems in Articles 9-15 which require clarification regarding their interplay with other Union legislation?

If so, please elaborate which specific aspects require clarification regarding their interplay with other Union legislation and point to concrete provisions of specific other Union law.

3000 character(s) maximum

ENNHRI submits that an area that would require clarification is the interplay between the risk management obligation under the AI Act and the risk-based human rights and environmental due diligence obligation under the Corporate Sustainability Due Diligence Directive (CSDDD), particularly relevant for large companies that are AI providers and therefore falling in the scope of both regulations (acknowledging that as of writing, the contents of the CSDDD are currently being debated in the context of the Omnibus I initiative). Article 5 CSDDD requires large companies to conduct risk-based human rights and environmental due diligence to assess, prevent, mitigate and remediate their adverse/negative impacts, including by integrating due diligence into their policies and risk management systems. In respect to human rights, the obligation to identify and address potential impacts under CSDDD creates a clear overlap with the obligation of AI system providers to identify and mitigate fundamental rights risks. However, the obligation under CSDDD is more extensive and includes, for example, obligations to assess negative impacts arising from business partners in the ‘chain of activities’ (art 8), to conduct meaningful engagement with stakeholders (art 13) and the remediation of negative impacts (art 12). The European Commission should clarify the interaction between the AI system-specific risk management measures and the more general company-wide due diligence requirements under CSDDD.

B. Obligations for providers of high-risk AI systems

Beyond ensuring that a high-risk AI system is compliant with the requirements in Articles 9-15, providers of high-risk AI systems have several other obligations as listed in Article 16 and further specified in other corresponding provisions of the AI Act. These include:

- *Indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable, their name, registered trade name or registered trademark, the address at which they can be contacted;*
- *Have a quality management system in place which complies with Article 17;*
- *Keep the documentation referred to in Article 18;*
- *When under their control, keep the logs automatically generated by their high-risk AI systems as referred to in Article 19;*
- *Ensure that the high-risk AI system undergoes the relevant conformity assessment procedure as referred to in Article 43;*

- *Draw up an EU declaration of conformity in accordance with Article 47;*
- *Affix the CE marking to the high-risk AI system, in accordance with Article 48;*
- *Comply with the registration obligations referred to in Article 49(1);*
- *Take the necessary corrective actions and provide information as required in Article 20;*
- *Cooperate with national competent authorities as required in Article 21;*
- *Ensure that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.*

Question 37. Are there aspects related to the AI Act's obligations for providers of high-risk AI systems for which you would seek clarification, for example through guidelines?

If so, please elaborate on which specific questions you would seek further clarification.

3000 character(s) maximum

Question 38. Are there aspects related to the obligations for providers of high-risk AI systems which require clarification regarding their interplay with other Union legislation?

If so, please elaborate which specific aspects require clarification regarding their interplay with other Union legislation and point to concrete provisions of specific other Union law.

3000 character(s) maximum

C. Obligations for deployers of high-risk AI systems

Article 3(4) defines a deployer as a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

Deployers of high-risk AI systems have specific responsibilities under the AI Act. Transversally, Article 26 obliges all deployers of high-risk AI systems to:

- *Take appropriate technical and organisational measures to ensure that AI systems are used in accordance with the instructions accompanying the AI systems;*
- *Assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support;*
- *Ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system;*
- *Monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Article 72;*

- *Keep the logs automatically generated by that high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system of at least six months.*

Additionally, Article 26 foresees the following obligations in specific cases:

- *For high-risk AI system at the workplace, deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system;*
- *Specific authorization requirements and restrictions apply to the deployer of a high-risk AI system for post-remote biometric identification for law enforcement purposes;*
- *Deployers of high-risk AI systems referred to in Annex III that make decisions or assist in making decisions related to natural persons shall inform the natural persons that they are subject to the use of the high-risk AI system.*

Question 39. Are there aspects related to the AI Act's obligations for deployers of high-risk AI systems listed in Article 26 for which you would seek clarification, for example through guidelines?

