Contribution ID: 862ecb69-c369-4008-8a33-d0e10c81bb62
Date: 18/07/2025 11:42:40

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

Eleftherios

* Surname

Chelioudakis

* Email address

e.chelioudakis@homodigitalis.gr

* 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

Homo Digitalis

* 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

EL - Greece

* Select the size of the organisation

Micro (0-9 employees)

* Sector(s) of activity

- [x] Information technology
- [ ] Employment
- [ ] Transport

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

* Describe the activities of your organisation or yourself

1300 character(s) maximum

Founded in 2018, Homo Digitalis focuses on promoting and defending human rights in the modern digital era in Greece. Through the three pillars of our actions, namely,a) raising awareness, b) shaping policy decisions, and c) strategic legal interventions, we aim to strengthen the protection of fundamental rights and freedoms for everyone, both in the digital and physical worlds, when new technologies, including artificial intelligence applications, are used by private or public entities. Homo Digitalis is the only full member in Greece of European Digital Rights (EDRi), the largest international association of organizations defending and promoting digital rights. We are also members of the South East Europe (SSE) Digital Rights Network and the Europeana Network Association (ENA)

---

* 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.*

- [x] Questions in relation to **Annex I of the AI Act.** (Section 1)
- [x] Questions in relation to **Annex III of the AI Act.** (Section 2)
- [ ] Questions on **horizontal aspects** of the high-risk classification. (Section 3)
- [x] Questions in relation to **requirements and obligations for high-risk AI systems and value chain obligations**. (Section 4)
- [x] 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 1. Questions in relation to the classification rules of high-risk AI systems in Article 6(1) AI Act and Annex I to the AI Act

According to Article 6(1) AI Act, irrespective of whether an AI system is placed on the market or put into service independently of the products referred to in points (a) and (b), that AI system shall be considered to be high-risk where both of the following conditions are fulfilled:

*a) the AI system is intended to be used as a **safety component** of a product, or the AI system is itself a product, covered by the Union harmonisation legislation listed in Annex I;*

*b) the product whose safety component pursuant to point 1 is the AI system, or the AI system itself as a product, is required to undergo a **third-party conformity assessment**, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonisation legislation listed in Annex I.*

Question 1. Do you consider yourself being already or becoming in the future a provider or a deployer of AI systems covered by Annex I of the AI Act (e.g. machinery, medical devices, toys, lifts, etc.)?

- ( ) Yes
- (•) No

Regarding the first condition 'safety component' for classification of a high-risk AI system, Article 6(1)(a) AI Act provides two options:

- *Either the AI system is intended to be used as a **safety component of a product covered by the Union harmonisation legislation listed in Annex I.***
- *Or the AI system **itself is a product**, covered by Union harmonisation legislation listed in Annex I.*

Question 2. The AI Act defines a 'safety component' as follows (Article 3(14) AI Act): *'safety component of a product or system' means a component of a product or of a system which fulfils a safety function for that*

product or system, or the failure or malfunctioning of which endangers the health and safety of persons or property. Based on this definition, in your opinion, what components listed below are covered by the AI Act definition of a 'safety component'?

- [x] A component of a product or of a system which is intended to **monitor and detect** situations which may lead to physical harm to people or property (e.g. AI system detecting abnormal system behaviour);
- [x] A component of a product or of a system which is intended to **monitor and detect** the need to schedule maintenance and inspections, which, if not conducted, may lead to physical harm to people or property (e.g. AI system detecting whether parts of a product are worn and may need replacement or maintenance);
- [x] A component of a product or of a system which is intended to **prevent** a physical harm to people or property (e. g. AI system preventing a start of a system if an abnormal behaviour is detected);
- [x] A component of a product or of a system which is intended to **control or limit** possible physical harm to people or property (e.g. AI system controlling specific behaviour or function of a system and adjusting its function accordingly);
- [x] A component of a product or of a system which is intended to **mitigate consequences** of possible physical harm to people or property (e.g. AI system that triggers action such as safe-stop if dangerous condition occurs);
- [x] A component of a product or of a system which **controls or supervises** another system that performs a safety function (e.g. AI systems supervisor through sensors an operation in real time of a safety component that directly performs the safety function);
- [x] A component of a product or of a system that **optimises a performance of a product** (e.g. efficiency; user preferences) but the failure of which would not directly lead to risks to health or safety of persons or property;
- [x] A component of a product or of a system that is critical for the **core functionality of the product** (whether or not related to safety);
- [ ] Other
- [ ] Can't answer this question.

Question 3. Do you have or know practical examples of AI systems that in your opinion are a **component** that is part of **a product** covered by Union harmonisation legislation listed in Annex I of the AI Act, which has to undergo a third-party conformity assessment, and that **fulfils a safety function**?

	The respective Union harmonisation legislation	Short description of the use case	Points where you need further clarification
1	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
	Legislation's name ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU		

2	○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
3	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*

	○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139		
4	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
	Legislation's name ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU		

5	○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
6	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*

	○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139		
7	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
	Legislation's name ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU		

8	○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
9	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*

	○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139		
10	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*

If you have more examples, please enter them in the section below, following the structure of question 3.

Question 4. The AI Act defines a **'safety component'** as follows (Article 3(14) AI Act): 'safety component of a product or system' means a component of a product or of a system which fulfils a safety function for that product or system, or the failure or malfunctioning of which endangers the health and safety of persons or property.

Do you have or know concrete examples of AI systems that in your opinion are **components** that are part of **a product** covered by Union harmonisation legislation listed in Annex I of the AI Act that **do not fulfil a safety function**, but whose **failure or malfunctioning may endanger the health and safety of persons or property**?

	The respective Union harmonisation legislation	Short description of the use case	Points where you need further clarification
1	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*

2	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
	Legislation's name ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425		

3	○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
4	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*

	○ Regulation (EU) 2018/1139		
5	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
	Legislation's name ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424		

6	○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
7	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*

	○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139		
8	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
	Legislation's name ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU		

9	○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
10	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*

	○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139		

If you have more examples, please enter them in the section below, following the structure of question 4.

*Regarding AI systems that are a component of an **AI system that is itself a product** covered by Union harmonisation legislation listed in Annex I:*

Question 5. Do you have or know practical examples of an AI system that in your opinion is **itself a product** covered by Union harmonisation legislation listed in Annex I of the AI Act, and that has to undergo a third-party conformity assessment pursuant to the Union harmonisation legislation listed in Annex I of the AI Act?

	The respective Union harmonisation legislation	Short description of the use case	Points where you need further clarification
1	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
	Legislation's name ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU		

2	○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
3	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*

	○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139		
4	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
	Legislation's name ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU		

5	○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
6	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*

	○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139		
7	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
	Legislation's name ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU		

8	○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*
9	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*

	○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139		
10	*Legislation's name* ○ Directive 2006/42/EC ○ Directive 2009/48/EC ○ Directive 2013/53/EU ○ Directive 2014/33/EU ○ Directive 2014/34/EU ○ Directive 2014/53/EU ○ Directive 2014/68/EU ○ Regulation (EU) 2016/424 ○ Regulation (EU) 2016/425 ○ Regulation (EU) 2016/426 ○ Regulation (EU) 2017/745 ○ Regulation (EU) 2017/746 ○ Regulation (EC) No 300/2008 ○ Regulation (EU) No 168/2013 ○ Regulation (EU) No 167/2013 ○ Directive 2014/90/EU ○ Directive (EU) 2016/797 ○ Regulation (EU) 2018/858 ○ Regulation (EU) 2019/2144 ○ Regulation (EU) 2018/1139	*Description* *750 character(s) maximum*	*Explain* *500 character(s) maximum*

If you have more examples, please enter them in the section below, following the structure of question 5.

Question 6. Do you have any additional feedback or suggestions for developing guidelines to support the implementation of Article 6(1) of the AI Act? If you do, please specify what specific elements of the definition require further clarification.

