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.

Information about the respondent

* First name

> Amandeep

* Surname

> Luther

* Email address

> amandeep.luther@afme.eu

* 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

> Association of Financial Markets in Europe (AFME)

* Type of organisation

> Association

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

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

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

> BE - Belgium

* Select the size of the organisation

> Medium (50-249 employees)

* Sector(s) of activity

- ☑ Information technology
- ☐ Employment
- ☐ Transport

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

* Describe the activities of your organisation or yourself

1300 character(s) maximum

> The Association for Financial Markets in Europe (AFME) is the voice of Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues. We represent the leading global and European banks and other significant capital market players. AFME's members are the lead underwriters of 89% of European corporate and sovereign debt, and 79% of European listed equity capital issuances.

---

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

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 Your name will not be published.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

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

  ◉ Yes, please anonymise my contribution.
  ◯ No

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

  ◉ Yes
  ◯ No

☑ I acknowledge the attached privacy statement.

    Privacy_statement_high_risks.pdf

---

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

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

Section 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'?

- ☐ 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);
- ☐ 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);
- ☐ 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);
- ☐ 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);
- ☐ 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);
- ☐ 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);
- ☐ 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;
- ☐ 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	Description	Explain
	○ Directive 2014/53/EU	*750 character(s) maximum*	*500 character(s) maximum*
	○ 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		
6	*Legislation's name*	Description	Explain
	○ Directive 2006/42/EC	*750 character(s) maximum*	*500 character(s) maximum*
	○ 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		
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

	Legislation's name		
	○ 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*

		Description	Explain
	○ 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.

> 24

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*

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

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

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

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

- *Point 1(a) of Annex III to the AI Act refers to the use of remote biometric identification systems. These systems aim at the remote (at a distance, without the active participation of the person in question) automated recognition of a natural person, for the purpose of establishing the identity of that person, by comparing the biometric data of that individual to biometric data of individuals stored in a database. Verification and authentication, used for the confirmation of the identity of a natural person, are not considered to be high-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 <u>high-risk AI systems related to biometrics.</u>

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*	*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*
2	*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*
3	*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*
4	*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*
5	*Name/description*	*Category* ○ Remote biometric identification (Point 1(a)) ○ Biometric categorisation (Point 1(b))	*High-risk* ○ Yes, completely ○ Partially ○ No	*Explain*	*Profiling* ○ Yes ○ No	*Exception* ○ Yes ○ No	*Explain*

#	Name/description	Category	High-risk	Explain	Profiling	Exception	Explain
			○ Emotion recognition (Point 1(c))	○ Unsure		○ Unsure	○ Unsure
6	*Name/description*	*Category* ○ Remote biometric identification (Point 1(a)) ○ Biometric categorisation (Point 1(b)) ○ Emotion recognition (Point 1(c))	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*
7	*Name/description*	*Category* ○ Remote biometric identification (Point 1(a)) ○ 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*
8	*Name/description*	*Category* ○ Remote biometric identification (Point 1(a)) ○ Biometric categorisation (Point 1(b)) ○ Emotion recognition (Point 1(c))	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*
9	*Name/description*	*Category* ○ Remote biometric identification (Point 1(a)) ○ Biometric categorisation (Point 1(b)) ○ Emotion recognition (Point 1(c))	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*
10	*Name/description*	*Category* ○ Remote biometric identification (Point 1(a)) ○ Biometric categorisation (Point 1(b)) ○ 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 <u>practical examples of AI systems related to biometrics</u> 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*	*Category* ○ Remote biometric identification (Point 1(a)) ○ Biometric categorisation (Point 1(b)) ○ Emotion recognition (Point 1(c))	*Category* ○ Real time remote biometric identification system (Art. 5(1)(h)) ○ Biometric categorisation system (Art. 5(1)(g)) ○ Emotion inference system (Art. 5(1)(f)) ○ Other ○ Unsure	*Explain*
2	*Name/description*	*Category* ○ Remote biometric identification (Point 1(a)) ○ Biometric categorisation (Point 1(b)) ○ Emotion recognition (Point 1(c))	*Category* ○ Real time remote biometric identification system (Art. 5(1)(h)) ○ Biometric categorisation system (Art. 5(1)(g)) ○ Emotion inference system (Art. 5(1)(f)) ○ Other ○ Unsure	*Explain*
3	*Name/description*	*Category* ○ Remote biometric identification (Point 1(a)) ○ Biometric categorisation (Point 1(b)) ○ Emotion recognition (Point 1(c))	*Category* ○ Real time remote biometric identification system (Art. 5(1)(h)) ○ Biometric categorisation system (Art. 5(1)(g)) ○ Emotion inference system (Art. 5(1)(f)) ○ Other ○ Unsure	*Explain*
4	*Name/description*	*Category* ○ Remote biometric identification (Point 1(a)) ○ Biometric categorisation (Point 1(b)) ○ Emotion recognition (Point 1(c))	*Category* ○ Real time remote biometric identification system (Art. 5(1)(h)) ○ Biometric categorisation system (Art. 5(1)(g)) ○ Emotion inference system (Art. 5(1)(f)) ○ Other ○ Unsure	*Explain*
		Category	*Category* ○ Real time remote biometric identification system (Art. 5(1)(h))	

5	*Name/description*	○ Remote biometric identification (Point 1(a)) ○ Biometric categorisation (Point 1(b)) ○ Emotion recognition (Point 1(c))	○ Biometric categorisation system (Art. 5(1)(g)) ○ Emotion inference system (Art. 5(1)(f)) ○ Other ○ Unsure	*Explain*

Question 9. If you see the <u>need for clarification</u> 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

Clarifications required: - In the absence of high risk PII processing, confirm that an AI use case would not meet the high risk requirement under the AIA. - Significant overlap between GDPR and EU AIA. Clarity with regard to what is / not in scope for high risk would be helpful. - use of Biometric data for fraud prevention / security, eg. Detection of fraud in video/audio, is a permissible use of AI and overlaps with GDPR regulation. The AI Act recital 133 recognizes that AI systems can "raise new risks of misinformation, and manipulation at scale, fraud , impersonation and consumer deception. The AI Act should therefore be future proof, enabling fraud detection and security to dynamically adapt to the attacks to ensure highest customer protection. - Clarification needed on the interconnection of Article 10 and with Regulation 2018/1724 Data Governance Act Recital 2 (recreation of common European data spaces). Specifically, what data requirements will be placed on firms above the EU AI Act where HRAI data is made available to market participants?