If so, please elaborate on which specific questions you would seek further clarification.

3000 character(s) maximum

Some uses of remote biometric identification (RBI) systems (including real-time, post, by private and public entities) in publicly accessible spaces may infringe on people's fundamental rights. Therefore, ENNHRI seeks further clarification, preferably in the form of guidelines, regarding the obligations of deployers of these specific high-risk AI systems where it is not apparent which safeguards would prevent fundamental rights violations and make their use acceptable in a democratic, rule-of-law-respecting society. An example of such a high-risk AI system can be seen in the current use of RBI in Paris, which was started during the Paris Olympics in 2023. This would likely be an infringement of Articles 7 and 8 of the EU Charter of Fundamental Rights and Article 9 GDPR. The French NHRI, CNCDH, published an opinion on this in June 2024 where it expressed its concern about the experimentation of algorithmic video surveillance during the Olympic Games. They deemed that this practice was not only an invasion of privacy but also has a dissuasive impact on the exercise of the freedom to demonstrate. Additionally, ENNHRI submits that further clarification is needed on the extent of deployers' responsibility to monitor the operation of high-risk AI-systems on the basis of the instructions for use in Article 26 (5). How does this relate to a possible fundamental rights impact assessment per Article 27 that might indicate more stringent, frequent or simply different types of monitoring are warranted than provided for in the developers' instructions for use? Would the monitoring standards in the instructions still be leading as the standard for deployers obligations under the AI Act? Additional guidance on the extent of the monitoring obligation in relation to the instructions of use and a possible FRIA would be useful.

Question 40. Are there aspects related to the obligations for deployers of high-risk AI systems listed in Article 26 which require clarification regarding their interplay with other Union legislation?

If so, please elaborate which specific aspects require clarification regarding their interplay with other Union legislation and point to concrete provisions of specific other Union law.

3000 character(s) maximum

ENNHRI submits that a lack of transparency requirements for high-risk systems leads to a need for further clarification. First, ENNHRI recommends that the guidelines clarify that a narrow interpretation should be given to the term 'sensitive operational data' as used in Article 26(10) of the AI Act. The guidance should avoid that the exemption of disclosure of sensitive operational data related to law enforcement would allow a loophole that would render oversight of high-risk systems impossible. To uphold fundamental rights and ensure meaningful oversight and accountability of law enforcement's use of high-risk AI, we recommend that the exception to the rule on disclosing operational data—namely, the reference to 'sensitive operational data'—be interpreted narrowly. This is because the need to comply with fundamental rights generally outweighs concerns about the potential sensitivity of operational data. Second, ENNHRI recommends that the guidelines should explicitly acknowledge that transparency obligations for high-risk AI systems are defined not only by the AI Act but also by other EU legal frameworks. Since these systems process personal data, Articles 13 & 14 of the GDPR apply, unless processing is conducted for law enforcement purposes, in which case the Law Enforcement Directive (LED) governs transparency requirements. Additionally, AI systems used by public bodies or entities exercising public functions are subject to national freedom of information (FOI) laws, which impose further transparency obligations. Clarification is needed on how high-risk AI systems under Annex III of the AI Act align with Article 22 and Article 15(1)(h) GDPR, especially in light of the Dun & Bradstreet Austria judgment on transparency in automated decision-making (C-203/22). For reference, in this case, the Court of Justice of the European Union (CJEU) ruled on the right to transparency in automated decision-making under the GDPR. The CJEU determined that individuals have the right to receive intelligible information about the logic involved in automated decision-making processes, including key parameters and their influence in the assessment. The Court also addressed the balance between transparency and the protection of trade secrets, stating that trade secret protection may not be invoked to deny access to relevant information.

*Moreover, according to Article 27, deployers of high-risk AI systems that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III, shall perform an **assessment of the impact on fundamental rights** that the use of such system may produce. The AI Office is currently preparing a template that should facilitate compliance with this obligation.*

Article 27 specifies that where any of its obligations are already met through the data protection impact assessment conducted pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 of this Article shall complement that data protection impact assessment.

