Contribution ID: 4fe4dc64-b73c-426b-86da-78ab6e320e0c
Date: 17/07/2025 14:10:56

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 prejudge 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.

[3]https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act.

Information about the respondent

* First name

Caterina

* Surname

Rodelli

* Email address

caterina@accessnow.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

Access Now

* 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

Medium (50-249 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
- [x] Others

* Please, specify

30 character(s) maximum

Human rights

* Describe the activities of your organisation or yourself

1300 character(s) maximum

Access Now defends and extends the digital rights of individuals and communties at risk

---

* 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

- [x] 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*

- [x] Biometrics
- [ ] Critical infrastructure
- [ ] Education and vocational training
- [ ] Employment, workers' management and access to self-employment
- [x] Access to and enjoyment of essential private services and essential public services and benefits
- [x] Law enforcement
- [x] 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-ris 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	*Name/description* Face and fingerprint scanners used by Greek police and migration authorities during stop and searches https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights	*Category* Remote biometric identification (Point 1 (a))	*High-risk* Yes, completely	*Explain* Biometric identification, even when conducted in a non-remote setting (i.e. systems used against individuals, not at a distance) , can have serious fundamental rights implications. These systems include hand-held facial image, fingerprint or palm scanners, voice or iris identification technology and, depending the context of use, they can lead to discrimination, surveillance or coercion of the person the system is used against .	*Profiling* Yes	*Exception* No	*Explain* To ensure regulatory consistency with the GDPR, it is vital that certain AI systems which process biometric data are considered high risk. Article 9 of the GDPR states that biometric data are very sensitive, and paragraph 4 further encourages additional national or EU laws to protect emerging uses of biometric data that pose a risk to people's fundamental rights.
2	*Name/description* The retrospective application of biometric identification analytics to a still image of a suspect taken from CCTV footage of a serious crime, where the footage is obtained lawfully (i.e post RBI)	*Category* Remote biometric identification (Point 1 (a))	*High-risk* Yes, completely	*Explain* In order to constitute permitted (but still restricted) post RBI - as opposed to prohibited real-time RBI - such a system could only be used to analyse stills (i.e. screen grabs) of individual faces of persons suspected of serious crimes, ensuring that no non-suspect persons faces or other features are analysed. The entirety of the footage could not be analysed, as this would entail untargeted analysis, which is not allowed under Article 26. The guidelines should clarify these points. What's more, even if such a use case is not specifically prohibited under the AI Act, we reiterate that it would still be unlawful under the Charter if, for example, the system has lower rates of effectiveness for certain demographics (e.g. people of colour) or if it is used disproportionately against those groups. In accordance with the Law Enforcement Directive, no decision can be taken which would have a legal effect solely on the basis of this system.	*Profiling* Yes	*Exception* No	*Explain* This use case does not contain any exception - and may even be de facto prohibited if it is used in a way that would constitute, in time or in effective function, the real-time use of a system. This point is particularly important because some governments may seek to avoid the prohibition on real-time RBI by using a system that for all intents and purposes operates in real or near-real time, whilst adopting features more commonly seen in post uses, as a way to circumvent the prohibition.
3	*Name/description* The use of a real-time RBI by law enforcement in publicly accessible spaces in accordance with one of the three exceptions established in Article 5 e.g. police	*Category*	*High-risk* Partially	*Explain* By definition, any real-time RBI system by police that is not prohibited would still be high risk, and would also have to follow the additional controls required for police uses of RBI. We reiterate that these use cases still entail extremely severe limitations on the fundamental rights of all people in the public spaces. The exceptions to the in-principle prohibition therefore need to meet an extremely high threshold. In a situation such as an imminent, genuine and foreseeable threat of a terror attack,	*Profiling* Yes	*Exception* No	*Explain*

	searching for a person believed to be about to detonate a bomb as part of a terror attack	Remote biometric identification (Point 1 (a))		there must still not be any permanent RBI infrastructure. Instead, the infrastructure must be temporary, clearly marked, and must meet all the criteria for authorisation, safeguards, limitations in geographic scope etc in order to meet requirements of strict necessity and proportionality. Any uses not meeting these strict criteria would still be prohibited.			
4	*Name/description* Real-time RBI by any actor other than police e.g. live facial recognition by a property developer in a public square, or by a supermarket at the entrance to their store, or a local council at the front of their building	*Category* Remote biometric identification (Point 1 (a))	*High-risk* No	*Explain* This system is not permitted by the AI Act nor the GDPR. The guidelines should clarify that even though it is not in Article 5, such a use is still prohibited.	*Profiling* Yes	*Exception* No	*Explain* There are no exceptions. The AI Act only allows real-time RBI under three specific circumstances on the basis of national law. In accordance with the GDPR's strict protections on biometric data, all uses that fall outside the aforementioned legalisation are not permitted in the EU.
5	*Name/description* iBorderCTRL	*Category* Emotion recognition (Point 1(c))	*High-risk* No	*Explain* iBorderCTRL was a pilot project designed to perform emotion recognition of people travelling to the EU and predict if they are being truthful in their immigration interviews. The purpose of the system was to assist border guards in their job to assess immigration applications. It clearly falls within the definition of an emotion recognition system, and it is in a workplace context (the system is being used for the work of the border guard) where there is a profound power imbalance; Hence this system should be prohibited.	*Profiling* Yes	*Exception* No	*Explain* This system should fall under the prohibitions, as it is meeting the criteria laid down in the act that it is emotion recognition in the workplace of the border guard. Hence, this system should be prohibited.
6	*Name/description*	*Category* Remote biometric identification (Point 1 (a)) Biometric categorisation (Point 1(b)) Emotion recognition (Point 1(c))	*High-risk* Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*
7	*Name/description*	*Category* Remote biometric identification (Point 1 (a))	*High-risk* Yes, completely Partially	*Explain*	*Profiling* Yes	*Exception* Yes	*Explain*

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

		Emotion recognition (Point 1(c))					

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	*Name/description* Polygraphs used in the migration context, iBorderCtrl	*Category* Emotion recognition (Point 1(c))	*Category* Emotion inference system (Art. 5(1)(f))	*Explain* All systems that perform remote biometric identification, emotion recognition or biometric categorisation should be ineligible for the criteria in Article 6(3) because they inevitably involve profiling. According to Recital 71 of the General Data Protection Regulation, profiling “consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.” Any system which uses biometric data for the purposes of remote biometric identification, emotion recognition or biometric categorisation, will involve some form of profiling and a severe infringement on fundamental rights to such an extent that no safeguards can make their use acceptable in a democratic, rule-of-law-respecting society. Therefore, they shall be declared unlawful and prohibited.
2	*Name/description* Post-remote biometric identification used in Austria https://www.derstandard.at/story/3000000275372/ngo-sieht-rechtswidrigen-einsatz-von-gesichtserkennung-bei-klimademo?ref=niewidget https://www.vol.at/data-protection-advocates-criticize-use-of-facial-recognition-at-climate-demonstration-in-vienna/9504071	*Category* Remote biometric identification (Point 1 (a))	*Category* Real time remote biometric identification system (Art. 5(1)(h))	*Explain* Austria operates a central facial recognition system that matches biometric data with a police image database containing over 600,000 photos, covering more than 8% of the population. These images originate from various sources, including police custody, identity checks, surveillance cameras, and other law enforcement contexts, with little public oversight. No court order is required for facial comparisons. Images remain in the system until the person turns 80, regardless of conviction. This amounts to lifetime biometric surveillance of potentially innocent individuals. The system has already caused harm: one Austrian was wrongfully arrested in Serbia after a false match. Similar errors have triggered domestic investigations against uninvolved persons. By enabling sensitive inferences, such as ethnicity, age, gender, or political affiliation, and lacking adequate safeguards, the system violates Articles 7, 8, and 11 of the EU Charter, Article 9 GDPR, and falls under Article 5(1)(g) of the EU AI Act, which prohibits biometric categorisation. This form of surveillance is incompatible with fundamental rights and principles and must be prohibited.
	Name/description Dialect recognition	*Category*	*Category*	*Explain* The system used by the the German Federal Office for Migration and Refugee for the examination of asylum applications. In full violation of the presumption of innocence, the dialect recognition systems is used to