2.B. Questions in relation to critical infrastructure (Annex III, point 2)

The classification of AI systems as high-risk under Point 2 of Annex III to the AI Act targets AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity. According to Article 3(14), 'safety component' means a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property. The underlying rationale is that the failure or malfunctioning of those safety components mentioned in point 2 may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities (Recital 55).

Point 2 of Annex III therefore covers the following distinct use cases:

- *AI systems intended to be used as safety components in the management and operation of critical digital infrastructure.*
- *AI systems intended to be used as safety components in the management and operation of road traffic.*
- *AI systems intended to be used as safety components in the management and operation of the supply of water.*
- *AI systems intended to be used as safety components in the management and operation of the supply of gas.*
- *AI systems intended to be used as safety components in the management and operation of the supply of heating.*
- *AI systems intended to be used as safety components in the management and operation of the supply of electricity.*

Question 10. Please provide practical examples of AI systems that in your opinion may fall within the scope of high-risk AI systems related to critical infrastructure and the use of AI system as safety component.

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 safety component	The system is considered high-risk	Motivate your previous answer	The AI system performs profiling of natural person	The AI system meets at least one of the exception criteria of Article 6(3)	Motivate your previous answer and specify any exception criteria that it meets, if applicable
1	Name/description	*Category* ○ Digital infrastructure ○ Road traffic ○ Supply of water ○ Supply of gas ○ Supply of heating ○ Supply of electricity	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*
2	Name/description	*Category* ○ Digital infrastructure ○ Road traffic ○ Supply of water ○ Supply of gas ○ Supply of heating ○ Supply of electricity	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*
3	Name/description	*Category* ○ Digital infrastructure ○ Road traffic ○ Supply of water ○ Supply of gas ○ Supply of heating ○ Supply of electricity	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*
		Category ○ Digital infrastructure	*High-risk*				

				Explain	Profiling	Exception	Explain
4	Name/description	○ Road traffic ○ Supply of water ○ Supply of gas ○ Supply of heating ○ Supply of electricity	○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	○ Yes ○ No ○ Unsure	○ Yes ○ No ○ Unsure	*Explain*
5	Name/description	*Category* ○ Digital infrastructure ○ Road traffic ○ Supply of water ○ Supply of gas ○ Supply of heating ○ Supply of electricity	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*
6	Name/description	*Category* ○ Digital infrastructure ○ Road traffic ○ Supply of water ○ Supply of gas ○ Supply of heating ○ Supply of electricity	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*
7	Name/description	*Category* ○ Digital infrastructure ○ Road traffic ○ Supply of water ○ Supply of gas ○ Supply of heating ○ Supply of electricity	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*
8	Name/description	*Category* ○ Digital infrastructure ○ Road traffic ○ Supply of water	*High-risk* ○ Yes, completely ○ Partially ○	*Explain*	*Profiling* ○ Yes ○	*Exception* ○ Yes ○	*Explain*

#	Name/description	Category	High-risk	Explain	Profiling	Exception	Explain
		○ Supply of gas ○ Supply of heating ○ Supply of electricity	○ No ○ Unsure		No ○ Unsure	No ○ Unsure	
9	*Name/description*	*Category* ○ Digital infrastructure ○ Road traffic ○ Supply of water ○ Supply of gas ○ Supply of heating ○ Supply of electricity	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*
10	*Name/description*	*Category* ○ Digital infrastructure ○ Road traffic ○ Supply of water ○ Supply of gas ○ Supply of heating ○ Supply of electricity	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*

Question 11. If you need <u>further clarification</u> on the concept of a **safety component** in the management and operation of critical infrastructure in the areas mentioned in *Point 2 of Annex III* to the AI Act, please specify and explain the use case where you need further clarification on

1500 character(s) maximum

Question 12. If you have or know <u>practical examples of components</u> intended to be used **solely for cybersecurity purposes** and would therefore not qualify as a safety component in the management and operation of critical infrastructure in the areas mentioned in *Point 2 of Annex III to the AI Act (recital 55 AI Act)*, please specify the practical example, how it is used in practice as well as the specific elements on which you would need further clarification in this regard

1500 character(s) maximum

Question 13. If you see the need for clarification of the high-risk classification in *Point 2 of Annex III to the AI Act* and its **interplay with other Union or national legislation**, e.g. to Directive (EU) 2022/2555 (NIS2)?, 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.C. Questions in relation to education and vocational training (Annex III, point 3)

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

- *Point 3(a) of Annex III to the AI Act refers to AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels.*

- *Point 3(b) of Annex III to the AI Act refers to AI systems intended to be used to evaluate learning outcomes, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels.*

- *Point 3(c) of Annex III to the AI Act refers to AI systems intended to be used for the purpose of assessing the appropriate level of education that an individual will receive or will be able to access, in the context of or within educational and vocational training institutions at all levels.*