3000 character(s) maximum

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
- [x] 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
- [x] 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* Smart policing project enabling facial recognition and fingerprint identification Smart policing project enabling facial recognition and fingerprint identification Smart policing project enabling facial recognition and fingerprint identification https://edri.org/our-work/facial-recognition-homo-digitalis-calls-on-greek-dpa-to-speak-up/ https://homodigitalis.gr/posts/5125/ https://www.astynomia.gr/images/stories/2018/prokirikseis18/12042018-texn_prod.	*Category* Remote biometric identification (Point 1 (a))	*High-risk* Yes, completely	*Explain* In 2019, the Greek police signed a €4 million contract for a smart policing project with Intracom Telecom, a global provider of telecommunications systems and solutions. According to the press release issued by the Greek police, 75% of the project is financed by the European Commission's Internal Security Fund (ISF) 2014-2020. This smart policing project consists of portable devices enabling the use of facial recognition and automated fingerprint identification technologies during police stops. More precisely, police officers will be able to use these devices during police stops in urban environments to take a photograph of an individual's face and/or collect their fingerprints. The fingerprints and the photographs collected are compared with data stored in national, EU, and third-country databases for identification purposes, such as SIS II, VIS and EURODAC. The tender call even makes references to databases held by Europol, international organisations like Interpol, or even databases of institutions of third countries, such as the FBI. The police is presenting this project as a more "efficient" way to identify people, compared to the current procedure which consists of bringing any individuals who do not carry identification documents with them to the nearest police station. Apart from fingerprints, it is important to highlight that these devices offer the capacity for police officers to use photographs of faces to search individuals on a police database or to scan an individual's face to search her/him on a police database. Specifically, as clearly noted in the document describing the technical specifications of the project, the devices: • Offer the possibility to send photographs to SIS II and other police databases, • Enable police officers to upload photograph files either through a dialog window, or by drag-and-drop (including in bulk), • Provide for the possibility to conduct bulk search based on multiple photos. • Provide for a facial recognition software that should support the definition of thresholds (matching scores), above which the software's response will be automatically returned without requiring confirmation by specialized personnel. The technical specifications' document does not clarify the distance at which such photos would be taken or whether the individuals shall be aware of the data collection process. However, the technical details provided, could suggest that remote photo capture, followed by analysis, could be an option. More precisely, according to the document, the vendor is required to provide software that will allow for (1) editing, processing, and enhancing the photographs, (2) applying forensic filters to improve the photographs, and (3) using forensic methods to enhance the images and conduct searches on a watchlist. Moreover, as one of the developers from	*Profiling* No	*Exception* No	*Explain* Homo Digitalis claims that the processing of biometric data, such as the data described in the contract, is allowed only when the three criteria of Article 10 of Directive 2016/680 are met: It is authorised by Union or Member State law; it is strictly necessary; and it is subject to appropriate safeguards for the rights and freedoms of the individuals concerned. None of the above-mentioned criteria are applicable in this case. Moreover, journalist Eftychia Soufleri has written a detailed article for NEWS247.gr (THE MAGAZINE) shedding light on the case and highlighting the key actions taken by Homo Digitalis since 2019. According to the report, despite the absence of any legal framework allowing their use, the Hellenic Police: Claims to have been using the devices operationally since 2021, even though the Hellenic Data Protection Authority (HDPA) has been investigating the matter since August 2020 and continues to do so today. Confirms that it fully utilizes the biometric

	pdf https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights#:~:text=(Athens)%20%E2%80%93%20Greece%20is%20planning,and%20Homo%20Digitalis%20said%20today			Intracom-Telecom, who worked in this project under a technical manager role, has stated, “This IT solution enabled police officers to perform personal inquiries on the field from their mobile phones using face, finger, or textual input”. The IT solution as was also described as a “face recognition app of smart policing”. It is understood that these devices clearly provide to the Hellenic Police the capacity to search individuals based on photos taken or the scanning of faces. Such photos could in theory be taken remotely, too, and then be uploaded to the platform to conduct searches, allowing for remote biometric identification. Such a capacity could have an immense chilling effect on public assemblies, since a police officer could in theory take a photo of a person, without her/his consent, and then upload his/her photo to the system and conduct related searches in police databases. Such searches could be related to any person, whose data are on police databases, including Greek passport holders or the holders of Greek IDs (since their facial images are collected in central police databases). Thus, it would be important to further clarify with the Hellenic Police related facial recognition functionalities and assess the Data Protection Impact Assessment of this project. In terms of timeline, these devices have already been piloted and were delivered to the Hellenic Police in September 2021.			processing capabilities of these devices (facial recognition, fingerprint identification). Validates what was outlined in the 2018 technical specifications document, namely that the devices are used for “preventive policing”, with the collected data potentially being used in the future to establish correlations, conclusions, and predictive analytics. We are still awaiting the Hellenic Data Protection Authority’s decision, as its investigation has now lasted almost 5 years (initiated in August 2020). The situation is escalating rapidly, and the risks to democracy and human rights protection are extremely high.
							Explain The EU legislator, through the provisions of Regulation 2024/1689, seeks to include within the definition of biometric data those data collected in the context of biometric categorization of individuals. Specifically, as explicitly stated in Recital 14, Regulation 2024/1689 provides that the concept of "biometric data" should be interpreted in light of the definitions found in Article 4 of Regulation 2016/679, Article 3 of Regulation 2018/1725, and Article 3 of Directive 2016/680. It further clarifies that biometric data may enable the verification of identity, identification, or categorization of natural persons, as well as the recognition of their emotional states. Notably, the definition

2	*Name/description* CENTAUROS - AI behavioral analysis system deployed by the Hellenic Ministry of Asylum and Migration in the Greek islands and mainland, where Closed Controlled Access Centers (CCACs) hosting asylum seekers are.	*Category* Emotion recognition (Point 1(c))	*High-risk* Yes, completely	*Explain* CENTAUROS is a multi-tool surveillance system composed of CCTV cameras, drones, and Artificial Intelligence-based Behavioral Analytics software. It monitors the perimeter and assembly areas of the CCACs. Using footage from the cameras, the AI algorithm analyzes individuals' movements (e.g., how they walk or behave) to predict behavioral traits, such as detecting when a fight has started or is likely to start in an assembly area. The system is designed to automatically signal alarms, flagging potentially unlawful behavior based on this analysis, enabling the deployment of drones and personnel to assess the situation. In February 2022, Homo Digitalis had filed a complaint before the Hellenic DPA against the Ministry of Immigration and Asylum for the "Centaurus" and "Hyperion" systems deployed in the reception and accommodation facilities for asylum seekers, in cooperation with the civil society organizations Hellenic League for Human Rights and HIAS Greece, as well as the academic Niovi Vavoula. In April 2024, the Hellenic DPA identified significant GDPR violations in this case by the Ministry of Immigration and Asylum and decided to impose a fine of €175.000 euro, the then highest ever imposed against a public body in the country. Together with I HAVE RIGHTS, Homo Digitalis is monitoring currently the lack of compliance of the Ministry of Asylum and Migration and we published last month a related report. https://homodigitalis.gr/en/posts/10874/ https://edri.org/our-work/greek-ministry-of-asylum-and-migration-face-a-record-breaking-e175000-fine-for-the-border-management-systems-kentauros-hyperion/ https://ihaverights.eu/border-tech-data-violations/	*Profiling* Yes	*Exception* No	of biometric data given in Article 3 of Regulation 2024/1689 makes no reference to the element of "unique identification" of an individual, which was a necessary component of the definition under the existing legal framework. Specifically, Article 3 defines biometric data as " personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data;." The same article defines a "biometric categorization system" as an "AI system for the purpose of assigning natural persons to specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons;" Neither of these definitions makes any reference to "unique identification." This leads to the conclusion that Regulation 2024/1689 explicitly aims to protect personal data resulting from specific technical processing related to the physical, physiological, or behavioral characteristics of a natural person, such as facial images or fingerprint data, or body posture and body movement data, that are not collected for the purpose of unique identification, but rather for the purpose of categorization or profiling of people (behavioral /emotional profiling and other types).