3	used in Germany as biometric categorisation https://algorithmwatch.org/en/bamf-dialect-recognition/	Biometric categorisation (Point 1 (b))	Biometric categorisation system (Art. 5(1)(g))	verify that asylum applicants are from where they claim to be. The systems process voice data, which qualifies as biometric data, and assign the person to a country of origin, hence inferring ethnicity. Deductions/inferences of “race” should be interpreted to include inferences about “ethnicity”, hence dialect recognition systems are prohibited under Article 5(1)(g)
4	*Name/description* Authorisation of remote biometric identification by the Hungarian government against certain infractions, including at Pride	*Category* Remote biometric identification (Point 1 (a))	*Category* Real time remote biometric identification system (Art. 5(1)(h))	*Explain* The recent amendments to the Hungarian legal code have permitted the use of RBI in publicly accessible spaces by law enforcement. Whilst the Hungarian government has insisted that this does not contradict the EU AI Act, it is clear that the authorising law does not preclude such systems being used in real-time mode - therefore violating the strict requirements for narrow exemptions established in the AI Act. Given that for all intents and purposes it allowed near-instant identification of protesters on mass, the actual use of the system against people at Budapest pride further would amount to a real-time (i.e. prohibited) and not post (i.e. restricted) RBI use, despite government claims to the contrary. Furthermore, it is clear that the AI Act would not allow the use of *any* RBI system against a group of protesters.
5	*Name/description*	*Category* Remote biometric identification (Point 1 (a))	*Category* Real time remote biometric identification system (Art. 5(1)(h))	*Explain* As also noted in question 7, there are several uses of RBI that would be considered high-risk if used in certain ways, but prohibited in others. For example, prohibited uses would include: - Any use of post (retrospective) RBI which identifies people in a close-to instant way, or which scans non-suspect persons in a CCTV feed, video or other input; - Any use of RBI (live or post) by entities other than law enforcement.

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

The guidelines must clarify that the high-risk classification in Point 1 does not prejudice the prohibition of remote biometric identification systems, emotion recognition and biometric categorisation systems in Article 5, and in order to comply with rights enshrined in the Charter of Fundamental Rights of the EU. All systems mentioned in points a,b,c, without exception infringe on people's fundamental rights to such an extent that no safeguards can make their use acceptable in a democratic, rule-of-law-respecting society, as also reiterated in the EDPB-EDPS Joint Opinion 5/2021. Given the exceptions for law enforcement and migration authorities using systems under Point 1, 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 legal frameworks, i.e. Articles 13 & 14 of the GDPR, unless processing is conducted for law enforcement purposes, in which case the Law Enforcement Directive (LED) governs transparency requirements. When it comes to non-remote uses of biometric identification, guidelines should clarify that, to ensure regulatory consistency with the GDPR Article 9, these systems are considered as high-risk. The Guidelines must also clarify that all RBI for non-law enforcement purposes is prohibited by the same article.

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	*Name/description*	*Category* Evaluation of eligibility for public assistance benefits and services (Point 5(a))	*High-risk* Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*
2	*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*
3	*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*
4	*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))	*High-risk* Yes, completely Partially No	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*

		○ Evaluation and classification of emergency calls (Point 5(d))	○ Unsure				
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*
6	*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*
7	*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*
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	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*
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))	*High-risk* ○ Yes, completely ○ Partially ○ No	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*

		○ Evaluation and classification of emergency calls (Point 5(d))	○ Unsure				
10	*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*

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 d**istinction from prohibited AI systems**, in particular Art. 5(1)(c) AI Act, please specify

There is ample 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/zwyj4), fraud detection algorithms used by the Danish welfare agency (https://shorturl.at/A6GzB), similar systems used in Sweden (https://shorturl.at/wmjB9) and France (https://shorturl.at/mh8AP), with the Swedish case being currently being investigated by the Swedish Privacy Protection Authority (IMY) here on discrimination grounds (https://shorturl.at/AL6q2). The most recent example of social protection automation which has led to further marginalisation of people and communities, including persons with disabilities, those living in poverty or who have serious health conditions has been uncovered in the UK (https://shorturl.at/U8xkn), demonstrating how technology exacerbates the gaps and the lack of human rights compliance in the overall social security system (https://shorturl.at/Hi65x). As highlighted in the civil society input to the consultation on prohibited AI-practices, AI Act guidelines must reflect the state of play in Europe and clarify that risk profiling and fraud detection systems, including above-noted examples, amount to social scoring https://tinyurl.com/yn36vb4r) and should be banned (https://shorturl.at/762Nk). Even simpler systems such as Serbia's social card registry system (https://tinyurl.com/y2hmcb64) and the DUO system used in the Netherlands (https://tinyurl.com/urcvehu8) have led to discriminatory outcomes for Roma, racialised people and persons with disabilities. Given this, AI systems influencing decisions on people's access to essential services and benefits should by default 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. The exceptions made in Points 5(b) and (c), and mentioned in recital 58, create dangerous levels of inconsistencies in the level of protection that the AI Act should guarantee. There is no reasonable justification why similar systems in the context of the provision of financial services should not have to adhere to the same level of regulation and human rights safeguards, including be subject to prohibitions, let alone not even be considered high-risk. As noted in the AI Act itself, these systems have real-life consequences on "persons' access to financial resources or essential services such as housing, electricity, and telecommunication services" and risk leading to "discrimination between persons or groups" and perpetuating "historical patterns of discrimination, such as that based on racial or ethnic origins, gender, disabilities, age or sexual orientation, or may create new forms of discriminatory impacts.". Crucially, the deployment of these systems is based on the arbitrary and ungrounded premise that beneficiaries and applicants present a risk of fraud or abuse of provided services even before they apply for those services, disproportionately targeting people with migrant background, racialized people, persons with disabilities, and people experiencing poverty. By essence this violates the presumption of innocence and the right to non-discrimination.