- *Point 3(d) of Annex III to the AI Act refers to AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels.*
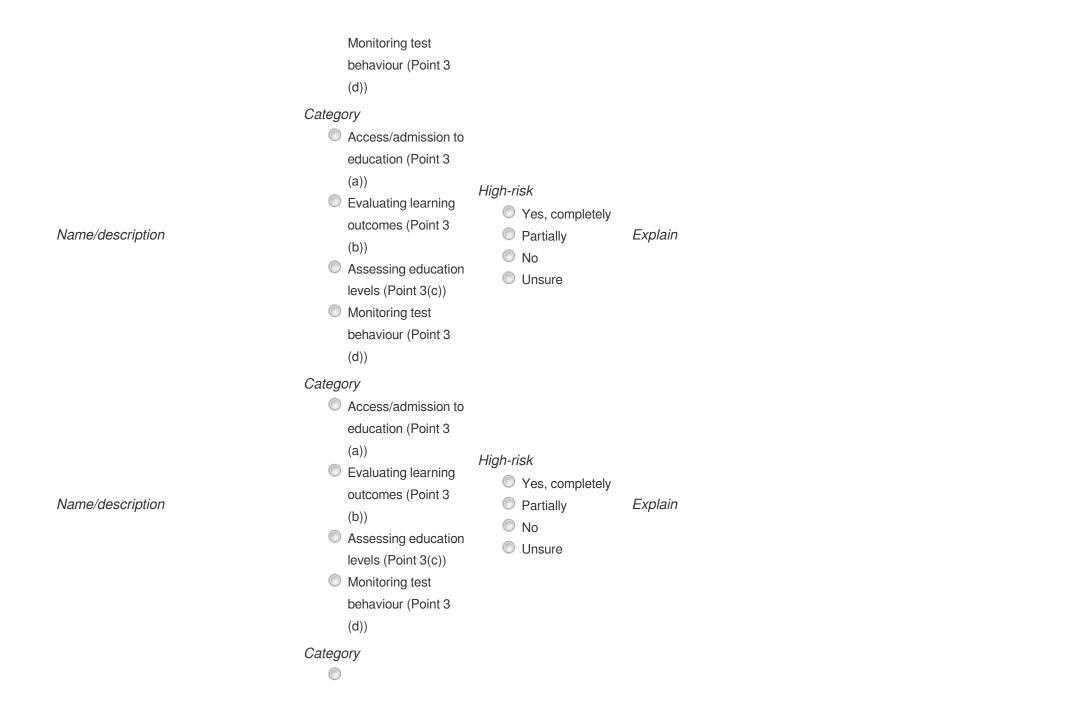
Question 14. Please provide practical examples of AI systems that in your opinion may fall within the scope of <u>high-risk AI systems related to education and vocational training.</u>

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

Name/description
Online Platform for Course Admission Based on AI Profile Matching

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

High-risk
| Yes, completely |

Explain Using internal company data such as previous courses, scores, previous role held by the person, previous evaluations, current level, identify next possible course / path and suggest it for upskilling / reskilling purposes

Profiling
| Unsure |

Exception
| No |

Explain If the system merely suggests suitable courses without limiting access, may it be excluded?

Name/description
Scoring for education levels by using inputs already present in the company

Category
| Assessing education levels (Point 3(c)) |

High-risk
| Yes, completely |

Explain On a specific skill, by using internal company data, score an employee; this scoring may then be used by humans to internal opportunities (projects, courses, other)

Profiling
| Unsure |

Exception
| No |

Explain If the system's output is then used by a human (employee's manager) to assess access to opportunities, is it high risk? If the system's output is also validated by the employee and then used by other human actors to access to opportunities, is it still high risk?"

Name/description

Category
- ○ Access/admission to education (Point 3 (a))
- ○ Evaluating learning outcomes (Point 3 (b))
- ○ Assessing education levels (Point 3(c))
- ○ Monitoring test behaviour (Point 3 (d))

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

Explain

Profiling
- ○ Yes
- ○ No
- ○ Unsure

Exception
- ○ Yes
- ○ No
- ○ Unsure

Explain

Category
- ○ Access/admission to education (Point 3 (a))
- ○

High-risk

Name/description

Evaluating learning outcomes (Point 3 (b))

○ Assessing education levels (Point 3(c))

○ Monitoring test behaviour (Point 3 (d))

○ Yes, completely
○ Partially
○ No
○ Unsure

Explain

Profiling
○ Yes
○ No
○ Unsure

Exception
○ Yes
○ No
○ Unsure

Explain

Category

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

○ Evaluating learning outcomes (Point 3 (b))

○ Assessing education levels (Point 3(c))

○ Monitoring test behaviour (Point 3 (d))

Name/description

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

Explain

Profiling
○ Yes
○ No
○ Unsure

Exception
○ Yes
○ No
○ Unsure

Explain

Category

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

○ Evaluating learning outcomes (Point 3 (b))

○ Assessing education levels (Point 3(c))

Name/description

○

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

Explain

Profiling
○ Yes
○ No
○ Unsure

Exception
○ Yes
○ No
○ Unsure

Explain

Monitoring test behaviour (Point 3 (d))

Category
- ○ Access/admission to education (Point 3 (a))
- ○ Evaluating learning outcomes (Point 3 (b))
- ○ Assessing education levels (Point 3(c))
- ○ Monitoring test behaviour (Point 3 (d))

Name/description

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

Explain

Profiling
- ○ Yes
- ○ No
- ○ Unsure

Exception
- ○ Yes
- ○ No
- ○ Unsure

Explain

Category
- ○ Access/admission to education (Point 3 (a))
- ○ Evaluating learning outcomes (Point 3 (b))
- ○ Assessing education levels (Point 3(c))
- ○ Monitoring test behaviour (Point 3 (d))