3	*Name/description* Haut.AI – AI Skin Analysis Tool	*Category* Biometric categorisation (Point 1 (b))	*High-risk* Yes, completely	*Explain* Infers sensitive physical traits (e.g., skin condition, age, ethnicity); use for beauty/health profiling	*Profiling* Yes	*Exception* Unsure	*Explain* Clarification needed on the scope of “targeted” law enforcement use
4	*Name/description* AnyVision (Oosto)	*Category* Remote biometric identification (Point 1 (a))	*High-risk* Yes, completely	*Explain* Used in stadiums and public venues for identification; often in real-time	*Profiling* Yes	*Exception* No	*Explain* Clarification needed on the scope of “targeted” law enforcement use
5	*Name/description* Realeyes	*Category* Emotion recognition (Point 1(c))	*High-risk* Yes, completely	*Explain* Identifies emotions for marketing campaigns	*Profiling* Yes	*Exception* No	*Explain* Unclear whether it qualifies as prohibited “emotion inference”
6	*Name/description* DeepSight AI	*Category* Biometric categorisation (Point 1 (b))	*High-risk* Yes, completely	*Explain* Real-time categorisation in retail; profiling by behavior	*Profiling* Yes	*Exception* No	*Explain* “Strict necessity” exemption likely not met
7	*Name/description* Entropik Tech	*Category* Emotion recognition (Point 1(c))	*High-risk* Yes, completely	*Explain* Emotion profiling in advertising and behavior targeting	*Profiling* Yes	*Exception* No	*Explain* Risk of manipulation; blurred line with prohibited affective computing
8	*Name/description* Kairos	*Category* Biometric categorisation (Point 1 (b))	*High-risk* Yes, completely	*Explain* Offers ethnicity-based profiling; could fall under Art. 5(1)(g)	*Profiling* Yes	*Exception* No	*Explain* Inference of ethnicity clearly aligns with GDPR Article 9(1); potentially prohibited
9		*Category*	*High-risk*		*Profiling*	*Exception*	*Explain* Are SDK providers liable under the AI

	Name/description Face++	Remote biometric identification (Point 1 (a))	Yes, completely	*Explain* Widely used SDK for real-time facial recognition	Yes	No	Act or only deployers?
10	*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*

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* Smart Policing devices of the Hellenic Police	*Category* Remote biometric identification (Point 1 (a))	*Category* Real time remote biometric identification system (Art. 5(1)(h))	*Explain* One could argue that, in the absence of necessary safeguards, the photographs used for facial recognition could theoretically be captured remotely and uploaded to the platform for real-time searches, thereby enabling real-time remote biometric identification—an activity that falls under the prohibited practices set out in Article 5.
2	*Name/description* Realeyes	*Category* Emotion recognition (Point 1(c))	*Category* Emotion inference system (Art. 5(1)(f))	*Explain* Infers emotional states for marketing—requires clarity on boundaries.
3	*Name/description* Dialect recognition used in Germany as biometric categorisation https://algorithmwatch.org/en/bamf-dialect-recognition/	*Category* Biometric categorisation (Point 1 (b))	*Category* Biometric categorisation system (Art. 5(1)(g))	*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 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* Kairos	*Category* Biometric categorisation (Point 1 (b))	*Category* Biometric categorisation system (Art. 5(1)(g))	*Explain* Offers ethnicity prediction; raises risk under GDPR Article 9(1).
	Name/description Authorisation of remote	*Category*	*Category*	*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

5	biometric identification by the Hungarian government against certain infractions, including at Pride	Remote biometric identification (Point 1 (a))	Real time remote biometric identification system (Art. 5(1)(h))	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. What's more, these developments in Hungary build on a) the systemic suppression of legitimate dissent / democratic counter-speech as part of wider rule of law breaches and b) the systemic persecution and suppression of the LGBTQI+ community. https://edri.org/our-work/open-letter-the-european-commission-must-act-now-to-defend-fundamental-rights-in-hungary/ https://edri.org/wp-content/uploads/2025/06/Legal-analysis-FRT-in-Hungary-and-AI-Act.pdf

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. Lastly, need guidance on the expansion of the definition of biometric data (see details in question 2a. 2, column 2 (CENTAUROS use-case).

2.D Questions related to employment, workers' management and access to self-employment

The classification of AI systems as high-risk under Annex III(4) AI Act targets certain AI systems which are intended to be used in different contexts of employment, workers' management and access to self-employment. Certain AI systems as listed in points 4(a) and 4(b) should also be classified as high-risk, since those systems may have an appreciable impact on future career prospects, livelihoods of those persons and workers' rights.

Additionally, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation.

Point 4 of Annex III to the AI Act distinguishes between two different types of use cases in the field of employment that are classified as high-risk.

- *Point 4(a) of Annex III to the AI Act refers to AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates.*

- *Point 4(b) of Annex III to the AI Act refers to AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual*

relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.

Question 17. Please provide practical examples of AI systems that in your opinion may fall within the scope of high-risk AI systems related to employment, workers' management and access to self-employment.

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
Hellenic Ministry's of Interior Ministry of Interior for the use of artificial intelligence algorithms for the reallocation of employees in the public sector

Category
Managing work relationships and performance monitoring (Point 4 (b))

High-risk
Yes, completely

Explain On 9 July Homo Digitalis filed a request (no. 5812/9.7.2024) before the Greek Data Protection Authority, in order for the latter to exercise its investigative powers against the Ministry of Interior. In particular, following the Authority's Decision 16/2024 in April 2024, by which it had imposed a record fine of 400,000 euros on the Ministry of Interior for significant breaches of data protection legislation, the Ministry is again in the spotlight, this time for the artificial intelligence tool it is developing for strategic staffing planning in the public sector. The tool concerns the reallocation of existing staff and the estimation of the needs for new staff, while it will be piloted in 9 public sector institutions, namely the Development Programmes Organisation and Management Unit, the Independent Public Expenditure Authority, the Public Employment Service, the Athens General Hospital "G. Gennimatas Hospital, the Municipality of Thessaloniki, the Region of Attica, the Ministry of Education and Religious Affairs, the Ministry of Environment and Energy and the Ministry of Culture and Sports. The pilot has been finalised already and the project is expected to be completed in December 2025, at a cost of €11,708,543 and deployed to the rest of the public sector. Because the tool needs to include functionalities for the collection, management and analysis of personal data, Homo Digitalis had filed a letter on 15 April 2024 before the then Minister of Interior Ms.Kerameos and the Data Protection Officer of the Ministry, in which it raised key questions regarding both the compliance required with the legislation on the protection of personal data and the legislation on the use of artificial intelligence and other emerging technologies in the public sector (Law 4961/2022). However, the Ministry did not provide any response, even after a written reminder of our request on 30 May, forcing us to address the DPA to investigate thoroughly the development, implementation and piloting of this tool and the implications for the rights of public sector employees. See more https://homodigitalis.gr/en/posts/133375/

Profiling
Yes

Exception
No

Explain

Name/description

Category
- ○ Recruitment/ selection of natural persons (Point 4(a))
- ○ Managing work relationships and performance monitoring (Point 4(b))

High-risk
- ○ Yes, completely
- ○ Partially
- ○ No
- ○ Unsure

Explain

Profiling
- ○ Yes
- ○ No
- ○ Unsure

Exception
- ○ Yes
- ○ No
- ○ Unsure

Explain

Category
- ○ Recruitment/ selection of natural persons (Point 4(a))
- ○

High-risk
- ○ Yes, completely
- ○

Profiling
- ○ Yes

Exception
- ○ Yes

Name/description

Managing work relationships and performance monitoring (Point 4(b))

Partially
No
Unsure

Explain

No
Unsure

No
Unsure

Explain

Category

Recruitment/ selection of natural persons (Point 4(a))
Managing work relationships and performance monitoring (Point 4(b))

High-risk

Yes, completely
Partially
No
Unsure

Name/description

Explain

Profiling

Yes
No
Unsure

Exception

Yes
No
Unsure

Explain

Category

Recruitment/ selection of natural persons (Point 4(a))
Managing work relationships and performance monitoring (Point 4(b))

High-risk

Yes, completely
Partially
No
Unsure

Name/description

Explain

Profiling

Yes
No
Unsure

Exception

Yes
No
Unsure

Explain

Category

Recruitment/ selection of natural persons (Point 4(a))

High-risk

Yes, completely

Profiling

Yes

Exception

Yes

Name/description

Managing work relationships and performance monitoring (Point 4(b))