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

This assessment should be based considering EU equality, data protection, and consumer rights laws, which are underpinned by the Charter of Fundamental Rights. While AI Act guidelines need to clarify that certain AI systems in this area amount to social scoring, some have already been challenged on the ground of violating data protection and non-discrimination rights (e.g. CNAF in France). More so, EU and Member States are bound by international human rights law, which is key when determining whether or not systems in this context

should be prohibited or considered high-risk. These frameworks include for example the the International Convention on the Elimination of All Forms of Racial Discrimination, International Covenant on Economic, Social and Cultural Rights, International Covenant on Civil and Political Rights, International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Conventions On The Rights Of Persons With Disabilities, on the Elimination of All Forms of Discrimination against Women, on the Rights of the Child, European Convention on Human Rights. Further, the guidelines must take into account the fact that AI systems are being deployed in already flawed and marginalising systems of social protection, therefore often amplifying existing structural harms and reinforcing punitive policies. Consequently, the guidelines must highlight the importance of avoiding technosolutionist approaches to complex systemic issues.

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* https://www.algorace.org/wp-content/uploads/2025/06/Report_Injustice-by-algorithm_JusticeandPolice-EN.pdf	*Category* ○ 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)	*Explain* As demonstrated under Q21, many risk scoring and fraud detection systems in the context of social protection should actually fall under the social scoring prohibition of the AI Act. These systems have also been challenged on the grounds of non-discrimination, equality, privacy and data protection and socio-economic rights. There is no reasonable justification why syimilar systems in the context of the provision of financial services should not have to adhere to the same level of regulation and human rights safeguards, including be subject to prohibitions, let alone not even be considered high-risk. As noted in the AI Act itself, these systems have real-life consequences on "persons' access to financial resources or essential services such as housing, electricity, and telecommunication services" and risk leading to "discrimination between persons or groups" and perpetuating "historical patterns of discrimination, such as that based on racial or ethnic origins, gender, disabilities, age or sexual orientation, or may create new forms of discriminatory impacts.". Crucially, the deployment of these systems is based on the arbitrary and ungrounded premise that beneficiaries and applicants present a risk of fraud or abuse of provided services even before they apply for those services, disproportionately targeting people with migrant background, racialized people, persons with disabilities, and people experiencing poverty. By essence this violates the presumption of innocence and the right to non-discrimination.
		Category ○ Exception of being intended for the purpose of detecting financial fraud (Point 5(b)) ○	

2	*Name/description*	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)	*Explain*
3	*Name/description*	*Category* ◯ 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	*Explain*

		undertakings' capital requirements (recital 58)	
4	*Name/description*	*Category* ○ 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)	*Explain*
		Category ○ Exception of being intended for the purpose of detecting financial fraud (Point 5(b)) ○ Exception of being intended for the purpose of detecting	

5	*Name/description*	fraud in the offering of financial services or for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements (recital 58)	*Explain*

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

EPV-R tool for gender-based violence in Basque country (Intimate Partner Femicide and Severe Violence Assessment). It supports authorities to decide on risk of severe re-incidence in cases of gender-based violence. https://www.algorace.org/wp-content/uploads/2025/06/Report_Injustice-by-algorithm_JusticeandPolice-EN.pdf

Category

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

High-risk

Yes, completely

Explain It is used in court to assess risk of “revictimisation” - or of “reincidence” - in gender-based violence cases, mostly to protect the victim: pending on the resulting level of risk, the Ertzaintza applies different protection measures for the victim which can include: interviews; arbitrary home visits and phone calls; individual transport to courts; 24/7 monitoring; and the assignment of escort patrols. Judges rely on it despite little transparency. Given the level of sensibility in which these systems are deployed (i.e. prevent gender-based violence) strict oversight and transparency rules must apply. The high-risk categorisation should also ensure that this type of application is included in a broader system of GBV prevention, led by the demands of feminist groups and civil society organisations.

Profiling

Yes

Exception

No

Explain

Name/description

VeriPol is an algorithmic system used by the Spanish National Police to detect allegedly false crime reports. It uses natural language processing techniques to scan the texts of reports on robbery, pickpocketing and purse snatching. It is effectively used as a lie detector. It was created to prevent fraud resulting from false reports. The main aim is to provide officers with a quick evaluation on whether or not a crime report is potentially false. In March 2025, it was reported that the National Police had stopped using VeriPol. The Spanish Ministry of the Interior said this was because the system lacked validity in judicial proceedings https://www.algorace.org/wp-content/uploads/2025/06/Report_Injustice-by-algorithm_JusticeandPolice-EN.pdf

Category

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

High-risk

Yes, completely

Explain VeriPol’s analysis predicts whether a person’ is likely lying on their crime report, based on prior patterns of false reports. It effectively automates credibility assessments and infers future criminal intent (fraud). VeriPol was trained on reports submitted to the police, which were manually catalogued by an officer as false or real. However, not all of those cases had been resolved, and so there was no objective or conclusive finding of truth or falsehood. The model was therefore built entirely using assumptions made by the police officer who catalogued the reports.137 It is remarkable that it took at least seven years for the Spanish authorities to recognise the problems with the system and halt its use. https://www.statewatch.org/media/4991/new-technology-old-injustice-25_6-english.pdf

Profiling

Yes

Exception

- Yes
- No
- Unsure

Explain Multiple studies have shown how natural language processing systems reproduce the biases that are inherent in society and represented in the language we use. In the case of Veripol, VeriPol’s creators suggest that the algorithm has a tendency to err towards classifying true reports as false. The ratio of false positives for VeriPol is 9.54%, which means that for every ten complaints analysed by the system, one is wrongly classified as false. Systems like this cannot be exempted from the high-risk classification. https://www.algorace.org/wp-content/uploads/2025/06/Report_Injustice-by-algorithm_JusticeandPolice-EN.pdf

Category

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))

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))

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

High-risk

Yes, completely
Partially
No
Unsure

Explain

Profiling

Yes
No
Unsure

Exception

Yes
No
Unsure

Explain

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

Name/description

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))

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))

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

High-risk

Yes, completely
Partially
No
Unsure

Explain

Profiling

Yes
No
Unsure

Exception

Yes
No
Unsure

Explain

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))