Question 41. Are there aspects related to the AI Act's obligations for deployers of high-risk AI systems for the fundamental rights impact assessment for which you would seek clarification in the template?

3000 character(s) maximum

ENNHRI submits that the AI Office should clarify the regulatory purpose of the template questionnaire and ensure it will support meaningful and effective FRIAs. At the moment it is unclear whether (i) this questionnaire is supposed to be used as a reporting tool, compliance tool or both, (ii) relatedly, whether the responses to the questionnaire are the only documentation that deployers should make available to the competent authorities to determine the deployer's compliance with art 27 of the AI Act; (iii) the legal consequences of not filling out the questionnaire or filling it out in a superficial manner. In NHRIs' experience and learning from practical pilots, deployers need fundamental rights expertise, practical detailed guidance and resources on how to conduct a FRIA, as well as regulatory certainty about what measures and actions are sufficient to demonstrate compliance with the AI Act. ENNHRI is concerned that a template questionnaire might not be sufficient to meet both needs and objectives. As such, ENNHRI encourages the AI Office to address the foundational question

about the objective of the template as a first critical step before developing its scope and content and gauging the need to complement this template with additional guidelines and examples. As further detailed in ENNHRI's dedicated statement, to ensure meaningful and effective FRIAs, ENNHRI recommends the following:

- **Quality:** The template should move beyond yes/no checklists and require clear procedural steps, open-ended responses, documentation of deliberation, and context-specific analysis. Deployers must update the FRIA after significant system or deployment changes.
- **Stakeholder Engagement:** Deployers should document how affected groups—especially impacted communities, fundamental rights experts, and CSOs—were involved. This includes missing voices, power imbalances, access to information, and allocated resources. Article 77 bodies should be engaged where relevant to guide risk identification and mitigation.
- **Justification:** FRIAs should not only assess risks, but also include justification for deploying the system at all, and address necessity, proportionality, and residual risk. A public mitigation and redress plan with actionable steps must be included.
- **Re-use of Providers' FRIAs:** While reuse is allowed under Art. 27(2), this must not bypass deployers' obligations to assess context-specific risks. The template should require explanation of how the provider's FRIA was used, any added risks, and communication between parties.
- **Transparency:** The template must define what is public, justify redactions, and ensure full access to competent authorities, including Art. 77 bodies. It must also enable individuals to access relevant information on rights and redress.
- **Oversight:** The FRIA should note any external reviews, complaint mechanisms, and communication with market surveillance or art. 77 authorities in cases of unresolved risk.

Question 42. In your view, how can complementarity of the fundamental rights impact assessment and the data protection impact assessment be ensured, while avoiding overlaps?

3000 character(s) maximum

ENNHRI submits that the FRIA and the DPIA differ in focus and function, and this distinction must be articulated in the guidance. The scope of a FRIA is wider than the scope of a DPIA insofar as a FRIA should consider impacts on any of the 50 rights of the EU Charter of Fundamental Rights (see recital 1 AI Act) while a DPIA is supposed "to assess the impact of the envisaged processing operations on the protection of personal data" (art 35(1) GDPR). Moreover, high-risk AI systems can have negative fundamental rights impacts that are not strictly related to the processing of personal data (for example, fundamental rights impacts that might be related to the displacement of workers as result of the introduction of a new AI system). In other words, while a FRIA will benefit from the analysis carried out in a DPIA, a DPIA will not be sufficient to fully capture the expectations under the AI Act. Against this backdrop, the implications for complementarity are twofold. First, for efficiency and information-sharing purposes, it would be advisable that deployers orchestrate the FRIA and DPIA as a single process – under one governance framework, conducted by the same team, and using a similar timeline. In such cases, however, it is important that the broader scope of FRIA be reflected in the competencies of the team doing the assessment (fundamental rights expertise additional to data protection is needed), the broader nature of stakeholder engagement to be conducted under FRIA (going beyond strictly data subjects but also affected and/or vulnerable groups), and the type of mitigation measures that should be put in place (human oversight measures, arrangements for internal governance and complaint mechanism – see art 27 in AI Act). Second, from a documentation of DPIA/FRIA perspective, there would be more legal certainty and ease of enforcement if deployers would be asked to produce different documentation for the two processes (which means tolerating a certain level of overlap in terms of the content produced). The reason is that (i) organisations have already developed bespoke DPIA tools and methodologies which vary across jurisdictions (there is no EU-level template in use) and might be reluctant to switch to a joint DPIA/FRIA template, (ii) there is no certainty that DPAs will exercise oversight over art 27 of the AI Act given that the landscape of setting up MSAs for enforcing the AI Act is still in motion across different jurisdictions. Further, ENNHRI believes it is important to encourage structured information exchange between providers and deployers to ensure that DPIAs and FRIAs are grounded in both system design and real-world use. This can support more robust and efficient assessments in both domains.

