DeutscherAnwaltVerein

Position Paper

of the German Bar Association prepared by the Committee on IT Law

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

Position Paper No.: 38/2025 Berlin/Brussels, July 2025

Members of the Committee

- Rechtsanwalt Prof. Niko Härting, Berlin (Chair)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München (Rapporteur)
- Rechtsanwalt Prof. Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwalt Dr. Helmut Redeker, Bonn
- Rechtsanwältin Dr. Kristina Schreiber, Köln
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

Guest Contributor

- Rechtsanwalt Nicolas Kötter, München (Rapporteur)

In charge in the Berlin Office

- Rechtsanwältin Nicole Narewski, Director

Contact in Brussels

- Rechtsanwältin Dorothee Wildt, LL.M., Deputy-Head
- Myra Jockisch, LL.M., Legal Advisor

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparency Register ID number:
87980341522-66

www.anwaltverein.de

The German Bar Association (Deutscher Anwaltverein – DAV) is the professional body comprising about 60.000 German lawyers and lawyer-notaries in 253 local bar associations in Germany and abroad. Being politically independent the DAV represents and promotes the professional and economic interests of the German legal profession on German, European and international level. The DAV is registered in the Lobby Registry for the representation of special interests vis-à-vis the German Bundestag and the Federal Government under register number R000952.

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

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

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

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

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

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

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

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

O Yes
X 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);

X A component of a product or of a system which is intended to **monitor and detect** the need to schedule maintenance and inspections, which, if not conducted, may lead to physical harm to people or property (e.g. AI system detecting whether parts of a product are worn and may need replacement or maintenance);

X A component of a product or of a system which is intended to **prevent** a physical harm to people or property (e.g. AI system preventing a start of a system if an abnormal behaviour is detected);

X A component of a product or of a system which is intended to **control or limit** possible physical harm to people or property (e.g. AI system controlling specific behaviour or function of a system and adjusting its function accordingly);

X A component of a product or of a system which is intended to **mitigate consequences** of possible physical harm to people or property (e.g. AI system that triggers action such as safe-stop if dangerous condition occurs);

X A component of a product or of a system which **controls or supervises** another system that performs a safety function (e.g. AI systems supervisor through sensors an operation in real time of a safety component that directly performs the safety function);

O 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;

O 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);

X Other

O Can’t answer this question.

Please specify

1500 character(s) maximum

In the case above ("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"), it depends on the type of core function to determine whether the AI system as defined in Art. 3 No. 14 “fulfills a safety function for this product or AI system or whose failure or malfunction endangers

the health and safety of persons or property.” Yes, if the AI system is e.g. autonomously driving; no if the AI system is generating text.

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**
Legislation's name Directive 2006/42/EC	*Description* *750 character(s) maximum* Industrial hydraulic press. Predictive maintenance, anomaly detection, safety monitoring.	*Explain* *500 character(s) maximum* Is it a safety component, because in general maintenance prediction prevents hazardous failures? Or only if it controls safety-critical operations (e.g., emergency stop)?
Legislation's name Directive 2009/48/EC	*Description* *750 character(s) maximum* Ride-on toy car. AI system for obstacle avoidance	*Explain* *500 character(s) maximum* Safety component since AI might prevent collisions even though speed really limited and therefore usually not life threating.
Legislation's name Directive 2014/33/EU	*Description* *750 character(s) maximum* System in passenger lift for load prediction, fault detection.	*Explain* *500 character(s) maximum* If AI prevents overloads or detects faults that could cause injury.
Legislation's name Regulation (EU) 2016 /424	*Description* *750 character(s) maximum* AI system checking on ski lift for safety analytics.	*Explain* *500 character(s) maximum* Safety component even though the AI system (e.g. camera with AI detection of material cracks is separate from the lift itself?

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**
Legislation's name Regulation (EU) 2018 /858	*Description* *750 character(s) maximum* AI for infotainment personalization in connected cars	*Explain* *500 character(s) maximum* Distraction or system crash could impair driver attention leading to accidents. Are such cases covered even though only human reaction leads to danger?