High-risk
- [ ] Yes, completely
- [ ] Partially
- [ ] No
- [ ] Unsure

Explain

Name/description

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	*Name/description* hessenDATA, a system that is used in Germany (Hesse State) to create extensive individual profiles on people. The system can show a record of known information about a person, including: when and where they have been stopped by police, record of arrests, whether they have ever been caught with drugs, and where they live. https://algorithmwatch.org/en/wp-content/uploads/2025/03/AlgorithmWatch_Report-Predictive-Policing.pdf	*Category* Profiling individuals in criminal investigations (Point 6(e))	*Category* Predicting criminal behaviour (Art. 5(1)(d))	*Explain* hessenDATA assembles personal and behavioural data into a risk profile used to assess future threats. This essentially serves as a pre-emptive classification tool based on assumptions about future behaviour, making it a form of individual-level behavioural prediction. It mirrors the logic of predictive policing, and its output can directly influence who is targeted by police interventions. https://www.statewatch.org/media/4991/new-technology-old-injustice-25_6-english.pdf
2	*Name/description* 'i-Police, in Belgium, has multiple functions, including: analysis and 'prediction' of patterns; predicting future crime for the purpose of 'prevention'; enabling monitoring and surveillance the allocation of police patrols, stops and checks; and other forms of intervention and enforcement https://www.liguedh.be/wp-content/uploads/2025/04/Predictive-justice-anglais.pdf	*Category* Profiling individuals in criminal investigations (Point 6(e))	*Category* Predicting criminal behaviour (Art. 5(1)(d))	*Explain* i-Police explicitly seeks to forecast future criminal activity and allocate policing resources accordingly. Though it is framed as 'prevention', it operationalises predictions about individual or group behaviours, directly aligning with the logic of predictive policing. Belgian police also profile people and groups and put them on specific databases, an issue considered in more depth below. This includes the use of these databases for so called 'urban gangs', a term laden with racism.People profiled as alleged 'gang' members have been targeted for monitoring, surveillance and increased stop and search. This use of AI anticipates and acts on assumed future crimes, in violation of Article 5(1)(d). Pag. 40 https://www.liguedh.be/wp-content/uploads/2025/04/Predictive-justice-anglais.pdf https://www.statewatch.org/media/4991/new-technology-old-injustice-25_6-english.pdf
	Name/description RisCanvi, a system used in Catalan prisons to 'predict' the risk of people re-offending. It is used to make decisions on parole, temporary release, and prisoner categorisation. This system is also known to discriminate on the basis of socio- economic	*Category*	*Category*	*Explain* RisCanvi assigns risk scores based on social and historical data to predict recidivism. From the risk score generated by combining these factors, the assessment department then decides what conditions to impose, such as eligibility for transfer to another prison, or for parole. In some cases, the risk scores are also included in reports received by judges when making decisions on release from

3	status or by association with others. It gives higher risk scores to people with a history of ‘unstable’ employment and finances, those without family or social support, and to people who have family members or parents with a criminal history	Assessing re-offending risk in law enforcements (Point 6 (d))	Predicting criminal behaviour (Art. 5(1)(d))	prison. This creates a mechanised assessment of future behaviour, which directly impacts liberty (like parole decisions). Its outputs are based on structural factors unrelated to individual guilt, thus embedding systemic discrimination and amounting to predictive policing. https://www.algorace.org/wp-content/uploads/2025/06 /Report_Injustice-by-algorithm_JusticeandPolice-EN.pdf
4	*Name/description* In Spanish prisons, a system called DRAVY is used to identify prisoners allegedly undergoing a process of so-called ‘jihadist’ radicalisation. As the main purpose of DRAVY is for assessing ‘jihadist’ radicalisation, it is fundamentally discriminatory on the basis that it is almost exclusively focused on Muslims	*Category* Profiling individuals in criminal investigations (Point 6(e))	*Category* Predicting criminal behaviour (Art. 5(1)(d))	*Explain* DRAVY functions as a predictive tool that classifies individuals based on assumed ideological paths, primarily targeting Muslims. The risk scores generated by DRAVY are used for making decisions about the level of individual monitoring of prisoners, defining security measures within facilities, and even probation decisionsIt lacks transparency and shows high error rates, marking people as high-risk based on ethnicity or religion. It typifies predictive policing and violates the prohibition against AI that makes decisions on future criminal acts based on profiling. The DRAVY system incorrectly predicts a high level of risk for almost half the people it assesses. https://www.algorace.org/wp-content/uploads/2025/06 /Report_Injustice-by-algorithm_JusticeandPolice-EN.pdf
5	*Name/description* Kriminalitätsbelastete Orte” (kbO) – “places affected by crime”, is a geographic crime ‘prediction’ data analysis used in Berlin, Germany. Berlin police classify certain locations allegedly affected by crime in the city as “Kriminalitätsbelastete Orte” (kbO) – “places affected by crime”. In kbOs the police are legally allowed to carry out identity checks and searches of people or objects in these locations regardless of any concrete suspicion – “depending on behavior”. Pre-Crime Observation System (PRECOBS) is a geographic crime ‘prediction’ system used by the Bavarian police, in Germany (discontinued in 2021) The system shows police officers a map with certain areas marked with different color codes, with the colors representing the different statistical	*Category* Profiling individuals in criminal investigations (Point 6(e))	*Category* Predicting criminal behaviour (Art. 5(1)(d))	*Explain* https://algorithmwatch.org/en/wp-content/uploads/2025/03 /AlgorithmWatch_Report-Predictive-Policing.pdf Places classified as kbO are usually frequented by a high proportion of people who are perceived as migrants. The stigmatization of a place by classifying it as ‘dangerous’ can in turn lead to harsh enforcement action by the police.Checks carried out by the police or other state authorities on the basis of racist attributions are supposed to be prohibited by law in Germany (Article 3 of the Basic Law). Discrimination exists “if the racial attribution was a criterion within a ‘bundle of motives’” (e.g., conspicuous luggage or behavior) for the decision to carry out a stop. A reference to skin color is generally not justifiable in police checks. However, this ban on discrimination is circumvented by location-based criminalization Geographic crime ‘prediction’ software such as PRECOBS does not necessarily establish chronic risk areas that the police perceive as permanent hotspots, patrol regularly and thus establish them in the long term – instead, the software-supported forecasts can guide patrols to more narrowly-defined and changeable areas such as streets (hotspots) allegedly prone to future burglaries that the police did not necessarily have on their radar. Given the lack of

	probabilities, or ‘predictions’ calculated by the system as to whether crimes will occur in these areas in the near future. https://algorithmwatch.org/en/wp-content/uploads/2025/03/AlgorithmWatch_Report-Predictive-Policing.pdf			scientific evidence, therefore, whether ‘predictive’ policing actually works is questionable. Furthermore, although the systems do not collect any personal data and instead refer to geographic areas, the checks in the alleged risk zones can still have discriminatory effects on individuals, given the existing structural and institutional discrimination by police in Germany towards people from racially minoritized backgrounds. Police suspicion towards racially minoritized people in those areas, for example, can reinforce racial profiling and police targeting of marginalized communities

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 i**nterplay 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

There is the need to clarify the interplay between Annex III Point 6 and the prohibition under Article 5(1)(d) on AI used for predictive policing. Most systems listed under Point 6 (such as for profiling, assessing reoffending risk, evaluating the reliability of evidence) operate as de facto tools to predict behavioural analysis, relying on past data, socio-economic indicators, or group-based characteristics to anticipate future actions. EU Law and national anti-discrimination frameworks apply, as well as the framework against police violence and brutality. The EU Charter of Fundamental Rights (Articles 7, 8, 21, 47), the Racial and ethnic equality Directive (2000/43 /EC), and national constitutional protections prohibit discrimination (even if indirect via these type of systems), as well as IHRL and the Charter, which forbid arbitrary interferences with FR, including data protection and privacy. The guidelines must clarify that the uses of high-risk systems by law enforcement authorities must be viewed within the wider context of police violence and brutality in the EU (https://shorturl.at/GkBTq). The guidelines should also clarify how the above mentioned human rights frameworks would comply with the exemptions from transparency obligations for law enforcement agencies allowed by Article 49 (4) of the AI Act. Unless adequate transparency and oversight is established for uses of AI systems under Point 6, these systems should be prohibited.