Name/description

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

Explain

Profiling
- ○ Yes
- ○ No
- ○ Unsure

Exception
- ○ Yes
- ○ No
- ○ Unsure

Explain

Category
- ○

Name/description

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

○ Evaluating learning outcomes (Point 3 (b))

○ Assessing education levels (Point 3(c))

○ Monitoring test behaviour (Point 3 (d))

High-risk

○ Yes, completely
○ Partially
○ No
○ Unsure

Explain

Profiling

○ Yes
○ No
○ Unsure

Exception

○ Yes
○ No
○ Unsure

Explain

Category

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

○ Evaluating learning outcomes (Point 3 (b))

○ Assessing education levels (Point 3(c))

○ Monitoring test behaviour (Point 3 (d))

Name/description

High-risk

○ Yes, completely
○ Partially
○ No
○ Unsure

Explain

Profiling

○ Yes
○ No
○ Unsure

Exception

○ Yes
○ No
○ Unsure

Explain

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

1500 character(s) maximum

```

```

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

1500 character(s) maximum

```

```

2.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 <u>high-risk AI systems related to employment,</u> <u>workers' management and access to self-employment.</u>

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.

Category

Name/description
Evaluation of learning outcomes for employees undertaking training courses. These might be delivered by a third party provider or built internally.

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

High-risk

Unsure

Explain Does this come under performance management or is evaluation of learning outcomes a different category?

Profiling

Unsure

Exception

No

Explain It is unclear if the application of: Annex III (3), which covers Education and Training. 3(a) covers access and admission, 3(b) covers the evaluation of learning outcomes, 3(c) covers the assessment of the type and level of training an individual should receive Applies to non-educational facilities and in training during the course of employment

Category

Name/description
AI systems used for Recruitment and Hiring Tools

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

High-risk

Yes, completely

Explain Systems that automate or assist in screening, ranking, or selecting job candidates. The AI system performs the initial selection phase, filtering and ranking candidates to streamline the recruitment process. A human recruiter or hiring manager intervenes subsequently, reviewing the AI-generated shortlist and making the final hiring decisions.

Profiling

Unsure

Exception

No

Explain

Category

Name/description
AI systems used for Recruitment and Hiring Tools

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

High-risk

Yes, completely

Explain AI Systems Supporting Recruitment and Hiring with Human-First Selection: In this recruitment workflow, the initial candidate selection is performed by human recruiters, who review applications and identify a pool of candidates. Subsequently, an AI system is applied to this human-selected pool to assist with tasks such as: - Further screening or ranking of candidates based on specific criteria - Checking qualifications, skills, or compatibility with the job requirements

Profiling

Unsure

Exception

No

Explain

Category

Name/description
Skill Matching and evaluating performance

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

High-risk

Yes, completely

Explain Internal selection based on skills - AI system

Profiling

Unsure

Exception

No

Explain

Category

○

Name/description

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

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

Explain

Name/description

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

Explain

Name/description

Profiling
○ Yes
○ No
○ Unsure

Exception
○ Yes
○ No
○ Unsure

Explain

Category
○

50

Name/description

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

Name/description

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

Name/description

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

Explain

Profiling
○ Yes
○ No
○ Unsure

Exception
○ Yes
○ No
○ Unsure

Explain

Question 18. Do you have or know <u>practical examples of AI systems related to employment, workers' management and access to self-employment</u> 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* ◎ 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*
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 <u>need for clarification</u> 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

Clarity needed on: • interplay between GDPR Art 22 (e.g. Schufa case) and high risk tools used for decision making regarding employees. How is "automated decision making supported by AI tools" defined? HR use cases likely involve employee PII data thus firms will need to consider both regulations. • interplay between DPIA (GDPR Art.35) and FRIA (AI Act Art. 29 & Recital 60(FRIA)): can completion of a DPIA under GDPR partially or fully satisfy the FRIA obligations • whether the scope is intended to include decisions made by the AI tool only or also when AI output informs an overall decision, ie. Where AI element is a "Preparatory Task". E.g. combining AI output with other data to assign performance rating. • how HRAI exception process will operate. eg. HR teams using AI for summarisation tasks? Would this be recorded as exceptions or excluded as not part of recruitment? • If firm uses AI tool for workforce management / performance monitoring, would this trigger obligations to consult employees or work councils under national labour laws? • what " targeted job advertisements" is intended to cover? How would it apply to firms using output/recommendations of 3rd party recruitment providers?

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 <u>high-risk AI systems related to essential private services and essential public services and benefits.</u>

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* Traditional creditworthiness assessment model using logistic regression. This system is used to estimate the probability of a default of a natural person applying for a loan, based on static, manually selected variables and a predefined scoring algorithm	*Category* Evaluation of creditworthiness/ credit score of natural persons (Point 5(b))	*High-risk* No	*Explain* This system should not be considered high-risk because it does not qualify as an AI system under Article 3(1) of the AI Act. Logistic regression models that are static, interpretable, and built through manual processes—without post-deployment adaptiveness, autonomy, or inference—do not meet the definition of an AI system. These models rely on deterministic rules and require expert input at all stages	*Profiling* No	*Exception* No	*Explain*
2	*Name/description* Automated pre-screening AI system for personal loan applications	*Category* Evaluation of creditworthiness/ credit score of natural persons (Point 5(b))	*High-risk* Unsure	*Explain* The AI system does not make final decisions but performs a pre-screening. According to the AI Act, this influence may be considered "material" if it significantly affects the outcome for individuals, even if the final decision is made by a human. What percentage of influence is considered material?	*Profiling* Yes	*Exception* No	*Explain*
3	*Name/description*	*Category* ◯ Evaluation of eligibility for public assistance benefits and services (Point 5(a)) ◯ Evaluation of creditworthiness/ credit score of natural persons (Point 5(b)) ◯ Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) ◯	*High-risk* ◯ Yes, completely ◯ Partially ◯ No ◯ Unsure	*Explain*	*Profiling* ◯ Yes ◯ No ◯ Unsure	*Exception* ◯ Yes ◯ No ◯ Unsure	*Explain*

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

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

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

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

> Clarification required on whether the use of customer spending habit data is considered prohibited or high risk. The legislation refers to "creditworthiness" or "establishing a credit score" but evaluating creditworthiness is a broad term and more detail is needed on what this is meant to cover.