Finally, deployers of high-risk AI systems may have to provide an explanation to an affected person upon their request. This right is granted by Article 86 AI Act to affected persons which are subject to a decision, which is taken on the basis of the output from a high-risk AI system listed in Annex III and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights.

Question 43. Are there aspects related to the AI Act's right to request an explanation in Article 86 for which you would seek clarification, for example through guidelines?

If so, please elaborate on which specific questions you would seek further clarification.

3000 character(s) maximum

ENNHRI submits that clarification is needed on how the AI Act's Article 86 right to an explanation aligns with Article 15(1)(h) GDPR, especially following the CJEU Dun & Bradstreet Austria judgment (C-203/22, 27 February 2025). The CJEU ruled that individuals must receive meaningful, intelligible information about the actual procedures and principles used in automated decisions, even if trade secrets are involved. The CJEU introduced a balancing test, weakening absolute trade secret protection when it conflicts with transparency rights - an approach that should be reflected in future guidelines. In that case, the CJEU ruled that the balancing of rights needs to be performed by the regulator or a relevant court, and not by the company. In the case of the AI Act, an analogous argument can be made. Additionally, ENNHRI submits that it would be useful to provide further guidance on the extent to which the explanation is required to be context and recipient sensitive. For example it should be clarified if the AI Act envisions one standard for explaining that would apply to all sectors, contexts, and types of affected persons, or, whether the standard of 'clear and meaningful' would take into account varied contexts and recipients. Secondly, guidance on the extent to which the explanation can include broader information on the distribution of decisions made by the AI systems could be useful. In many cases a full understanding of how an AI system has affected a specific person can only be obtained if it is known how the system functions overall and how it treats different categories of people and situations. Therefore, it would be useful to know to what extent this type of information is also included in the right to an explanation.

D. Substantial modification (Article 25 (1) AI Act)

Article 3 (23) defines a substantial modification as a change to an AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider. As a result of such a change, the compliance of the AI system with the requirements for high-risk AI systems is either affected or results in a modification to the intended purpose for which the AI system has been assessed.

The concept of 'substantial modification' is central to the understanding of the requirement for the system to undergo a new conformity assessment. Pursuant to Article 43(4), the high-risk AI system should be considered a new AI system which should undergo a new conformity assessment in the event of a substantial modification.

This concept is also central for the understanding of the scope of obligations between a provider of a high-risk AI system and other actors operating in the value chain (distributor, importer or deployer of a high-risk AI system). Pursuant to Article 25, any distributor, importer, deployer or other third-party shall be considered to

be a provider of a high-risk AI system and shall be subject to the obligations of the provider, in any of the following circumstances:

(a), they put their name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual arrangements stipulating that the obligations are otherwise allocated;

(b), they make a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service in such a way that it remains a high-risk AI system;

(c), they modify the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service in such a way that the AI system concerned becomes a high-risk AI system.

Question 44. Do you have any feedback on issues that need clarification as well as practical examples on the application of the concept of 'substantial modification' to a high-risk AI system.