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

The guidelines should clarify what actors would be considered as 'acting on behalf of competent public authorities [...]' and in what context this applies. Clarify that private companies to which migration management is outsourced to fall within scope. For example: involvement of private military companies in Cyprus (https://shorturl.at/cah6Z), contractors that operate EU migration databases (https://shorturl.at/5YIgK), cooperative managing the detention center in Albania (https://shorturl.at/VOUCk). This resource provides an overview of private companies that should fall under the definition of 'acting on behalf of competent public authorities [...]' (https://shorturl.at/arUiX). Clarify that international organisations that implement EU migration policies are within scope, such as: the International Organization for Migration (https://www.iom.int/project), the International Centre for Migration Policy Development (https://shorturl.at/kMJG2), Civipol (https://www.civipol.fr/en/missions-and-projects/projects). The guidelines should also clarify that 'Union agencies' apply to Frontex, Europol and eu-LISA, and that obligations arising from the high-risk classification should apply to all the above-mentioned actors implementing EU migration policies also outside of the EU territory and in the context of EU bi/multilateral agreements. Examples: Frontex's operations in West Africa (https://shorturl.at/KmFC6); projects under EU Trust Fund for Africa (https://shorturl.at/eC6H9).

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	*Category*	*High-risk*		*Profiling*	*Exception*	
Mobile phone data extraction against asylum seekers in Germany https://freiheitsrechte.org/en/themen/digitale-grundrechte/refugee-daten	Assisting with asylum and visa applications (Point 7(c))	Yes, completely	*Explain* In 2023, the German Federal Administrative Court ruled illegal the practice of regularly analysing data carriers (https://shorturl.at/ubLs4) , including mobile phones, of asylum seekers. (https://shorturl.at/Tm7Jr). Data extracted was used to inform decision on the asylum application.	Yes No Unsure	Yes No Unsure	*Explain*
Name/description	*Category*	*High-risk*		*Profiling*	*Exception*	
Mobile phone data extraction against asylum seekers in the UK	Assisting with asylum and visa applications (Point 7(c))	Yes, completely	*Explain* In 2022, the UK High Court found unlawful the seizures of asylum seekers' phones, in breach of Article 8 ECHR and UK data protection laws, as did the extraction and analysis of data from the phones to inform the decision on the asylum application (https://privacyinternational.org/legal-action/r-hm-and-ma-and-kh-v-secretary-state-home-department) .	Yes No Unsure	Yes No Unsure	*Explain*
Name/description	*Category*	*High-risk*		*Profiling*	*Exception*	
Drones in border patrolling	Identifying individuals in migration and border control (Point 7(d))	Yes, completely	*Explain* Since 2018, human rights organisation Border Violence Monitoring Network has collected 38 testimonies impacting over 1,000 people where drones were detected prior to an illegal pushback, as a means of facilitating the location and apprehension of a transit group'. https://borderviolence.eu/reports/eu-member-states-use-of-new-technologies-in-enforced-disappearances/	Yes No Unsure	Yes No Unsure	*Explain*
Name/description	*Category*	*High-risk*		*Profiling*	*Exception*	
Drones in border patrolling in the Central Mediterranean https://www.hrw.org/news/2022/12/12/eu-frontex-complicit-abuse-libya	Identifying individuals in migration and border control (Point 7(d))	Yes, completely	*Explain* Human Rights Watch and Border Forensics denounced the use of unmanned drones in the Central Mediterranean by Frontex, which led to the interception of people escaping from Libya. With the use of border surveillance systems, Frontext facilitated the interception and consequent push back of asylum seekers escaping Libya. https://www.hrw.org/video-photos/interactive/2022/12/08/airborne-complicity-frontex-aerial-surveillance-enables-abuse	Yes No Unsure	Yes No Unsure	*Explain*
Name/description	*Category*	*High-risk*		*Profiling*	*Exception*	
AI-powered thermal cameras/Night vision systems	Identifying individuals in migration and border control (Point 7(d))	Yes, completely	*Explain* Thermal cameras are used to locate and apprehend groups of migrants transiting through the Western Balkans, specifically between Croatia and Bosnia (https://shorturl.at/NHgYT)	Yes No Unsure	Yes No Unsure	*Explain*
Name/description	*Category*	*High-risk*		*Profiling*	*Exception*	
			Explain In 2019, the EU inked a deal to provide nearly 20 million euros' (about $21.4 million) worth of radar, undersea and airborne drones, radios and other technology, as well as training, to the			

Situational awareness systems provided by ICMPD in Northern Africa https://www.codastory.com/authoritarian-tech/icmpd-eu-refugee-policy/	Identifying individuals in migration and border control (Point 7(d))	Yes, completely	government of Tunisia. EU officials made a similar agreement with Moroccan authorities. The Border Management Programme for the Maghreb region was designed to arm coast guard authorities in North Africa with new technology to be deployed along migration routes to Europe and to train them to use it.	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*

Category	*High-risk*					
Name/description AI-powered radars to detect refugee boats in the Aegean sea	Identifying individuals in migration and border control (Point 7(d))	Yes, completely	*Explain* Radars used ie. to detect boats on the Aegean sea around Cyprus. see for example Cyprus BorderScape https://cyprusborderscape.com/interactive-map	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*

Category	*High-risk*					
Name/description AI-supported analytics (e.g. threat detection, movement detection) developed within EU-funded projects on border surveillance	Identifying individuals in migration and border control (Point 7(d))	Yes, completely	*Explain* EU funded projects such as Trespass (https://trespass-project.eu/) or ROBORDER (https://roborder.eu/) aim at developing autonomous border surveillance system with unmanned mobile robots including aerial, water surface, underwater and ground vehicles which will incorporate multimodal sensors as part of an interoperable network	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*

Category	*High-risk*					
Name/description Mobile fingerprint and face scanners provided by migration authorities in Greece	Identifying individuals in migration and border control (Point 7(d))	Yes, completely	*Explain* In 2021, the Hellenic police (Greece) procured devices to scan the fingerprints of people stopped in the street. The risks of procedural abuses and discrimination are high, so it is essential that police using these devices are properly equipped with safeguards and also that the machines are robust and tested. (https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights)	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*

Category	*High-risk*					
Name/description	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))	Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*