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

1500 character(s) maximum

> In the case of the financial sector, credit scoring is already subject to strict supervision by sectoral regulators. Credit scoring models are already validated and monitored by supervisory authorities under prudential regulation frameworks, and subject to rigorous governance, validation, and audit processes. We emphasize the need to ensure consistency among existing and new AI act supervision, ensuring coordination and to avoid creating duplicate requirements for entities. Divergent national interpretations—e.g. broader definitions of AI by data protection authorities—may lead to fragmented enforcement. Therefore, a clearer delineation is needed between AI systems subject to the AI Act and conventional models governed under existing horizontal and sectoral rules.

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* Anti-fraud transaction monitoring tool. Eg.as used in loan origination. It flags anomalous behaviors that may indicate fraudulent applications, such as inconsistencies between stated income and behavioral data (e.g., device fingerprinting, usage anomalies	*Category* 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* The tool's exclusive purpose is to detect potentially fraudulent behaviors before a credit decision is made. It is not used to evaluate creditworthiness or to establish a credit score, but rather to ensure the integrity of the loan application process. This aligns directly with the exemption outlined in Point 5(b) and Recital 58, which excludes AI systems intended to detect financial fraud from the high-risk classification.
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	*Explain*

		institutions' and insurance undertakings' capital requirements (recital 58)	
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*
		Category ○ Exception of being intended for the purpose of detecting financial fraud (Point 5(b)) ○	

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

		undertakings' capital requirements (recital 58)	

Section 3. Questions on horizontal aspects of the high-risk classification

The classification of AI systems as high-risk is made depending on the intended purpose of the AI system.

The intended purpose is defined by Article 3(12) AI Act as the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation.

Question 33. What aspects of the definition of the intended purpose, as outlined in Article 3(12) AI Act, need additional clarification?

Please specify the concrete elements and the issues for which you need further clarification; please provide concrete examples

1500 character(s) maximum

Clarification regarding: - Intended Purpose definition: The AI System guidance suggests that the functionality or AI system objectives alone are not enough to capture the intended purpose and the business context is needed. More guidance is needed on this to understand how granular the business context needs to be. - The AI System guidance implies that the use of the same AI system in two different departments of the same organisation would be two intended purposes - the functionality is the same but the use of the AI system in a business context is different. Is that the correct interpretation? This has significant impact on inventory and material change processes which seek to catch substantial modifications. - For general-purpose AI systems, does "intended purpose" require providers to actively prevent high-risk applications (e.g., preventing a general system from being used for recruitment)? Or is "intended" solely determined by the designed purpose, regardless of potential misuse? - Is the text, "as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation" intended to be exhaustive or can any other communication method suffice.

While the high-risk classification pursuant to Article 6(1) and Annex I AI Act is based on the concept of an AI system being used as a safety component of products regulated under Union harmonisation laws referred to in Annex I, Article 6(2) and Annex III AI Act list certain use cases considered to be high-risk. The two categories are in principle intended not to overlap.

Question 34. If you have or know underline practical examples of AI systems that in your opinion could be relevant for the high-risk classification according to **both Article 6(1) and 6(2) AI Act** and **thus require further clarification**, please specify the concrete AI system, how it is used in practice and how all the necessary elements described above are fulfilled

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

> 1. Risk Management (Article 9): We urge the Commission to clarify that compliance with existing financial sector regulatory frameworks is sufficient to meet the risk management requirements in Article 9. All financial services firms are facing supervisory questions regarding their risk management of AI systems and it is unclear regarding how this supervision interrelates with the requirements under the AI Act. 2. Data and Data Governance (Article 10). Clarification is required re acceptable data quality thresholds and error tolerances,. 3. Technical Documentation and Record-Keeping (Articles 11–12). Clarification on the types of data to be logged, structure of logs, retention policies, and examples of minimum logging requirements; obligations when AI is embedded in complex architectures; clarification on duplicative existing record-keeping requirements (eg. DORA); What level of change would necessitate a new record eg. Upgrading to new version of a model. 5. Human Oversight (Article 14). Further detail is needed on acceptable forms of human oversight, especially in settings where decisions are augmented by AI but still formally taken by a human under well-defined procedures (e.g. credit decisions involving scoring systems). 6. Robustness, Accuracy and Cybersecurity (Art 15): requirements under Art 15 materially overlap with existing cybersecurity and resilience regulation in the EU, introducing duplicative and lower standards for the financial sector. DORA's Risk Management Framework RTS has higher requirements on financial sector with re logging, testing, monitoring & governance. Clarity should be provided regarding the recognition of DORA-related requirements and governance and how they interrelate with the AIA.