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

-

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

-

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

The respective Union harmonisation legislation	Short description of the use case	Points where you need further clarification
Legislation's name Regulation (EU) 2017 /745	*Description* *750 character(s) maximum* AI Chatbot for Mental Health Support. Gives misleading advice, worsening a user's condition.	*Explain* *500 character(s) maximum* According to the MDR, software (including AI systems like chatbots) is considered a medical device if it is intended by the manufacturer to be used for diagnosis, prevention, monitoring, prediction, prognosis, treatment, or alleviation of disease (Article 2(1) MDR). What if the chatbot is not designed but can be used for such purposes? (in several cases AI chatbots led user to commit suicide). Probably not covered, correct?

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

Clarification of whether a safety component can also be pure software. The explanation of the term "ai system" in recital 12 (2) indicates this understanding because AI systems shall be distingushied from classic software.

What if AI is not part of the product, but if the AI system does not work or works incorrectly, consequential damage can occur, e.g., a camera on bridges or ski lifts that

detects and reports damage through image recognition? Interaction with sector-specific definitions of the term “safety component”, e.g., for medical devices in the context of essential functions (see IEC 60601-1:2022) or analogously in the automotive industry (according to ISO 26262 and IEC 61508). In addition, there are national laws and European regulations that contain similar definitions (e.g., German BSI Act § 2 (13) for critical components in critical infrastructure, Annex 3 in Directive 2014/33/EU on lifts and safety components for lifts)". Is an AI system with a safety function not a safety component if there are redundant safety mechanisms? Example: In the AI-supported energy supply of a gas processing plant, there may be redundant systems that kick in if the AI system fails or is faulty. Would the AI system no longer be a safety component in this case.

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

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

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

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

situations when such AI systems would not be classified as high-risk if one or more of the following conditions are fulfilled:

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

However, this exception cannot be applied if the AI system performs profiling of natural persons.
A provider who considers that an AI system referred to in Annex III falls within one or more of the
exceptions should document its assessment before that system is placed on the market or put into service and register it according to Article 49(2).

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

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

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

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

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

- *Point 1(a) of Annex III to the AI Act refers to the use of remote biometric identification systems. These systems aim at the remote (at a distance, without the active participation of the person in question) automated recognition of a natural person, for the purpose of establishing the identity of that person, by comparing the biometric data of that individual to biometric data of individuals stored in a database. Verification and authentication, used for the confirmation of the identity of a natural person, are not considered to be high-ris AI systems performing biometric categorisation may fall under the scope of prohibited systems if they fulfil the cumulative conditions defined in Article 5(1)(g) AI Act which are further developed in Section 8 of the Commission Guidelines on prohibited AI practices.*
- *Point 1(b) of Annex III to the AI Act refers to the use of biometric categorisation AI systems that are categorising natural persons according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics, unless the categorisation is ancillary to another commercial service and strictly necessary for objective technical reasons (Article 3(40) AI Act). According to recital 54, AI systems intended to be used for biometric categorisation according to sensitive attributes or characteristics are those attributes and characteristics protected under Article 9 (1) of Regulation (EU)*

2016/679. AI systems performing biometric categorisation may fall under the scope of prohibited systems if they fulfil the cumulative conditions defined in Article 5(1)(g) which are further developed in Section 8 of the Commission Guidelines on prohibited AI practices.

- *Point 1(c) of Annex III to the AI Act refers to the use of emotion recognition systems. These are AI systems for identifying or inferring emotions or intentions of natural persons on the basis of their biometric data. As clarified in recital 18 AI Act, emotion recognition includes for example emotions such as happiness, sadness, or anger. It explicitly excludes the recognition of physical states such as pain or fatigue. AI systems intended to perform emotion recognition may fall under the scope of prohibited systems if they fulfil conditions defined in Article 5(1)(f) AI Act, which are further developed in Section 7 of the Commission Guidelines on prohibited AI practices.*

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

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

Name and description of the system	**Category of biometric system**	**The system is considered**	**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**
	Remote biometric identification (Point 1	*High Risk:* Yes, completely	*Explain:* AI analyses archived video	*Profiling: Unsure*	*Exception: Unsure*	*Explain:* Profiling might take place through

	(a))		footage to identify suspects after a crime. No prohibition since not in real time.			analysis of location but only regarding a past moment in time. Performance of a narrow procedural task? Rather not.