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	*Name/description* Netherlands Visa Risk Scoring - social scoring related to the trustworthiness of a visa applicant to not overstay the visa	*Category* Assessing risks for individuals entering a Member State (Point 7 (b))	*Category* Social scoring (Art. 5(1) (c))	*Explain* This use of visa risk scoring amounts to social scoring related to the trustworthiness of a visa applicant to not overstay the visa. The evaluation is based on personal characteristics (nationality) that lead to indirect discrimination, as nationality is a proxy for race. Applicants from Morocco and Suriname were consistently ranked as 'high-risk', and were automatically moved to an "intensive track" subject 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 classify as 'high score' individuals deemed as at 'risk' of applying asylum, therefore breaching the right to seek international protection. Unjustified treatment included extensive investigation, delay, unfair rejection, therefore breaching the right to a good administration.
2	*Name/description* ETIAS Risk Profiling The ETIAS Regulation enables profiling to categorise travellers into pre-defined risk profiles related to purported migration, security or public health risks. This profiling takes place with a number of factors, including historical data on rates of over-staying or refusal and information provided by Member States as to security risks. https://onlinelibrary.wiley.com/doi/10.1111/eulj.12513 ETIAS Risk Profiling The ETIAS Regulation enables profiling to categorise travellers into pre-defined risk profiles related to purported migration, security or public health risks. This profiling takes place with a	*Category*	*Category*	*Explain* The ETIAS Regulation enables profiling to categorise travellers into pre-defined risk profiles related to purported migration, security or public health risks. This profiling takes place with a number of factors, including historical data on rates of over-staying or refusal and information provided by Member States as to security risks. Predicts risk in 'pre-crime' areas, as many aspects of migration are criminalised at the EU level, the profiling happening in ETIAS seeks to predict likelihood of

	number of factors, including historical data on rates of over-staying or refusal and information provided by Member States as to security risks. https://onlinelibrary.wiley.com/doi/10.1111/eulj.12513	Assessing risks for individuals entering a Member State (Point 7 (b))	Social scoring (Art. 5(1) (c))	criminality, illegality, overstaying, or security risks in the future. As such, profiling occurs based on a number of factors, generating risk scores which have an outcome for the individual, including potential criminal outcomes, not based on actual criminal behaviour but nationality, level of education and other characteristics.
3	*Name/description* I Border Control (https://shorturl.at/MAoCt) This was a pilot project designed to perform emotion recognition of people travelling to the EU and predict if they are being truthful in their immigration interviews. The purpose of the system was to assist border guards in their job to assess immigration applications.	*Category* Assessing risks for individuals entering a Member State (Point 7 (b))	*Category* Other	*Explain* iBorderCTRL amounts to emotion recognition and it should therefore be prohibited. It clearly falls within the definition of an emotion recognition system, and it is in a workplace context (the system is being used for the work of the border guard) where there is a profound power imbalance
4	*Name/description* Dialect recognition system used by the German Federal Office for Migration and Refugee for the examination of asylum applications. The systems process voice data to assign the person to a country of origin. https://algorithmwatch.org/en/bamf-dialect-recognition/	*Category* Assisting with asylum and visa applications (Point 7(c))	*Category* Other	*Explain* Dialect recognition amounts to biometric categorisation and should therefore be prohibited, The processing of voice data qualifies as biometric data, and is processed in real time during the asylum interview. The system is based on an inference of ethnicity and “race”, and thus violates Article 5(1)(g). The system also violates the presumption of innocence.
5	*Name/description* ITFlows, predictive analytics systems used to forecast migration movements https://www.accessnow.org/open-letter-itflows-consortium/	*Category* Identifying individuals in migration and border control (Point 7(d))	*Category* Other	*Explain* AI-based systems to predict migration flows hold a serious risk of leading to punitive migration responses, such as violence at the borders and push-backs. These risks have also been indicated by the Horizon 2020 project ITFlows, which is building a migration forecasting tool. Following an external preliminary impact assessment, the ITFlows Consortium itself indicated that the use of the forecasting tools could jeopardise a number of fundamental rights, as per the image below (see pag. 10). https://www.itflows.eu/wp-content/uploads/2022/07/7.-D2.3-ITFLOWS-R.pdf

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

The guidelines should specify that the EU Charter on Fundamental Rights, International Human Rights Law and national constitutional protections against-discrimination are the guiding basis that leads the implementation of the AI Act when it comes to uses of high-risk systems under Point 7 . The guidelines should also specify that the uses of high-risk systems by migration, asylum and border management authorities (and other authorities implementing EU migration policies) must be viewed within the wider context of discrimination, border violence, racism and prejudice in the European Union. Against this background, the guidelines should clarify how the above mentioned human rights frameworks would comply with the exemptions from transparency obligations for migration, asylum and border management agencies allowed by Article 49 (4) of the AI Act. Unless adequate transparency and oversight is established for uses of AI systems under Point 6, these systems should be prohibited.

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

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

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

When it comes to the use of post remote biometric identification allowed for per Article 26, the guidelines should clarify the specific and limited conditions under which the authorisation might be granted. In order to constitute permitted (but still restricted) post RBI such a system could only be used to analyse stills (i.e. screen grabs) of individual faces only of persons suspected of serious crimes, ensuring that no non-suspect persons faces or other features are analysed. The entirety of the footage could not be analysed, as this would entail untargeted analysis, which is not allowed under Article 26. What's more, even if such a use case is not specifically prohibited under the AI Act, we reiterate that it would still be unlawful under the Charter if, for example, the system has lower rates of effectiveness for certain demographics (e.g. people of colour) or if it is used disproportionately against those groups. In accordance with the Law Enforcement Directive, no decision can be taken which would have a legal effect solely on the basis of this system. The exceptions to the in-principle prohibition therefore need to meet an extremely high threshold. In a situation such as an imminent, genuine and foreseeable threat of a terror attack, there must still not be any permanent RBI infrastructure. Instead, the infrastructure must be temporary, clearly marked, and must meet all the criteria for authorisation, safeguards, limitations in geographic scope etc in order to meet requirements of strict necessity and proportionality. Any uses not meeting these strict criteria would still be prohibited. The Guidelines should clarify that the authorisation provided for in Artcile 26 does apply to the problematic uses discussed in question 8, which in fact amount to a prohibited practice. Specifically Article 26 does not apply to the case of Austria which operates a central facial recognition system that matches biometric data with a police image database containing over 600,000 photos (originating from various sources, with little public oversight), where no court order is required for facial comparisons - because of which wrongful arrest took place, and the identification of climate activist taking part in a protest in Vienna in 2023 (https://shorturl.at/G5tGC). It also does not apply to Hungary, as the recent amendments to the Hungarian legal code, permits the use of RBI in publicly accessible spaces by law enforcement. Whilst the Hungarian government has insisted that this does not contradict the EU AI Act as it because of it is ‘near-instant nature’, the guidelines must specify that this type of uses do not fall under the provided for in Article 26 but rather it is considered prohibited practice under Article 5 and Recital 17.

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

In light of the exemptions provided for in Article 49 (4) for law enforcement and migration authorities, the guidelines must clarify how Article 26 complies with existing Union and national law which impose transparency obligations when the above mentioned public authorities act as deployers. While Article 26 seeks to establish obligations for deployers to ensure safety, human oversight and the maintenance of sound technical standards, Article 49 (4) exempts said authorities from disclosing crucial documentation, namely: a summary of the findings of the fundamental rights impact assessment conducted in accordance with Article 27, as well as of the data protection impact assessment carried out in accordance with Article 35 of GDPR and Article 27 of LED; a summary of the main characteristics of the plan for testing in real world conditions. Article 49 (4) allows exempts also providers from documentation which is key for the fulfilment of deployer’s obligations as laid out in Article 26, namely: a basic and concise description of the information used by the system (data, inputs) and its operating logic; the type, number and expiry date of the certificate issued by the notified body and the name or identification number of that notified body, and a scanned copy of said certificate; a short summary of the

grounds on which the AI system is considered to be not-high-risk in application of the procedure under Article 6 (3); information over the status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled). 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 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). Guidelines should clarify what 'sensitive operational data' used in the context of post RBI under Article 26 (10) refer to to avoid the creation of loopholes and ensure any restricted use of retrospective RBI is duly documented and market surveillance authorities can exercise oversight over it.