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

Already noted in our response to Question 35, financial institutions operate within a strict and well-established regulatory framework, including CRR, GDPR, MiFID II, DORA, and EBA guidelines. The requirements of the AI Act—if not carefully aligned—risk creating overlapping, and at times conflicting, obligations. A single risk management framework should apply to one firm, allowing for more effective oversight, accountability and simplicity. The AI risk management system should be a technology-specific addendum to a firm's wider ICT risk management framework. This reflects how financial services have been regulated in the EU and best practice for cybersecurity governance. Hence, DORA should be included within Annex I as the RMF requirements can be required to demonstrate conformity with Section 2. Enforcement of DORA, in addition, is undertaken by financial regulators and supervisors. Supervision of risk management and cybersecurity is comprehensive and firms are facing a significant increase in RFIs regarding risk management of AI systems prior to the AI Act coming in force. It is unclear how alternative enforcement will occur and if the sector will be subject to competing cybersecurity regimes in the EU. Article 9 on risk management may duplicate existing model risk control mechanisms under CRR, EBA's internal model validation framework and ECB's Guide to IRB models (EGIM) Is a processor role under GDPR inconsistent with a provider role under the AI Act or is there no correlation between these at all? Further guidance /analysis on this topic would be helpful, given that the AI (SaaS) System operator may determine the way in which data are processed under the AI and the Deployer has limited control/visibility.

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

Clarification required that: - Intra-group deployment does not create "provider" responsibilities. (see response to question 49 for more detail). - The scope of applicability of the CE marking requirement under Article 48. Many HRAI systems are not embedded in tangible products, but exist entirely as digital services or internal software components. It is unclear whether and how CE marking should be applied in such cases. - how the conformity assessment procedure under Article 43 interacts with existing supervisory approvals for regulated models and internal risk systems - Article 19 Automatically Generated Logs. Financial regulations already exist for audit, operational risk, and security purposes. Do the AIA Act obligations supplement or replace these, and what level of granularity and retention period is expected? Without alignment, institutions may face burdensome duplication and conflicting requirements, particularly in cross-border or cloud-based environments. - Article 17 - quality management system (QMS). The QMS must be defined in a way that is consistent with existing operational risk management frameworks and already implemented quality and model governance processes. - Obligations and procedures for informing competent authorities of non-compliance or incidents. - The specific time window allowed for submitting the necessary information for EU database registration, following the placing of the system on the market or other triggering events.

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

Fundamental rights assessment and how it interplays with existing requirements under GDPR e.g DPIA. Would welcome clarification in terms of division of duties between deployer/provider and interplay between specifically assigned obligations (e.g. A16/A26) and non-specifically assigned articles (e.g. 9 – 15). As already stated in Questions 35–37, obligations for providers of HRAI systems require clarification regarding their interplay with existing Union legislation. For example, the conformity assessment requirement (Article 43), log retention obligations (Article 19), and documentation and transparency obligations (Articles 11 and 13). Alignment with existing regulations such as CRR, DORA, GDPR or MIFID II and cross-sectoral coordination are essential to ensure legal certainty and proportional compliance. Article 17(4) and 72 states that for providers that are financial institutions, requirements shall be deemed to be fulfilled by complying with the rules on pursuant to the relevant Union financial services law. We would welcome confirmation that FI HRAI providers should take Union financial services law as precedent over the AI Act for Article 17 and 72 and therefore full substituted compliance applies.

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

> As already noted in questions 35–38, financial institutions are already subject to extensive supervisory frameworks and internal control obligations, which in some cases overlap or may conflict with the new duties imposed on deployers under the AI Act. However, a summary is below: - Details on human oversight requirements and how to evidence necessary training, competence, authority and support. There is a reference in 26 to "exercising control over input data" but its not entirely clear what that means or how one should evidence that their data is "relevant and sufficiently representative" - scope and content of record-keeping obligations that apply to deployers of AI systems under the EU AI Act. Specifically, guidance on the following aspects would be useful: o key requirements & objectives of record-keeping for deployers? o What types of logs /documentation to be maintained during deployment /operation? o What specific info should records include to ensure compliance (e.g.system usage data, human oversight actions, incidents or anomalies detected, updates or modifications applied)? o Does transparency on HRAI usage in decision need to be explicit before customer

receives a decision from AI or only after the decision? - Additionally, it could be useful to have practical examples of processes such as: - inform workers' representatives of the usage of AI systems (which information do you need to provide?) - The meaning of the term "immediately" should be clarified, explaining whether it means "within the same day" and whether there is a maximum delay acceptable for informing providers and authorities. - how to interpret the obligation to ensure that input data is "relevant and sufficiently representative". Would data limitations that are justified under sectoral rules still meet the AI Act's expectations? - Re requirements to inform affected individuals when a HRAI system is used to support decision-making may already be partially fulfilled under GDPR (e.g. Articles 13–15) and consumer credit legislation. - Re log retention obligation for deployers. Clarification re what it means for logs to be "under their control", and how responsibility is allocated when deployers rely on external platforms. - Clarity around the proportionate treatment of intra-group deployments, given comprehensive risk management oversight obligated under existing financial regulations.

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

As already indicated in Question 39, several obligations for deployers under Article 26—such as data representativeness, log retention, and information duties—require clarification in relation to existing Union law, particularly GDPR, CCD, and DORA. These areas would benefit from consultation with financial authorities, to ensure proportional and harmonised application of obligations We would welcome confirmation that FI HRAI providers should take Union financial services law as precedent over the AI Act for Article 26(5) and therefore full substituted compliance applies. Article 26(5) states that for deployers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to the relevant financial service law

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

The FRIA template should clarify which risks fall outside the scope of GDPR but within the FRIA, e.g., algorithmic bias affecting access to credit, even if not involving special category data; and how to treat ancillary systems, such as customer-facing chatbots or documentation analysis tools, which support but do not determine decisions The template should offer sector-specific examples and clarify how FRIA content should interact with risk management obligations under Articles 9–10. It would be beneficial to include practical examples illustrating both the completion of the relevant documentation and the interpretation of results. Additionally, clarification is requested on the application of specific thresholds, if any, and how these thresholds should be considered during the evaluation process, especially if different thresholds are in conflict Clarifications should be provided regarding the relationship between Risk assessment and the Fundamental Rights Impact Assessment (FRIA) so to simplify and make more effective and efficient the management of these two requirements.