Partially
No
Unsure

Explain

No
Unsure

No
Unsure

Explain

Category

Recruitment/ selection of natural persons (Point 4(a))
Managing work relationships and performance monitoring (Point 4(b))

High-risk

Yes, completely
Partially
No
Unsure

Profiling

Yes
No
Unsure

Exception

Yes
No
Unsure

Name/description

Explain

Explain

Category

Recruitment/ selection of natural persons (Point 4(a))
Managing work relationships and performance monitoring (Point 4(b))

High-risk

Yes, completely
Partially
No
Unsure

Profiling

Yes
No
Unsure

Exception

Yes
No
Unsure

Name/description

Explain

Explain

Category

Recruitment/ selection of natural persons (Point 4(a))

High-risk

Yes, completely

Profiling

Yes

Exception

Yes

Name/description

Managing work relationships and performance monitoring (Point 4(b))

Partially
- No
- Unsure

Explain

Name/description

Category
- Recruitment/ selection of natural persons (Point 4(a))
- Managing work relationships and performance monitoring (Point 4(b))

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

Explain

- No
- Unsure

- No
- Unsure

Explain

Profiling
- Yes
- No
- Unsure

Exception
- Yes
- No
- Unsure

Explain

Question 18. Do you have or know practical examples of AI systems related to employment, workers' management and access to self-employment 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*	*Category* Managing work relationships and performance monitoring (Point 4(b))	*Category* ○ Subliminal techniques (Art. 5(1)(a)) ○ Exploitation of vulnerabilities (Art. 5(1)(b)) ○ Social scoring (Art. 5(1)(c)) ○ Other	*Explain*
2	*Name/description*	*Category* ○ Recruitment/ selection of natural persons (Point 4(a)) ○ Managing work relationships and performance monitoring (Point 4 (b))	*Category* ○ Subliminal techniques (Art. 5(1)(a)) ○ Exploitation of vulnerabilities (Art. 5(1)(b)) ○ Social scoring (Art. 5(1)(c)) ○ Other	*Explain*
3	*Name/description*	*Category* ○ Recruitment/ selection of natural persons (Point 4(a)) ○ Managing work relationships and performance monitoring (Point 4 (b))	*Category* ○ Subliminal techniques (Art. 5(1)(a)) ○ Exploitation of vulnerabilities (Art. 5(1)(b)) ○ Social scoring (Art. 5(1)(c)) ○ Other	*Explain*
4	*Name/description*	*Category* ○ Recruitment/ selection of natural persons (Point 4(a)) ○ Managing work relationships and performance monitoring (Point 4 (b))	*Category* ○ Subliminal techniques (Art. 5(1)(a)) ○ Exploitation of vulnerabilities (Art. 5(1)(b)) ○ Social scoring (Art. 5(1)(c)) ○ Other	*Explain*
5	*Name/description*	*Category* ○ Recruitment/ selection of natural persons (Point 4(a)) ○ Managing work relationships and performance monitoring (Point 4 (b))	*Category* ○ Subliminal techniques (Art. 5(1)(a)) ○ Exploitation of vulnerabilities (Art. 5(1)(b)) ○ Social scoring (Art. 5(1)(c)) ○ Other	*Explain*

Question 19. 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

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* Eligibility engine for social housing: AI system that evaluates applicant profiles for eligibility, urgency level, and prioritization for social housing units based on income, household size, age, employment status, and location.	*Category* Evaluation of eligibility for public assistance benefits and services (Point 5(a))	*High-risk* Yes, completely	*Explain* Directly impacts access to essential housing benefits and often substitutes or significantly influences human decision-making.	*Profiling* Yes	*Exception* No	*Explain* Involves automated profiling and decisions without falling into exceptions under Art. 6(3).
2	*Name/description* Automated creditworthiness scoring for online rental platforms: Used by private landlords to assess applicants based on open banking data, social media behavior, and payment history.	*Category* Evaluation of creditworthiness/ credit score of natural persons (Point 5(b))	*High-risk* Partially	*Explain* Impacts access to essential housing in private rental markets. While not a public authority, the output can significantly limit access to a basic need.	*Profiling* Yes	*Exception* Unsure	*Explain* Clarification needed whether these uses are sufficiently covered if not used by financial institutions.
3	*Name/description* Health insurance dynamic pricing engine: Predicts premiums based on age, location, behavior inferred from wearable data and online health searches	*Category* Risk assessment and pricing in relation to natural persons for life/health insurance (Point 5 (c))	*High-risk* Yes, completely	*Explain* AI system assesses and personalizes costs, which can discourage coverage or create exclusionary pricing	*Profiling* Yes	*Exception* No	*Explain* Explicitly covered by 5(c); not fraud-related.
4	*Name/description* Call triage system in emergency response centers: Classifies 112 calls using natural language processing to assign urgency level and route responders.	*Category* Evaluation and classification of emergency calls (Point 5(d))	*High-risk* Yes, completely	*Explain* Decisions made by the AI system directly affect emergency care prioritization, with potential health and safety implications.	*Profiling* No	*Exception* No	*Explain* Essential function; clear fit under 5(d).
5	*Name/description* Unemployment benefits recommender system: Suggests approval, rejection, or further review of unemployment claims based on digital dossiers and behavioral data.	*Category* Evaluation of eligibility for public assistance benefits and services (Point 5(a))	*High-risk* Yes, completely	*Explain* System mediates access to essential social security benefits and may replace nuanced human judgment.	*Profiling* Yes	*Exception* No	*Explain* Significant impact on fundamental rights; no exception under Art. 6(3).
	Name/description Banking app-based microloan approval system: Uses mobile data (app usage, call metadata, GPS	*Category*	*High-risk*	*Explain* System targets financially excluded populations, affects access to	*Profiling*	*Exception*	*Explain* Clarification needed whether purpose

6	patterns) to infer creditworthiness.	Evaluation of creditworthiness/ credit score of natural persons (Point 5(b))	Partially	essential credit, but falls in a grey area regarding profiling justification.	Yes	Unsure	qualifies under fraud-detection exemption.
7	*Name/description* AI risk model in life insurance: Predicts individual risk based on genomic data, lifestyle markers, and socio-demographic inputs.	*Category* Risk assessment and pricing in relation to natural persons for life/health insurance (Point 5 (c))	*High-risk* Yes, completely	*Explain* Discriminatory pricing or denial of coverage could result, affecting health security and affordability.	*Profiling* Yes	*Exception* No	*Explain* Not intended for fraud detection; therefore high-risk.
8	*Name/description* AI tool prioritizing home-care service allocation: Used by local authorities to distribute limited in-home care hours.	*Category* Evaluation of eligibility for public assistance benefits and services (Point 5(a))	*High-risk* Yes, completely	*Explain* AI influences the distribution of care resources essential for dependent or elderly persons.	*Profiling* Yes	*Exception* No	*Explain* Access to essential care services; likely includes profiling.
9	*Name/description* Mental health crisis triage chatbot: Uses natural language understanding to assess severity and urgency of chat-based contacts with emergency mental health services.	*Category* Evaluation and classification of emergency calls (Point 5(d))	*High-risk* Yes, completely	*Explain* Directs mental health intervention responses, carries risk of misclassification.	*Profiling* No	*Exception* No	*Explain* Fits emergency triage function.
10	*Name/description* Public health preventive screening recommender: Suggests personalized invitations for preventive screenings (e.g., mammograms) based on population segmentation.	*Category* Evaluation of eligibility for public assistance benefits and services (Point 5(a))	*High-risk* Yes, completely	*Explain* While not directly denying access, can influence uptake and prioritize certain groups.	*Profiling* Yes	*Exception* Unsure	*Explain* Clarification needed whether this qualifies under exception criteria based on indirect influence.