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

Learning from practical pilots, deployers need both detailed guidance on how to conduct a FRIA, as well as regulatory certainty about what measures are sufficient to demonstrate compliance. We encourage the AI Office to address the foundational question about the objective of the template as a first step before developing its scope and content. We emphasise the need for FRIA to include not only the template but also guidance and examples. Quality: To prevent the risk of superficial compliance, the template should focus on outlining clear procedural steps and standards and move beyond yes/no checklists, including space for open-ended responses, documentation of deliberation, and context-specific analysis. It must require deployers to update the FRIA following significant changes in the system or its deployment. Stakeholder engagement: Apart from identifying affected groups and relevant risks, deployers should document efforts to actively involve those groups in the FRIA process describing how both internal and external stakeholders - esp. affected communities, fundamental rights experts, and CSOs - were engaged, as well as whose voices may be missing, how power imbalances were addressed, whether stakeholders had access to relevant information, and what resources were allocated to support participation. Article 77 bodies should also be involved, 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. The template must include fields for explaining the necessity and proportionality of the system and of residual risk, along with a mitigation and redress plan. This plan must outline actionable steps in case of fundamental rights infringements and must be publicly available.Use of providers' FRIAs: While Article 27(2) allows reuse of FRIAs conducted by providers, this must not bypass deployers' obligations to assess context-specific risks. The template should require explanation of how the provider's FRIA was used,

what additional risks were identified, and what communication occurred between the two parties to ensure a complete understanding of system limitations and impacts.Transparency: Transparency is essential for public trust and oversight. The template must clarify what must be made public, and under what conditions information can be withheld. It should require clear justification for redactions and ensure that full FRIA documentation is accessible to competent authorities, incl. Art. 77 bodies. Importantly, the template should provide a mechanism for individuals to access relevant information about their rights and redress channels. Oversight: To ensure accountability, the template must include sections documenting whether the FRIA underwent external review and how complaints mechanisms are structured. Deployers should also indicate any communication with market surveillance or art. 77 authorities in cases of unresolved risks

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

1. Clarify distinct but complementary scopes The FRIA and the DPIA differ in focus and function, and this distinction must be articulated in the guidance: In practice, DPIAs primarily address privacy and data protection risks, including data minimisation, lawfulness, and discrimination as it relates to personal data processing. FRIAs have a broader function to assess impacts on the full spectrum of fundamental rights, including dignity, social protection, equality, freedom of expression, access to essential services, and more. High risk AI systems can have negative fundamental rights impacts that are not strictly related to the processing of personal data (e. g. impacts related to the displacement of workers as result of the introduction of a new AI system). While FRIA will benefit from the analysis carried out in a DPIA, a DPIA might not be sufficient to fully capture the expectations under the AI Act. 2. Promote synergy between DPIA and FRIA processes For efficiency and information-sharing purposes, deployers should 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, it is important that the broader scope of FRIA be reflected in the competencies of the team doing the assessment (incl. fundamental rights expertise), the broader nature of stakeholder engagement to be conducted (including not only data subjects but also affected and/or vulnerable groups), and the specification of mitigation measures. From a documentation perspective, there would be more legal certainty if deployers produced different documentation for the two processes (which means tolerating a certain level of overlap in terms of documentation). The reason is that (i) organisations have already developed bespoke DPIA tools which vary across jurisdictions and might be reluctant to switch to a joint DPIA/FRIA template, (ii) there is no certainty that DPAs will exercise oversight over FRIAs given that the landscape of setting up MSAs for enforcing the AI Act is still in motion across different jurisdictions. 3. Promote synergy between providers and deployers 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

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 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 Court introduced a balancing test, weakening absolute trade secret protection when it conflicts with transparency rights - an approach that should be reflected in future guidelines.

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

‘Substantial changes’ to an AI System should be defined as ‘substantial modifications’ of the output of the model and hence the performance and impact of the model. This is crucial, as a small change to the code of the model, ie. the architecture or the optimisation method used, can yield big differences on the output side. This is equally true for the training process, the training data and the data processing part. In fact, models that were trained under only slightly different conditions are often cherry picked for their good performance on specific metrics to be the final model, for example if a model is retrained with different seeds or the training data or training data processing is modified. Hence, we stress that even minor modifications to the code, including the architecture of the model, the optimisation process, as well as changes to the data (pre)processing, the training data and the training process can lead to ‘substantial changes’ of the model output (https://dl.acm.org/doi/abs/10.1145/3447548.3470817, https://link.springer.com/article/10.1007/s11831-024-10110-w) . Hence, these changes should be considered as resulting in ‘substantial modifications of the AI system’. The 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 harm without adequate protection or accountability. The Guidelines must explicitly define any modification that leads to the reclassification of an AI system as high-risk as a “substantial modification.” Apart from being integrated in GPAI systems, LLM models or other algorithmic systems can also be integrated in high-risk AI systems. Given the rapid pace of advancement in large language models (LLMs) and other algorithmic systems , it is expected that companies will regularly replace or upgrade the underlying models in their AI systems to take advantage of improved or different performance and reasoning capabilities. Guidelines should explicitly state that any upgrade or change to an AI system involving the integration of a new or changed LLM is considered a substantial modification under the AI Act, even more crucially so, when LLM plays a crucial role in decision-making.

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

First, ‘continue to learn’ should be defined very narrowly. Any change to the way the model does ‘continue to learn’ in terms of minor modifications to the code, including the architecture of the model, the optimisation or learning process, as well as changes to the data (pre)processing, the training data for the online learning and the training process should be considered as resulting in ‘substantial modifications of the AI system’, as in this case there is effectively no difference between changes to online and offline learning. Second, continuous learning can lead to ‘substantial modifications’ to the output of the model as we have seen many times, most recently with the Grok Hitler case (https://www.npr.org/2025/07/09/nx-s1-5462609/grok-elon-musk-antisemitic-racist-content). Therefore, the changes that should be considered substantial shall, as stressed under Q44,

always focus on the ‘substantial change’ to the output and thereby impact of the model. However, since continuous learning constitutes a constant modification of the training data set of the model (https://www.sciencedirect.com/science/article/abs/pii/S0925231221006706), which has a significant impact on the mode output, these models need to be subject to additional measures. It is a well established fact that with the training data changing, the model quality changes (https://dl.acm.org/doi/abs/10.1145/3447548.3470817).Therefore, AI systems with ‘continuous learning’ should need to undergo a new conformity assessment at least once every 6 months and constant testing in terms of output quality and in case of any ‘substantial changes’ to the output the model shall be considered having a ‘substantial modification’ and undergo a new conformity assessment.