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 ensure complementarity between the FRIA and the DPIA when analyzing data protection risks, while avoiding overlaps, it is essential that the FRIA template explicitly builds upon existing DPIA outputs, and includes only additional elements specific to fundamental rights not covered by GDPR, such as fairness in decision-making, access to services, or indirect socio-economic discrimination. Both assessments should follow a modular structure, with cross-references to avoid repeating documentation, especially for institutions that already assess models for regulatory, operational, and reputational risk under financial law. In this regard, it would be highly useful to have access to illustrative examples clarifying how both assessments interact and how they can be efficiently integrated in practice.

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

Request clarity on: - what the impact on article 86 is, if it's not the deployer of the AI system taking the relevant decision but a user of the output. Who is accountable to explain the decision in that case? - Timeframe for Submitting Explanation Requests: Clarification is needed on whether there are specific time limits for affected individuals to request an explanation for a decision, such as a maximum number of days after the decision - Timeframe for Responding to Explanation Requests: Guidance is sought on the deadline for the deployer to respond to an explanation request, including whether there is a mandatory response period - Content and Granularity Requirements of the Explanation: Clarification is requested on the required level of technical detail in the explanation, including minimum content requirements such as decision logic, data sources, and risk factors - Acceptable Formats for Delivering Explanations: Clarification is needed on the acceptable formats for explanations, including whether specific or standardized formats are required and if the explanation should be accessible to non-experts - Clarification is needed on whether the explanation given following GDPR and CCD

obligations is sufficient or, on the contrary, further details on the technical functioning of the AI system or on the factors that influenced the outcome shall be provided. - Also clarify the threshold for when the output of an AI system is deemed to "significantly affect" the person.

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

• Clarity that substantial modification and placing on the market do not relate to inter-affiliate or intragroup provision of IT services via shared intragroup resources. • Specific clarity is needed on 2hat constitutes a substantial modification where: o Provider has not provided sufficient information to a deployer to assess if a substantial modification has occurred. o Deployer modifies weights of model using tools supplied by Provider, without changing the model architecture or intended purpose, does this constitute substantial modification requiring a new conformity assessment? What if modifications were already foreseen in conformity assessment o In view of article 111, given the exemption for AI systems in service before 2 Aug 2026, unless significant

changes in their design), and particularly in financial services where AI systems are subject to continuous updates due to supervisory, validation, or recalibration processes without changing the underlying model architecture or logic. • Guidance needed on how to assess digital modifications as products evolve, eg. product updates, without triggering disproportionate regulatory obligations. Should be aligned across the relevant regulations including the CRA. Additional clarification on: - is substantial modification, same as "significant change in design" under Article 111 - the scope and definition of a "foreseen" change for the purpose of the first part of A3(23) (Definition of Substantial Modification), in particular: o Is A3(23) exhaustive as to where a "foreseen" change can be found or just an example, i.e. will a change only be seen as "foreseen" by provider if foreseen or planned in their original conformity assessment? o What if in technical documentation, monitoring plans, instructions for use, promo/sales materials, risk management system, DPIAs, FRIAs etc.? o What if a change should have been reasonably foreseen by the provider, but was not explicitly stated in the CA/other documentation? - interplay of "foreseen" changes A3(23) with wider scope of where "intended purposes" in A3 (12)? - Clarification that the following would not be considered substantial modification: o re-training of a HRAI system, with new datasets or altered training parameters? o version upgrades of programming language o security measures to ensure that sensitive financial data is protected o integrating the LLM to integrate with existing banking systems, such as CRM, transaction processing systems, and risk management tools o adjustments to ensure LLM adheres to financial regulations eg. KYC/AML o Actions to minimise bias in the LLM o fine-tuning the LLM o customizing UX o scaling and efficiency improvements. - Re Article 25 : if any Deployer rebrands a HRAI system is it classed as Provider? Is there a materiality threshold?

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

Clarification is needed on how to operationalise the exception for "pre-determined changes" under Article 43(4). In practice, many AI systems in financial services—especially scoring or fraud detection models—are designed with pre-approved update procedures. These may include: - Scheduled re-training of models on new data sets; - Threshold adjustments based on concept drift or distribution shift; - Parameter recalibration within predefined operational limits. If these updates are defined and documented at the time of initial deployment and included in the technical documentation (e.g. model lifecycle governance), they should not be deemed substantial or require a new conformity assessment, even when performance metrics shift as a result.

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

> Members expect that in most circumstances they will be Deployers or consumers of AI systems. Depending on use cases, some firms may also be considered Providers of some systems. . Additionally within the corporate group structure there could be multiple entities performing different roles in the value chain across the group.

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

> Clarity is needed on the relationships between: 1) GPAI model providers (e.g., GPT series), 2) GPAI system providers (e.g., ChatGPT), and 3) downstream providers/deployers. Specifically, if a company adapts a GPAI system, adds its own branding, and deploys it, are they considered the "provider" of the system but not the model? ? Is the answer different if no branding is added or if it is disclosed that the AI system is "powered by e. g. ChatGPT". Further is this scenario different if it is intra-group? There should be clarity on the Article 25 requirements suggesting a GPAI model/system provider must provide information to downstream providers of HRAI to a enable compliance. Currently, vendors can resist providing certain information citing commercial reasons Eg. A GPAI provider should provide the following: 1. Documentation of the model training data (sources, types,pre processing) 2. Analysis that the provider has conducted around bias and fairness analysis 3. Disclosure of security and privacy features and testing conducted 4. Performance metrics, known limits of the model 5. Confirmation of adherence to industry standards 6. Enabling access, so the deployer can audit and monitor the model's performance. How should the dependencies between an AI system and the entire ecosystem be treated? For example: The integration of AI and non-AI components creates a broader decision-making ecosystem where biases can emerge from interactions between systems and rules.