3000 character(s) maximum

Given the rapid pace of advancement in large language models (LLMs), it is expected that companies will regularly replace or upgrade the underlying models in their AI systems to take advantage of improved performance and reasoning capabilities. ENNHRI recommends that guidelines should explicitly state that any upgrade to an AI system involving the integration of a new LLM with enhanced reasoning or decision-making capacity is considered a substantial modification under the AI Act, especially in cases when an LLM plays a crucial role in decision-making. Furthermore, such guidelines should explicitly define any modification that leads to the reclassification of an AI system as high-risk as a “substantial modification.” Guidelines should establish clear thresholds and detailed criteria for what constitutes “substantial modification”, specifying exactly which types of modification require new conformity assessment. This is essential to ensure that AI systems do not evolve without proper oversight, potentially exposing people to fundamental rights harm without adequate protection or accountability. Since AI systems, including high-risk AI systems, are software, any change to their code, that changes the network architecture, including the optimisation process, should be considered.

Article 43(4) second sentence describes the circumstances under which the change does not qualify as a substantial modification: ‘For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.’

Question 45. Do you have any feedback on issues that need clarification as well as practical example of pre-determined changes which should not be considered as a substantial modification within the meaning the Article 43(4) of the AI Act.

3000 character(s) maximum

E. Questions related to the value chain roles and obligations

Throughout the AI value chain, multiple parties contribute to the development of AI systems by supplying tools, services, components, or processes. These parties play a crucial role in ensuring the provider of the high-risk AI system can comply with regulatory obligations. To facilitate compliance with regulatory obligations, Article 25(4) require these parties to provide the high-risk AI system provider with necessary information, capabilities, technical access and other assistance through written agreements, enabling them to fully meet the requirements outlined in the AI Act.

However, third parties making tools, services, or AI components available under free and open-source licenses are exempt from complying with value chain obligations. Instead, providers of free and open-source AI solutions are encouraged to adopt widely accepted documentation practices, such as model cards and datasheets, to facilitate information sharing and promote trustworthy AI.

To support cooperation along the value chain, the Commission may develop and recommend voluntary model contractual terms between providers of high-risk AI systems and third-party suppliers.

Question 46. From your organisation's perspective, can you describe the current distribution of roles in the AI value chain, including the relationships between providers, suppliers, developers, and other stakeholders that your organisation interacts with?

3000 character(s) maximum

While it seems that the questions related to value chain roles and obligations are largely addressed to actors within the value chain, it is important to keep in mind that impact from AI systems, both upstream and downstream, is largely felt by individuals and the environment. Therefore, ENNHRI submits it is important under this section to consider challenges to fundamental rights and the environment as a way to call attention for addressing them during the allocation of roles and responsibilities within the AI value chain.

Question 47 Do you have any feedback on potential dependencies and relationships throughout the AI value chain that should be taken into consideration when implementing the AI Act's obligations, including any upstream or downstream dependencies between providers, suppliers, developers, and other stakeholders, which might impact the allocation of obligations and responsibilities between various actors under the AI Act? In particular, indicate how these dependencies affect SMEs, including start-ups.

3000 character(s) maximum

Question 48. What information, capabilities, technical access and other assistance do you think are necessary for providers of high-risk AI systems to comply with the obligations under the AI Act, and how should these be further specified through written agreements?

3000 character(s) maximum

Question 49. Please specify the challenges in the application of the value chain obligations in your organisation for compliance with the AI Act's obligations for high-risk AI systems and the issues for which you need further clarification; please provide practical examples.

1500 character(s) maximum

Section 5. Questions in relation to the need for possible amendments of high-risk use cases in Annex III and of prohibited practices in Article 5

Pursuant to Article 112(1) AI Act, the Commission shall assess the need to amend the list of use cases set out in Annex III and of the list of prohibited AI practices laid down in Article 5 by 2 August 2025 and once a year from then onwards.