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

	Name and description of the system	**Category of biometric system**	**Category of prohibited AI system with which there may be an interplay**	**Motivate your previous answer**
1	AI systems used at concerts or sports venues to identify banned individuals.	Remote biometric identification (Point 1 (a))	*High Risk* Unsure	*Explain* Probably a real-time' remote biometric identification system falling under art. 5 (h). If not prohibited under Art. 5(1)(g)? But probably not because only AI systems that process very specific types of biometric data and derive information from them are such as race, political opinions, trade union membership, religious or philosophical beliefs, sexual life, or sexual orientation are prohibited under art. 5 (g).
2	AI system for biometric categorisation not specifically	Biometric categorisation (Point 1 (b))	Biometric categorisation system (Art. 5(1)(g))	*Explain* Art. 5 (g) only applies to "categorisation systems that categorise individually natural

	targeting individuals unlike above			persons based on their biometric data". Annex III no. 1 (b) does not mention the individual categorisation ("AI systems intended to be used for biometric categorisation ..."). How to differentiate those use cases? Put differently: How do you determine whether or not an AI system directly targets people individually?

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

1500 character(s) maximum

-

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
AI system for detecting anomalies in remote commands or requests for access that is also intended to prevent power grids from being overloaded.	Supply of electricity	*High Risk* Unsure	*Explain* According to recital 55 safety components used exclusively for cybersecurity purposes are not to be covered. How to distinguish those safety components from other safety components if cybersecurity risks are also intended to prevent physical damage to critical infrastructure?	*Profiling* *No*	*Exceptio n* *No*	*Explain* -

Question 11. If you need further clarification 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

According to recital 55 safety components used exclusively for cybersecurity purposes are not to be covered.

How to distinguish those safety components from other safety components if cybersecurity risks are also intended to prevent physical damage to critical infrastructure?

Question 12. If you have or know practical examples of components 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 high-risk AI systems related to education and vocational training.

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

Name/description	Category	High-risk	Explain	Profiling	Exception	Explain
Generative AI (e.g. ChatGPT)	Access/admission to education (Point 3(a))	*Unsure*	The difficulty we see is that depending on the prompt they can switch from a simple supporting role like creating teaching materials to grading tests or deciding which candidate to pick. When is a multi- purpose AI system intended to be used for high-risk task? Only if the manual of the provider says so?	*No*	*Unsure*	Might only execute a narrow task depending on the prompt.

Question 15. If you have or know practical examples of AI systems related to education and vocational training for which you need further clarification regarding the **distinction from prohibited AI systems**, please specify which category of AI system is concerned.
1500 character(s) maximum

How should generative AI (e.g. ChatGPT) be handled? The difficulty we see is that depending on the prompt they can switch from a simple supporting role like creating teaching materials to grading tests or deciding which candidate to pick. Who should limit the use to non-high risk use cases?

The provider can exclude high-risk use cases in the manual; if that is the case but the AI system is also used for other purposes, the deployer becomes the provider acc. to art. 25 AI Act.

Question 16. If you see the need for clarification of the high-risk classification in *Point 3 of Annex III to the AI Act* and its **interplay with other Union or national legislation**, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay
1500 character(s) maximum
-

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

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

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

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

- *Point 4(a) of Annex III to the AI Act refers to AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates.*
- *Point 4(b) of Annex III to the AI Act refers to AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.*

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

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

Name/description	Category	High-risk	Explain	Profiling	Exception	Explain
AI system for any decisions that affects working conditions in the employment relationship.	Managing work relationships and performance monitoring (Point 4(b))	Unsure	Is it true that this high-risk area has been significantly expanded in the legislative process and, instead of covering only certain cases, such as promotion, termination, performance and conduct monitoring, or the assignment of tasks, as originally planned, the final wording now covers all decisions that affect	Unsure	Unsure	Depends on the specific use case.

			working conditions in the employment relationship? The wording "in particular" in (a) indicates such understanding.			
AI system for any probability based prediction that might affect working conditions in the employment relationship.	Managing work relationships and performance monitoring (Point 4(b))	Unsure	Is it true that the term “decision” in (b) must be interpreted as broadly as possible in light of the ECJ's SCHUFA ruling (ECJ, judgment of December 7, 2023, case C-634/2, para. 62) on the concept of “automated individual decision-making” under Art. 22(1) GDPR? If yes, is it correct that even a mere prediction based on a probability value is to be understood as a decision, even if it is made by a third party, provided that the actions of the person to whom this probability value is communicated are significantly influenced by it?	Unsure	Unsure	Depends on the specific use case.

Question 18. Do you have or know practical examples of AI systems related to employment, workers’ management and access to self-employment where you need further clarification regarding the **distinction from prohibited AI systems**?