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

The deployment of high-risk AI systems in essential private and public services raises uncertainty about how to consistently apply the obligations under the AI Act. The following examples highlight use cases where further clarification would help implementers and regulators apply requirements effectively: 1. Automated Eligibility and Prioritization for Social Benefits Public administrations increasingly use AI to support eligibility checks, prioritization, and fraud detection in distributing social benefits (e.g. housing assistance, disability support). While classified as high-risk, many of these systems are integrated into complex workflows with human caseworkers. Clarification needed: What level of transparency and human oversight is expected when the AI output is used as a recommendation rather than a final decision? Should traceability and logging requirements differ for systems used in batch versus real-time processing? 2. AI-Based Credit Scoring for Essential Financial Services Banks and fintech platforms use AI to assess loan eligibility or set credit limits for consumers seeking essential services such as overdrafts or installment payments. These systems often rely on behavioral or proxy indicators, which can be difficult to audit for fairness. Clarification needed: - How should providers demonstrate appropriate risk management when using inferred or third-party features in credit scoring models? - What level of input feature transparency is required to comply with explainability obligations? 3. Personalized Health Insurance Pricing Models Private insurers use AI to classify customers into premium tiers or policy groups using data from wearables, lifestyle questionnaires, or medical history. These applications affect access to critical health-related financial services. Clarification needed: - What constitutes adequate model monitoring and documentation when using dynamically adapting pricing algorithms? - Should specific rules apply to ensure stability and predictability over long-term service access? 4. Education Admission and Resource Allocation Tools Public and private institutions are adopting AI to screen candidates for scholarships, limited-capacity courses, and educational support programs. These systems may include engagement metrics or socioeconomic proxies. Clarification needed: - Are there minimum standards for fairness auditing or bias mitigation in education-related high-risk systems? - Should AI that filters access to publicly funded education or vocational training be subject to stricter conformity assessment criteria? Conclusion These examples reflect recurring areas where high-risk classification is clear, but practical implementation of AI Act obligations—such as transparency, oversight, traceability, and data quality—requires sector-specific guidance. Greater clarity would support consistent compliance and ensure trust in AI deployments across essential services.

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

Yes, clarification is needed on the interplay between Annex III(5) of the AI Act and Union legislation such as the GDPR (Regulation (EU) 2016/679) and the Charter of Fundamental Rights, particularly regarding automated decisions in essential services. For example, Article 22 GDPR restricts decisions based solely on automated processing that produce legal or similarly significant effects — a threshold often triggered in Annex III(5) scenarios. However, the AI Act does not fully clarify how obligations under Articles 26–27 (e.g., human oversight, fundamental rights impact assessments) relate to or complement Article 22 safeguards. In particular, high-risk AI systems used to evaluate eligibility for public assistance (Annex III(5)(a)) often involve processing sensitive personal data and may function in tension with Article 9 GDPR prohibitions unless specific derogations apply. Where AI systems operate with partial human involvement, it is unclear whether such involvement is sufficient to avoid triggering Article 22, and whether the AI Act's oversight obligations suffice to meet the GDPR's requirements for meaningful human review. In conclusion, clearer guidance is needed to resolve these overlaps and to ensure legal certainty for deployers regarding compliance, considering EU

equality, data protection, and consumer rights laws, which are underpinned by the Charter of Fundamental Rights. More so, EU and MSs are bound by international human rights law that should comply with.

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*	*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*
2	*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*
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 undertakings' capital requirements (recital 58)	*Explain*
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*
5	*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*

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
Hellenic Coast Guard Smart Bot for social media monitoring

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

High-risk
Yes, completely

Explain In February 2022, researcher Phoebus Simeonidis discovered a social media monitoring tender call of the Hellenic Coast Guard. According to this tender, the goal of the Hellenic Coast Guard is to use this AI- enabled software for profiling individuals, surveilling the exchange of information on migration matters in social media channels and instant messaging applications, as well as for predicting migration flows towards Greece. The cost of the project is more than 726.000 euro (including VAT), while it is partially funded by the ISF. Homo Digitalis, Privacy International, the Hellenic League for Human Rights HIAS Greece and researcher Phoebus Simeonidis collectively submitted a request before the Hellenic Data Protection Authority to investigate this case and assess its compliance with the applicable rules on data protection. The Hellenic DPA officially informed the coalition that it is investigating the case since the very beginning, while it is close to concluding its assessment. In the meanwhile, BYTE, jointly with the Greek company GRIVAS, was awarded the contract. • More info https://homodigitalis.gr/en/posts/132775/

Profiling
Yes

Exception
No

Explain

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.

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

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
No

Explain

Category
- Assessing victim risk in law

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

Name/description

Smart policing project enabling facial recognition and fingerprint identification

Category

- Assessing victim risk in law enforcement (Point 6(a))
- Polygraph use in law enforcement (Point 6(b))
- Evaluating of evidence reliability in

High-risk

- Yes, completely
- Partially
- No
- Unsure

Explain

Profiling

- Yes
- No
- Unsure

Exception

- Yes
- No
- Unsure

Explain

High-risk

- Yes, completely

Profiling

Exception

Name/description

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 enforcements (Point 6(d))
-

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

Explain

Name/description

Profiling
- Yes
- No
- Unsure

Exception
- Yes
- No
- Unsure

Explain

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

Category

- Assessing victim risk in law

Profiling

- Yes
- No
- Unsure

Exception

- Yes
- No
- Unsure

Explain

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))

Name/description

Category
- Assessing victim risk in law enforcement (Point 6(a))
- Polygraph use in law enforcement (Point 6(b))
- Evaluating of evidence reliability in

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

Explain

Profiling
- Yes
- No
- Unsure

Exception
- Yes
- No
- Unsure

Explain

High-risk
- Yes, completely

Profiling

Exception

Name/description

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 enforcements (Point 6(d))
-

- Partially
- No
- Unsure

Explain

Yes
- No
- Unsure

Yes
- No
- Unsure

Explain

Name/description

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

Explain

Profiling
- Yes
- No
- Unsure

Exception
- Yes
- No
- Unsure

Explain

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

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	*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

3	discriminate on the basis of socio- economic 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))	decisions on release from 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”. 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* 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 https://algorithmwatch.org/en/wp-content/uploads/2025/03/AlgorithmWatch_Report-Predictive-Policing.pdf

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
Hellenic Coast Guard Smart Bot for social media monitoring

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

High-risk
Yes, completely

Explain In February 2022, researcher Phoebus Simeonidis discovered a social media monitoring tender call of the Hellenic Coast Guard. According to this tender, the goal of the Hellenic Coast Guard is to use this AI- enabled software for profiling individuals, surveilling the exchange of information on migration matters in social media channels and instant messaging applications, as well as for predicting migration flows towards Greece. The cost of the project is more than 726.000 euro (including VAT), while it is partially funded by the ISF. Homo Digitalis, Privacy International, the Hellenic League for Human Rights HIAS Greece and researcher Phoebus Simeonidis collectively submitted a request before the Hellenic Data Protection Authority to investigate this case and assess its compliance with the applicable rules on data protection. The Hellenic DPA officially informed the coalition that it is investigating the case since the very beginning, while it is close to concluding its assessment. In the meanwhile, BYTE, jointly with the Greek company GRIVAS, was awarded the contract. • More info https://homodigitalis.gr/en/posts/132775/

Profiling
Yes

Exception
No

Explain

Name/description
Automated Border Surveillance Systems (ABSS) Pylons in Evros, Greece

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

High-risk
Yes, completely

Explain https://borderviolence.eu/reports/surveillance-technologies-at-european-borders-evros/

Profiling
Yes

Exception
No

Explain

Name/description
Mobile phone extraction tools enable police and border management officials to download content and associated data from people's phones. It involves the use of 'push-button' extraction tools, retention and analysis of data extracted from a phone and cloud-stored data. Such technologies enable police and others to obtain device information, phonebooks, call logs, texts, videos and photos, audio files,

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

High-risk
Yes, completely

Explain Several European countries persist in screening the mobile phones of asylum seekers. According to the European Migration Network's 2017 report, mobile phone screening was standard practice in the Netherlands and Estonia, and optional in Croatia, Germany, Lithuania and Norway. In Latvia and Luxembourg, mobile phones were confiscated in the context of criminal procedures. Research shows that data analysis of mobile phone content has been implemented in the Netherlands, Germany, Norway, and, to some extent, Denmark and the UK. Belgium, Austria and Switzerland have also amended their laws to permit such practices. In Greece, existing investigation are taking place by I HAVE RIGHTS

Profiling
Yes

Exception
No

Explain

emails and other information about people on the move. Testimonies and evidence showcase related use in a wide range of EU member states, illegaly.