The Commission is empowered to adopt delegated acts to amend Annex III by adding or modifying use-cases of high-risk AI systems pursuant to Article 7(1) AI Act. The findings of the assessment carried out under Article 112(1) AI Act are relevant in this context. The empowerment to amend Annex III requires that both of the following conditions are fulfilled:

- *the AI systems are intended to be used in any of the areas listed in Annex III and*
- *the AI systems pose a risk of harm to health and safety, or an adverse impact on fundamental rights, and that risk is equivalent to, or greater than, the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.*

Article 7(2) AI Act further specifies the criteria that the Commission shall take into account in order to evaluate the latter condition, including:

(a) the intended purpose of the AI system;

(b) the extent to which an AI system has been used or is likely to be used;

(c) the nature and amount of the data processed and used by the AI system, in particular whether special categories of personal data are processed;

(d) 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;

(e) 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;

(f) 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;

(g) 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;

(h) 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;

(i) 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;

(j) 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;

(k) 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.

Question 50. Do you have or know concrete examples of AI systems that in your opinion need **to be added to the list of use cases in Annex III, among the existing 8 areas, in the light of the criteria and the conditions in Article 7(1) and (2)** and should be integrated into the assessment pursuant to Article 112(1) AI Act?

If so, please specify the concrete AI system that fulfils those criteria as well as evidence and justify why you consider that this system should be classified as high-risk.

3000 character(s) maximum

Question 51. Do you consider that some of the use cases listed in Annex III require adaptation in order to fulfil the conditions laid down pursuant to Article 7(3) AI Act and should therefore **be amended** and should be integrated into the assessment pursuant to Article 112(1) AI Act?

- ☐ Yes
- ☐ No

Question 52. Do you consider that some of the use cases listed in Annex III no longer *fulfil* the conditions laid down pursuant to Article 7(3) AI Act and should therefore **be removed from the list of use cases in Annex III** and should be integrated into the assessment pursuant to Article 112(1) AI Act?

- ☐ Yes
☐ No

Pursuant to Article 112(1) AI Act, the European Commission shall assess the need for amendment of the list of prohibited AI practices laid down in Article 5 once a year. In order to gather evidence of potential needs for amendments, respondents are invited to answer the following questions.

Question 53. Do you have or know concrete examples of AI practices that in your opinion contradict Union values of respect for human dignity, freedom, equality and no discrimination, democracy and the rule of law and fundamental rights enshrined in the Charter and for which there **is a regulatory gap because they are not addressed by other Union legislation?**

If so, please specify the concrete AI system that fulfils those criteria and justify why you consider that this system should be prohibited and why other Union legislation does not address this problem.

3000 character(s) maximum

Many of the technologies used in the field of asylum, migration and border governance pose a significant risk to human rights and fall within the unacceptable or high-risk categories. ENNHRI outlined in a scoping paper on “Technologies, migration, and human rights: the role of European NHRIs” several examples of harmful AI systems/practices related to migration and law enforcement that should potentially be added under Article 5. One of these practices concerns emotion recognition systems used by migration and law enforcement authorities, as although there is a ban on emotion recognition in workplaces and education under the AI Act, for law enforcement and migration purposes, emotion recognition is classified as high risk and AI systems in this field can still be used. An example of such a system noted in the scoping paper is the “iBorderCtrl Project” which has been consistently criticised by human rights actors for inadequate and insufficient consideration of its human rights impacts. Concerns include that emotion or lie detection technologies are built on pre-existing data which contains biases in migration contexts and can easily open the door to inaccurate results and misinterpretation, including for example, due to cultural differences in expressing emotion. Furthermore, the AI Act includes in Annex 3 AI systems able to assess the risk for security posed by a migrant. However, ENNHRI suggests that the authorisation of such use raises questions with regard to the prohibition of the use of a system that assesses the risk of a person committing an offence (Art. 5, 1, d).

Question 54. Do you consider that some of the prohibitions listed in Article 5 AI Act are already sufficiently addressed by other Union legislation and should therefore **be removed from the list of prohibited practices in Article 5 AI Act?**

- ☐ Yes
☐ No