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 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. It would have been more appropriate for the European Commission to reflect this reality without undue skew of the questionnaire towards economic actors to ensure a meaningful consultation process. Despite this shortcoming, answers provided under this section address challenges to human 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. One issue that has come up as a prominent concern in the relationship between developers and deployers of AI systems is the opacity of government procurement of AI tools. Research from civil society organisations and journalists has demonstrated how across the public sector, agencies commonly rely upon public-private collaborations or purchase off-the-shelf commercial offerings such as Predpol (in the law enforcement context https://shorturl.at/anVf6). Amnesty International’s research into the Danish welfare agency UDK (https://shorturl.at/7n7Ti) alongside other examples from social security agencies around the world, has highlighted the challenges that arise from public-private sector collaborations. First, private sector collaboration can exacerbate opacity given commercial secrecy exemptions that commonly exist under Freedom of Information legislative acts. Further, the distributed responsibilities over the design,

development and ownership of the AI systems can create a lack of clearly delineated responsibilities and obligations on conducting rigorous risk mitigation measures, as well as related to liability in case of harm.

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

When discussing value chain responsibilities and relevant liability and compliance measures, it is vital to emphasise the harmful trend of downgrading corporate sustainability rules (CSDDD), withdrawing the AI Liability Directive, the Horizontal Equal Treatment Directive, and calls for pausing, delaying, and even revisiting established AI Act safeguards. Proposed changes to the CSDDD have been denounced as “catastrophic” given their risk of eroding human rights and environmental protections (https://shorturl.at/sHjmx). Civil society has also highlighted the unrealistic expectation for people to identify, prove and challenge discriminatory use of AI systems without an appropriate regulatory framework for civil liability applicable to AI systems (https://shorturl.at/rSKPG). Changes to the newly adopted AI Act risk watering down the few protections established in the Act, leading to discriminatory outcomes for people and legal uncertainty amongst developers and deployers. As AI technologies depend on resource extraction for their development, when examining and addressing upstream impacts in the value chain, extractive practices that risk labour rights and the environment, including outside of the EU must be considered. In relation to labour rights, the category of ‘ghost work’ in the tech sector – invisible or hidden labour, usually performed by precarious or otherwise vulnerable workers – is a phenomenon that demonstrates how the sector instrumentalises and capitalises upon weak protections for workers. In the supply chain of many social media and tech companies it typically refers to image labellers, content moderators, and other tasks that are key to training and maintaining the AI systems these companies are using. Regarding resource extraction, the environmental impact of AI’s production as it comes with a heavy carbon footprint. This is incurred partially by the hardware component of AI and the raw materials mined to build it, but also significantly by the energy costs of powering data centres and carbon emissions of training large models. Therefore, it is crucial to address the environmental costs posed by the development of AI systems and surrounding infrastructure when discussing value chain relationships and responsibilities (https://shorturl.at/QtsWy). For downstream impact, export of AI systems developed in the EU must be addressed. Companies based in EU countries have been known to provide rights-violating technologies, including biometrics surveillance tools to states which use them to target and oppress marginalized communities, with notable examples in China and the Occupied Palestinian Territory (https://shorturl.at/ZZWgB), as well as uses by Union agencies acting outside of the EU territory (https://shorturl.at/oXDm6). Exporters must be considered part of the value chain under EU AI rules, to avoid export of prohibited technologies and ensure exported high-risk systems meet the same technical and procedural safeguards.

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

Non-remote uses of biometric identification systems must be added in Annex III. Biometric identification is not the same as verification (sometimes known as 1:1 matching), which includes things like unlocking your phone or using a passport with a biometric chip to go through the ePassport gate at an airport. Biometric identification is a process of comparing one's data to multiple other sets of data (1:many) in some form of database. Non remote uses of biometric identification carry dangerous risks of discrimination, unlawful and disproportionate surveillance as well as data leaks. Considering Articles 7 (2) (e) and (h), biometrics identification systems by law enforcement authorities are already proven to increase racial profiling practices and discriminatory stop-and-search practices, as ethnicity or skin colour is viewed as a proxy for an individual's migration status or a link to criminal behaviour proved to discriminate against [https://racialjusticenetwork.co.uk/reports/7027/]. Considering Article 7 (2) (b) the likelihood for these systems to be used by police and migration authorities is

extremely high as biometric identification has been indicated as priority in the framework of EU home affairs and migration policies. Moreover, Annex III should include predictive analytics systems used to forecast migration, other than those that could lead to the interdiction of border crossings which should instead be prohibited (see Question 53). Predictive analytic systems may deploy a range of methods, including data mining, predictive modelling and machine learning, and process different forms of data including social media data, and data in relation to past events and trends. Systems used to generate predictions as to migration flows may have vast consequences for fundamental rights and access to international protection procedures. Often these systems influence how resources are assessed and allocated in the migration control and international protection contexts. Incorrect assessments about migration trends and reception needs will have significant consequences for the preparedness of Member States, but also for the likelihood that individuals can access international protection and numerous other fundamental rights. Examples include displacement forecast model designed by the Danish Refugee Council https://drc.ngo/what-we-do/innovation/digital-innovation/foresight-displacement-forecasts/ .

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

Please justify why you consider that the use case needs to be adapted in order to fulfil the conditions as per Article 7(3) AI Act

3000 character(s) maximum

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

It is of utmost importance that the Guidelines specify that the current list of prohibited practices must be safeguarded by any attempt to undermine it. The purpose of prohibitions is to prevent any harm - amending Article 5 as suggested by Question 54 would fundamentally risk the AI Act capacity to anticipate and prevent harm. Given the irreversible harm caused by AI applications currently not prohibited, the following systems should be added to Article 5. Firstly, location-focused methods of 'predictive' policing, as abundant evidence proves existing uses disproportionately target and criminalise racially minoritised and low-income people and communities(see examples from Belgium, France, Germany and Spain https://shorturl.at/oIabY). Secondly, retrospective biometric identification, as the use of these systems produces a chilling effect in society on how comfortable we feel attending a protest, seeking healthcare — such as abortion in places where it is criminalised — or speaking with a journalist (https://shorturl.at/979DT). These systems have already been proved to interfere with the right to assembly (Article 12 of the EU Charter) in Austria, as the system was used to identify a climate activist attending a protest (https://shorturl.at/G5tGC), while other EU countries threaten to deploy them as part of new rights-violating legislations aimed at limiting people's freedom of association and assembly, e.g. Hungary's legal code (https://shorturl.at/UuiYR) and the Italian Security Decree (https://shorturl.at/XBITJ). Thirdly, emotion recognition must be banned when used by migration and law enforcement authorities. It remains incomprehensible that the prohibition does not cover these areas, where the power balance and negative consequences are most extreme. Fourthly, the prohibition on social scoring must include scoring practices in the welfare (https://shorturl.at/A6GzB) and in the migration contexts, such as during visa procedures (https://shorturl.at/guayd). Finally, AI-based systems to predict migration movements in the context of border management hold a serious risk of leading to punitive migration responses, such as violence at the borders and push-backs. These risks have also been indicated by the Horizon 2020 project ITFlows, which built a migration forecasting tool. Following an external preliminary impact assessment, the ITFlows Consortium itself indicated that the use of the forecasting tools could jeopardise a number of fundamental rights, as per the image below (see pag. 10 https://shorturl.at/oFAz1).

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

Contact

Contact Form