Name/description

Smart Policing tools of the Hellenic Police

Category

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

High-risk

Yes, completely

Explain In 2019, the Greek police signed a €4 million contract for a smart policing project with Intracom Telecom, a global provider of telecommunications systems and solutions. According to the press release issued by the Greek police, 75% of the project is financed by the European Commission's Internal Security Fund (ISF) 2014-2020. This smart policing project consists of portable devices enabling the use of facial recognition and automated fingerprint identification technologies during police stops. More precisely, police officers will be able to use these devices during police stops in urban environments to take a photograph of an individual's face and/or collect their fingerprints. The fingerprints and the photographs collected are compared with data stored in national, EU, and third-country databases for identification purposes, such as SIS II, VIS and EURODAC. The tender call even makes references to databases held by Europol, international organisations like Interpol, or even databases of institutions of third countries, such as the FBI. The police is presenting this project as a more "efficient" way to identify people, compared to the current procedure which consists of bringing any individuals who do not carry identification documents with them to the nearest police station. Apart from fingerprints, it is important to highlight that these devices offer the capacity for police officers to use photographs of faces to search individuals on a police database or to scan an individual's face to search her/him on a police database. Specifically, as clearly noted in the document describing the technical specifications of the project, the devices: • Offer the possibility to send photographs to SIS II and other police databases, • Enable police officers to upload photograph files either through a dialog window, or by drag-and-drop (including in bulk), • Provide for the possibility to conduct bulk search based on multiple photos. • Provide for a facial recognition software that should support the definition of thresholds (matching scores), above which the software's response will be automatically returned without requiring confirmation by specialized personnel. The technical specifications' document does not clarify the distance at which such photos would be taken or whether the individuals shall be aware of the data collection process. However, the technical details provided, could suggest that remote photo capture, followed by analysis, could be an option. More precisely, according to the document, the vendor is required to provide software that will allow for (1) editing, processing, and enhancing the photographs, (2) applying forensic filters to improve the photographs, and (3) using forensic methods to enhance the images and conduct searches on a watchlist. Moreover, as one of the developers from Intracom-Telecom, who worked in this project under a technical manager role, has stated, "This IT solution enabled police officers to perform personal inquiries on the field from their mobile phones using face, finger, or textual input". The IT solution as was also described as a "face recognition app of smart policing". It is understood that these devices clearly provide to the Hellenic Police the capacity to search individuals based on photos taken or the scanning of faces. Such photos could in theory be taken remotely, too, and then be uploaded to the platform to conduct searches, allowing for remote biometric identification. Such a capacity could have an immense chilling effect on public assemblies, since a police officer could in theory take a photo of a person, without her/his consent, and then upload his/her photo to the system and conduct related searches in police databases. Such searches could be related to any person, whose data are on police databases, including Greek passport holders or the holders of Greek IDs (since their facial images are collected in central police databases). Thus, it would be important to further clarify with the Hellenic Police related facial recognition functionalities and assess the Data Protection Impact Assessment of this project. In terms of timeline, these devices have already been piloted and were delivered to the Hellenic Police in September 2021.

Profiling

No

Exception

No

Explain

Category

- Polygraph use by public authorities (Point 7(a))
- Assessing risks for individuals entering a

Name/description

Member State (Point 7(b))
- Assisting with asylum and visa applications (Point 7(c))
- Identifying individuals in migration and border control (Point 7(d))

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

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

Explain

Profiling
- Yes
- No
- Unsure

Exception
- Yes
- No
- Unsure

Explain

Name/description

Category

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

Explain

Profiling
- Yes
- No
- Unsure

Exception
- Yes
- No
- Unsure

Explain

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))

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

Explain

Profiling
- Yes
- No
- Unsure

Exception
- Yes
- No
- Unsure

Explain

Category

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

Name/description

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

Explain

Profiling
- Yes
- No
- Unsure

Exception
- Yes
- No
- Unsure

Explain

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

Name/description

Category

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

High-risk

- Yes, completely
- Partially
- No
- Unsure

Explain

Profiling

- Yes
- No
- Unsure

Exception

- Yes
- No
- Unsure

Explain

Category

- Polygraph use by public authorities (Point 7(a))
- Assessing risks for individuals

Name/description		*High-risk*	*Explain*	*Profiling*	*Exception*	*Explain*
	entering a Member State (Point 7(b))	○ Yes, completely ○ Partially ○ No ○ Unsure		○ Yes ○ No ○ Unsure	○ Yes ○ No ○ Unsure	
	○ Assisting with asylum and visa applications (Point 7(c))					
	○ Identifying individuals in migration and border control (Point 7(d))					

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

	Name and description of the system	Category of AI system	Category of prohibited AI system with which there may be an interplay	Please motivate your answer
1	*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	*Category* Assessing risks for individuals entering a Member State (Point 7 (b))	*Category* Social scoring (Art. 5(1) (c))	*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 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.
		Category ○ Assessing risks for individuals entering a Member State (Point 7(b)) ○	*Category* ○ Social scoring (Art. 5 (1)(c)) ○	

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

		Identifying individuals in migration and border control (Point 7(d))	identification system (Art. 5(1)(h)) Other	

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.

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

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

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

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

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

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

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

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

Name/description
AI Interpretation tool for trials with non Greek speaking persons by the Hellenic Ministry of Justice

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

High-risk
Yes, completely

Explain A new Greek collaboration between the Ministries of Justice and Digital Governance will replace human court interpreters with AI systems for non-Greek-speaking witnesses. Professional interpreters warn this shift endangers fair trials—automated translations lack nuance, dialect understanding, and accuracy. The Judicial Interpreters' Association cautions that lives could hinge on algorithmic interpretation. Cases involving vulnerable refugees https://www.news247.gr/magazine/to-dikaio-ton-prosfigon-sta-xeria-tis-texnitis-noimosinis/

Profiling
No

Exception
No

Explain

Name/description

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

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

Explain

Profiling
- Yes
- No
- Unsure

Exception
- Yes
- No
- Unsure

Explain

Name/description

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

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

Explain

Profiling
- Yes
- No
- Unsure

Exception
- Yes
- No
- Unsure

Explain

Name/description

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

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

Explain

Profiling
- Yes
- No
- Unsure

Exception
- Yes
- No
- Unsure

Explain

Category

High-risk

Name/description	◯ Assisting judicial authorities or used in similar ways in alternative dispute resolution (Point 8(a)) ◯ Influencing election outcomes or voting behaviour (Point 8(b))	◯ Yes, completely ◯ Partially ◯ No ◯ Unsure	*Explain*	*Profiling* ◯ Yes ◯ No ◯ Unsure	*Exception* ◯ Yes ◯ No ◯ Unsure	*Explain*
Name/description	*Category* ◯ Assisting judicial authorities or used in similar ways in alternative dispute resolution (Point 8(a)) ◯ Influencing election outcomes or voting behaviour (Point 8(b))	*High-risk* ◯ Yes, completely ◯ Partially ◯ No ◯ Unsure	*Explain*	*Profiling* ◯ Yes ◯ No ◯ Unsure	*Exception* ◯ Yes ◯ No ◯ Unsure	*Explain*
Name/description	*Category* ◯ Assisting judicial authorities or used in similar ways in alternative dispute resolution (Point 8(a)) ◯ Influencing election outcomes or voting behaviour (Point 8(b))	*High-risk* ◯ Yes, completely ◯ Partially ◯ No ◯ Unsure	*Explain*	*Profiling* ◯ Yes ◯ No ◯ Unsure	*Exception* ◯ Yes ◯ No ◯ Unsure	*Explain*
Name/description	*Category* ◯ Assisting judicial authorities or used in similar ways in alternative dispute resolution (Point 8(a)) ◯ Influencing election outcomes or voting behaviour (Point 8(b))	*High-risk* ◯ Yes, completely ◯ Partially ◯ No ◯ Unsure	*Explain*	*Profiling* ◯ Yes ◯ No ◯ Unsure	*Exception* ◯ Yes ◯ No ◯ Unsure	*Explain*
Name/description	*Category* ◯ Assisting judicial authorities or used in similar ways in alternative dispute resolution (Point 8(a)) ◯ Influencing election outcomes or voting behaviour (Point 8(b))	*High-risk* ◯ Yes, completely ◯ Partially ◯ No ◯ Unsure	*Explain*	*Profiling* ◯ Yes ◯ No ◯ Unsure	*Exception* ◯ Yes ◯ No ◯ Unsure	*Explain*
	Category					