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

A clear expectation on the documentation which Providers must provide for organisations using their systems. See Q47 for details

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

Clarity required: -that HRAI deployment by a firm for inter-affiliate purposes (eg. multi-national firms that centrally modify models for use across group affiliates), should not be captured under the definition of HRAI provider, but instead considered "own-use". -that the definition of "placing on the market" does not apply to firms using HRAI internally only, and therefore does not deem the firm a "Provider". -what responsibility is placed on firms using industry wide vendor/third-party AI systems. E.g, where firms access models via cloud providers, what level of documentation will a HRAI provider be required to provide to a cloud provider to ensure a level of comfort in meeting the technical documentation requirements for HRAI -regarding the application of the risk propagation principle under the EU AI Act, particularly: -regarding complex system architectures where HRAI modules are used as components or inputs in broader workflows: 1.how to determine where the AI system starts and ends? Guidance including use cases would support consistent risk categorization and avoid unintentionally extending scope of the AI Act. 2.if a non-AI system uses the output of an AI system, does it become an AI system itself? 3.If HRAI outputs are inputs into other processes, does the HRAI risk classification "propagate" downstream, or is each component assessed independently? Do exceptions apply, eg. if process outputs in a limited, non-deterministic, or human-in-the-loop context

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 <u>concrete examples of AI systems</u> 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

We believe it is premature to consider including new high-risk cases in Annex III, as doing so would only increase uncertainty in the industry regarding AI adoption by adding further cases while we are still defining requirements and adapting our systems. It is important to recognize that companies must undergo a transition to this new framework—one that requires time, resources and careful planning—and that stability is crucial. In our view, new use cases should only be added when there is clear evidence of risks already materializing in terms of health, safety or fundamental rights. On the other hand, however, we consider it justified to refine the existing list of high-risk cases by excluding specific use cases that might technically fall within its scope but do not, in fact, pose a high risk to individuals. This will provide certainty to companies and simplify implementation.

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

◉ Yes
◯ No

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

3000 character(s) maximum

The use cases listed in Annex III should be adapted to exclude systems based on basic statistical techniques, such as logistic regressions, when these systems are static and do not exhibit autonomy or adaptiveness. Also the scope of Point 5(b) should be narrowed to cover only AI systems that support decision-making on access to credit by natural persons. Other uses of AI in credit-related processes—such as internal risk analysis, pricing simulations, or customer segmentation—do not have a direct impact on fundamental rights, health, or safety and therefore should be explicitly exempted from complying with obligations on HRAI systems as already foreseen for AI systems used for the purpose of detecting financial fraud. Additionally, we propose that the following categories be considered for adaptation: Point 4 – Employment, workers' management and access to self-employment: The scope should explicitly exclude AI systems that are not intended to evaluate, guide or influence employee behaviour or performance, but are used exclusively to ensure compliance with legal obligations (e.g. logging of access, communications, or documentation in regulated environments). Point 5 – Access to and enjoyment of essential private and public services: The rationale for exempting financial fraud detection systems should be extended to other AI systems used strictly for compliance with specific financial regulations. Point 6 – Law enforcement: Clarification is needed to explicitly exclude AI systems used solely to meet Anti-Money Laundering (AML), Know Your Customer,, transaction monitoring, or financial sanctions screening obligations. These systems are not used to investigate or prosecute crimes, but to generate alerts or reports to be assessed by human analysts before being submitted to competent authorities. As stated in Recital 59, administrative functions carried out for AML compliance do not qualify as law enforcement activities

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

Please justify why you consider that this system should no longer be classified as high-risk

3000 character(s) maximum

We do not consider that any of the use cases listed in Annex III should be removed. However, we remain concerned about the broad interpretation of the AI system definition under Article 3(1), which may lead to the unjustified inclusion of systems that do not pose comparable risks within the scope of high-risk obligations— particularly in relation to Point 5(b). If the definition of an AI system is interpreted too expansively—e.g. to include static, rule-based systems or basic statistical tools such as logistic regression models—it could bring into scope technologies that lack autonomy, learning capability, or complexity, and whose risks are already mitigated through existing sectoral regulation and human oversight. This does not question the relevance of the use cases listed in Annex III, but rather highlights the need to ensure that only systems meeting the AI definition and associated risk criteria are captured under the high-risk classification. Point 5(b) should be narrowed to cover only AI systems that support decision-making on access to credit by natural persons. Other uses of AI in credit-related processes, eg. internal risk analysis do not have a direct impact on fundamental rights, health, or safety so should be exempted. Where models do not take a final decision but instead provide output for a human assessment, these should not fall within the high-risk scope. If a low risk model output is input into a high-risk use case, the input model should not be considered as part of the high-risk system. Access to financial services such as credit cards or pre-approved credits are not considered in the scope of high-risk use cases. Those services would not impact "the right of people to fully participate in society or to improve one's standard of living" as described in recital 58 and should be excluded from the scope of high-risk. Although not specifically on Annex III, we raise some additional questions: o Regarding the scope of "placing on the market or "putting into service" (art. 2 would this apply irrespective of the end-user's location, or only to systems whose operation directly or indirectly affects EU residents or citizens. o clarification on what is "materially influencing" (Art 6.3). Needs an objective criteria or a common methodology to assess materiality. We propose clarifying that a system's influence is not material if it is limited to pre-filtering or preliminary classification tasks, without effectively restricting access to services

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 <u>concrete examples of AI practices</u> 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

Annex III paragraph 4 – Not all HR tools pose the risks identified under 7(3). This section should be clarified /more nuanced to distinguish between decision making tools and support tools.

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](#)