Name/description

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

High-risk

- ○ Yes, completely
- ○ Partially
- ○ No
- ○ Unsure

Explain

Profiling

- ○ Yes
- ○ No
- ○ Unsure

Exception

- ○ Yes
- ○ No
- ○ Unsure

Explain

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

1500 character(s) maximum

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

A. Requirements for high-risk AI systems

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

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

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

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

3000 character(s) maximum

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

In relation to Articles 9 to 15 of the proposed regulation, several critical points require clarification to ensure effective implementation and accountability. Regarding Article 9 (Risk Management), it remains unclear how

terms like “adequate” and “reasonable” will be defined and assessed in practice. The boundary of “reasonably foreseeable misuse” is vague. Who determines this threshold, and how are fines or accountability measures enforced? Additionally, the role of the deployer in adjusting risk assessments post-deployment must be specified, including who is responsible for continuous monitoring. Under Article 10 (Data Governance), mechanisms for verifying data origin and ensuring that data sets are appropriate, representative, and non-discriminatory must be established. Questions also arise regarding the detection of bias and the required documentation for using sensitive data. In Article 11 (Technical Documentation), the definition of “adequate” documentation must be clarified. Should this include source code, model assumptions, or only descriptive overviews, and how will trade secrets be protected? For Article 12 (Logging), the level of detail required, retention periods, and privacy safeguards need specification, particularly concerning sensitive or personal data. Article 13 (Transparency) must address how complex systems are explained accessibly to users and what the provider’s responsibility is if the user fails to comprehend the information. Regarding Article 14 (Human Supervision), the extent and form of human involvement, whether continuous or intermittent, and how its sufficiency is demonstrated should be clarified. Finally, Article 15 (Accuracy and Cybersecurity) must define technical standards for accuracy, resilience including against adversarial attacks, and the testing required. Cross-cutting concerns include the coordination of these articles, responsibility for compliance (provider vs. user), and whether special provisions apply for SMEs or startups.

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

Ambiguity and Interpretability Some obligations, such as the requirement to maintain a "quality management system" or ensure compliance with "accessibility requirements," can be open to interpretation. Providers might struggle to determine exactly what constitutes compliance in practical terms, especially without harmonized standards or detailed technical guidance. Without clear delineation of roles between providers, deployers, developers, and sub-contractors, responsibility for conformity assessments, post-market monitoring, or taking corrective action may become a legal grey zone, leading to regulatory arbitrage or litigation risk. Conformity Assessment Challenges The need to conduct a conformity assessment (Article 43) may require engagement with Notified Bodies, introducing delays, costs, and a reliance on external evaluations. There is also concern about capacity bottlenecks if many providers are seeking assessment at the same time. Logging and Data Management Issues The obligation to keep logs (Article 19) raises concerns around data storage, privacy, and cybersecurity. Ensuring logs are both complete and secure over potentially long periods could become a liability if systems generate massive amounts of data. For example, maintaining logs for traceability (Article 19) may contradict data minimization principles under the GDPR, especially if logs contain user-identifiable data. The lack of regulatory interoperability mechanisms or a formal hierarchy among EU regulations increases the risk of non-compliance due to legal inconsistency. Accessibility Compliance Ensuring accessibility as required by Directives (EU) 2016/2102 and 2019/882 can be especially difficult for AI providers whose systems include non-traditional user interfaces (e.g., voice assistants, vision-based systems). There's a lack of clear guidance on how accessibility standards apply in these contexts. Corrective Measures and Liability The need to take corrective action and cooperate with authorities (Articles 20 and 21) introduces potential legal liability. Providers may be held accountable for issues beyond their immediate control, particularly in dynamic or learning systems where behavior evolves post-deployment.

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

Several aspects of Article 26 would benefit from clarification to ensure consistent interpretation across sectors and deployment contexts: 1. "Appropriate technical and organisational measures" and "Use in accordance with instructions" Clarify how deployers must verify technical compliance (e.g. certifications, system versioning, environmental conditions) and what kind of documentation is required. This is especially relevant when systems are deployed across diverse operational settings (e.g. different countries or teams). 2. Competence and authority of human oversight More specificity is needed on what qualifies as "necessary competence" and "necessary support". Must oversight persons have technical AI knowledge or just domain expertise (e.g. HR, healthcare)? Guidance should also clarify whether oversight must be continuous through the whole life-cycle of the system or event-triggered. 3. Input data obligations It remains unclear to what extent deployers are expected to vet or clean input data. Are they responsible for identifying bias or outliers in operational data, especially when input pipelines are partially controlled by the provider? What does "relevant and sufficiently representative" input data mean? It must be specified and clear what deployers must do to secure representative and accurate/relevant data. 4. Logging obligations Clarify what logs must be stored (e.g. full inference logs, metadata, user interactions) and under what conditions deployers may rely on the provider's infrastructure to satisfy this obligation. 5. Threshold for "monitoring" What does effective monitoring entail? Should deployers track KPIs (e.g. error rates, false positives), or is functional compliance with documentation

sufficient? There is also uncertainty about the scope of “inform providers where relevant” under Article 72—what triggers notification? 6. Worker and subject notification In use cases involving employees or end-users (e.g. productivity monitoring, loan applications), more clarity is needed on the format, timing, and depth of required disclosure. 7. Post-remote biometric identification for law enforcement purposes What are the specific authorization requirements and restrictions that apply to the deployer of a high-risk AI system for post-remote biometric identification for law enforcement purposes? This must be clarified, so that there is no room for violations.Recommendation: Issue specific guidelines that provide examples and clarity to the above matters, as well as sectoral guidance on deployer obligations, distinguishing between types of deployers (e.g. SMEs, hospitals, municipalities), AI systems (e.g. pre-trained, continuously learning), and levels of deployer technical capacity.

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

Article 26 obligations interact with multiple pieces of EU legislation. Clarifications are needed to prevent regulatory conflict or duplication: 1. GDPR (Regulation 2016/679) Overlap arises with Articles 5, 24, and 32 GDPR regarding data quality, accountability, and security. Clarify how deployers should coordinate their obligations around data representativeness and oversight mechanisms. For instance, does data minimization under GDPR conflict with the need for “sufficiently representative” data under Article 26(2)(c)? Also, what is the relationship between FRIAs (as required in article 27 of the AI Act) and DPIAs (as required in the GDPR)? This needs to be further clarified. 2. OSH Framework Directive (89/391/EEC) Deployers in the workplace context must inform workers of monitoring AI systems. Clarify whether this duty interacts with broader OSH obligations on psychological health, autonomy, and risk prevention. 3. NIS2 Directive (2022/2555) If high-risk AI systems qualify as essential services (e.g. in healthcare or transport), deployers may face dual obligations on logging, monitoring, and incident response. Clarification is needed on log retention overlap and responsibilities in case of AI-related incidents. 4. ePrivacy Directive (2002/58/EC) Where high-risk systems interact with communications metadata or behavioral data, deployers may face additional consent or privacy obligations. It is unclear how these apply when deployers act as data processors rather than controllers. 5. Digital Services Act (Regulation [EU] 2022/2065] While the DSA is not specifically designed to regulate AI, its provisions can apply to AI systems used by these platforms. Just like the AI Act, the DSA also requires transparency, testing, oversight mechanisms, protection of user rights etc. Recommendation: 6.Law Enforcement Directive (2016/680) 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 27 of LED. The AI Office should provide an integrated mapping of obligations across EU law, along with examples of how deployers can structure compliance strategies that satisfy multiple regimes efficiently.

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

1. Scalability A tiered approach (e.g. based on system risk profile or organizational capacity) would avoid burdening small entities disproportionately. 2.Scope FRIAs have a public character, they concern public bodies or private entities providing public services, which is problematic. The AI Office should publish guidelines, to encourage private companies to systematically assess the impact of high-risk AI systems on the citizens' fundamental rights. 3. Compliance The risk assessment for a high-risk AI system must be carried out before its development has even started or before it's used for the first time. The AI Act doesn't set a specific time limit, so this must be specified. 3. Risk severity and likelihood Should deployers apply a quantitative or qualitative approach to risk? Is there a required methodology (e.g. probabilistic models, stakeholder consultations), or is flexibility allowed? 4. Use of external auditors Clarify whether assessments can be outsourced or if internal teams should lead the process. Is co-signature by an ethics officer, legal team, or board required? 5. System updates It's not clear when a FRIA needs to be updated. Also, the decision to update the FRIA is left entirely to the discretion of implementing bodies. A distinction is needed: changes in the procedures, duration and frequency of use of the AI system are not significant and don't require a new FRIA. However, regarding natural persons affected, risks of harm, human oversight measures and measures in the event risks materialise, these are significant and require a new FRIA. 6. Information to market surveillance authority The implementing body must inform the market surveillance authority as soon as the FRIA is carried out. A clear timeframe is needed for informing the competent supervisory authority about the conduct and results of the FRIA. It should also be clarified what the consequences are in case this timeframe is not respected. 7. Exceptions The market surveillance authority may authorise the direct use and placing on the market of high-risk AI systems without carrying out a FRIA if it considers that there are exceptional grounds of public safety, protection of life, health, the environment and critical infrastructure. There is ambiguity in this exemption. There is an urgent need for a specific list of exceptions. 8. Publishing results Article 49(4) provides that in the areas of law enforcement, immigration and asylum management and border controls, the entry shall be made in a non-public part of the database. This provision is a violation of transparency and the protection of fundamental rights. 9. DPIA/FRIA According to the AI ACT, if a DPIA has already been carried out, the FRIA will supplement that DPIA. The relationship between the two tools should be clarified, specifying the different scopes of application and the points where they overlap.

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

To avoid redundancy and ensure consistency between the FRIA and the Data Protection Impact Assessment (DPIA) under GDPR: 1. Clear division of scope DPIA focuses on data protection risks (e.g. lawful basis, data minimization, security), while FRIA should expand to broader impacts (e.g. discrimination, exclusion, chilling effects). The FRIA template should reference completed DPIA sections and avoid duplicating them. 2.

Harmonized risk methodologies Encourage common scoring scales or risk matrices between DPIA and FRIA to support alignment. This allows joint assessments or modular structures. 3. Sequencing and reuse Allow the DPIA to be conducted first, feeding into FRIA. Clarify how shared findings (e.g. risks to data subjects) can be reused to streamline work. 4. Joint templates and toolkits The AI Office and EDPB could develop a common toolkit or dual-purpose template to assist deployers in addressing both obligations simultaneously. 5. Sector-specific alignment In health, education, and employment, specific interplay exists with existing ethics, human rights, and administrative procedures. Guidance should note how FRIA can integrate with these. 6.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 domain 7.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. 8.. Clarify distinct but complementary scopes 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.

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

The right to explanation under Article 86 is essential for ensuring transparency and contestability. However, several aspects need clarification: 1. Scope of "significant adverse impact" Clarify whether purely procedural or reputational harms (e.g. lower performance reviews, increased surveillance) qualify, formal decisions (e.g. credit denial, hiring rejection) or some kind of harm needs to be proved (financial, psychological, physical) and how. 2. Form of explanation Should deployers provide a technical rationale, a lay summary, or both? What level of detail is sufficient to meet the obligation without compromising IP or trade secrets? 3. Roles and responsibilities Clarify whether the deployer alone must respond, or whether the provider is also obligated to contribute. What happens when a deployer cannot technically access the explanation? 4. Timeline and format Is there a prescribed timeframe for responding to explanation requests? Should explanations be written, oral, or accessible through digital portals? 5. Interaction with other laws How does this obligation interact with GDPR's Article 15 and Recital 71 on the right to meaningful information about automated decisions, as well as the right to access? Recommendation: Develop interpretive guidance with example explanation formats (e.g. causal

charts, performance breakdowns), thresholds/practical examples for “adverse impact,” and joint responsibilities between deployers and providers to ensure feasible implementation. Special attention shall be given to existing CJEU caselaw, 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

The concept of "substantial modification" needs to be clarified and specified through guidelines and examples. “Affecting compliance” Further guidance is needed on which changes to model architecture, data pipelines, or learning behaviour impact compliance. ● Does re-training a high-risk system on new datasets with significantly

different demographics constitute a substantial modification? ● If a high-risk system continuously self-trains on new data, must it be continuously monitored for potential substantial modifications? ● For self-learning non-high-risk systems, can substantial modification apply if the learning results in the system becoming high-risk under Article 25(1)(c)? Modifications by deployers vs. providers Ambiguity exists on whether unplanned changes by deployers (e.g., fine-tuning for internal use) trigger reclassification as a provider. If such changes do not materially affect performance or purpose, should they still be deemed substantial? Role of automated updates Many AI systems operate with continuous updates. A clearer distinction is needed between pre-determined updates and ad hoc changes. What human oversight must the provider build in, and what monitoring must deployers perform to detect thresholds requiring re-assessment? Interplay with intended purpose It's unclear when an "evolution" of use constitutes a change in intended purpose under Article 25(1)(c). More precise indicators (e.g., function shift, risk profile change) would aid interpretation. Practical Examples ● Biometric system context shift: A system designed for indoor facial recognition is updated for outdoor use with variable lighting. This alters risk conditions and likely requires reassessment. ● Deployer-induced input change: A hospital integrates a CE-marked diagnostic AI with a pre-processing tool altering image inputs. This affects compliance and may constitute a substantial modification. ● Functionality extension: A resume screening tool is updated with video interview analysis. This adds modalities and risks, likely requiring a new conformity assessment. ● Dataset composition shift: A credit scoring AI is re-trained with data including more young, rural users. Although model architecture is unchanged, the demographic shift may affect fairness or performance. If this change was not pre-documented, it may be substantial—especially if detected post-deployment as a statistical anomaly. ● Alert threshold tuning: A worker monitoring AI increases alert frequency after client feedback. Does this parameter change, with possible ethical implications, amount to a substantial modification? ● External data enrichment: Adding third-party APIs to supplement user profiles could introduce new risks without altering the core model. Is this substantial? Recommendation Develop sector-specific guidance and a decision framework to assess whether changes affect compliance materially.

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

Article 43(4) provides that changes pre-determined and documented at the time of conformity assessment are not considered substantial. This is crucial for systems that evolve post-deployment. However, clarification is needed on how this applies in practice. Granularity of pre-determination Clarify whether "pre-determined" refers to concrete parameters (e.g., model weights, frequency of updates) or general classes of updates (e.g., "retraining allowed every 6 months using internal data"). More guidance is needed on what constitutes sufficient specificity to exclude a modification from reassessment. Criteria for substantial modification threshold What cumulative or performance-related changes over time would cross the boundary from pre-determined into substantial? Can a change remain non-substantial if its cumulative impact was not fully foreseeable? Documentation standards There is a need to standardize expectations under Annex IV(2)(f). Clear criteria for documenting acceptable update types, triggers, and model evolution cycles would support consistency across assessments. Tooling and monitoring Providers should implement update control tools (e.g., versioning,

logging, differential analysis) to ensure only anticipated updates are applied. Regulators should clarify what tooling is adequate to demonstrate traceability and integrity of changes. Practical Examples ● Scheduled model retraining: A medical diagnostic AI is re-trained every six months using the same pipeline and data sources. This is clearly pre-determined and documented, and not a substantial modification. ● Threshold configuration: A fraud detection tool allows sensitivity adjustments within defined operational limits. If thresholds remain within the documented range, the change is not substantial. ● Software patching: An industrial AI system receives periodic patches to improve speed and security, with all changes documented in advance. These are not substantial if they don't affect the risk profile or intended purpose. ● Dormant feature activation: If a documented but inactive feature (e.g., biometric liveness detection) is later enabled without prior notice in the conformity file, it's unclear whether this counts as pre-determined. Recommendation Develop a checklist or standard template for conformity documentation that defines: ● Acceptable types and frequency of changes ● Risk thresholds and update triggers ● Monitoring obligations and fallback mechanisms This would enable providers to design systems with documented flexibility while maintaining regulatory compliance.

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

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