-

Question 19. If you see the need for clarification of the high-risk classification in *Point 1 of Annex III to the AI Act* and **its interplay with other Union or national legislation**,

please specify the practical provision in other Union or national law and where you see need for clarification of the interplay

1500 character(s) maximum

-

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

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

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

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

Point 5(b) of Annex III to the AI Act refers to AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud. According to recital 58, AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and

insurance undertakings' capital requirements should not be considered to be high-risk under the AI Act. Point 5(b) of Annex III therefore contains two distinct use cases:

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

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

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

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

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

Examples may include systems for which you have uncertainties or system that you consider should not be considered high-risk as they are outside the use cases listed in

Annex III or they fulfil one or more of the conditions for the exceptions in Article 6(3) AI Act.

Name and description of the system	**Category of AI system**	**The system is considered**	**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**
AI systems that exclusively make positive decisions (e.g. the clear positive cases) and refer other cases to human decision maker.	Evaluation of creditworthiness/ credit score of natural persons (Point 5(b))	*High-risk* Unsure	*Explain* Is it sufficient for an AI system to only make decisions in one direction (approval, rejection, etc.), or must it be able to decide in both directions?	*Profiling* Unsure	*Exception* No	*Explain* Profiling most likely takes places. Unlikely to perform only narrow task.
Credit rating algorithm (usable for access to essential and non-essential services)	Evaluation of creditworthiness/ credit score of natural persons (Point 5(b))	*High-risk* Partially	*Explain* What is the significance of the introductory text (“essential services”)? Is it restrictive, e.g., is it only relevant for credit rating if it also influences access	*Profiling* Unsure	*Exception* No	*Explain* Profiling most likely takes places. Unlikely to perform only narrow task.

			to essential services? That is our understanding acc. to recital 58. What about an AI-system usable for rating of credit worthiness for access to essential and non-essential services? Does the provider have to specify that the rating is only for access to essential services or is a case-to-case assessment necessary?			
AI Chabot used by public administration, usable for non-critical purposes, but also for inquiries regarding essential services, e.g., for the assessment of an application for	Evaluation of eligibility for public assistance benefits and services (Point 5(a))	*High-risk* Unsure	*Explain* The development and use of general AI systems in public administration should expressly not be covered or hindered (recital 58 (4)). However, how to deal with cases where a multi-purpose AI system can also	*Profiling Unsure*	*Exception Unsure*	*Explain* Depends on specific case.

unemployment benefits.			be used for high-risk use cases?			

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

How can AI systems using profiling be distinguished from prohibited social scoring when it comes to access to and use of basic private and public services and benefits?

Is social scoring deemed to exist only if, in addition to objective and factual criteria, personality-related or behavioural characteristics are also used to determine access to public services or private credit, or only when leading to unjustified and disproportionate discrimination?

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

1500 character(s) maximum

-

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*?

-

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

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

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

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

natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 (defined as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements) in the course of the detection, investigation or prosecution of criminal offences.

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

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

Name and description of the system	Category of AI system	High-risk	Explain	Profiling
AI systems that predict where crimes are likely to occur or who is likely to commit them, based on historical crime data and personal profiles.	Assessing re-offending risk in law enforcements (Point 6(d)) AND Profiling individuals in criminal investigations (Point 6(e))	Unsure	Possibly considered high-risk, but it remains questionable whether the AI system is intended to be used by law enforcement authorities or in support of law enforcement-	Yes

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

Name and description of the	Category of AI system	Category of prohibited AI	Please motivate your answer

system		system with which there may be an interplay	
AI system using personal data and location related data (e.g. traffic) to predict criminal behaviour by providing police officers suggestions, which can be dismissed by them.	Assessing re-offending risk in law enforcements (Point 6 (d))	Predicting criminal behaviour (Art. 5(1)(d))	*Explain* The wording of Art. 5(1)(d) of the AI Act only prohibits risk assessments that are "based solely on the profiling of a natural person or the evaluation of their personality characteristics and traits." Thus, only personal risk assessments are covered, not location-based risk assessments. The prohibition of personal prediction systems within the meaning of Article 5(1)(d) of the AI Act is also restricted by two points in particular: First, predictive policing must be based exclusively on profiling, personality traits, and characteristics. Second, the prohibition does not apply if the AI system is used to support human review and this review is based on objective and verifiable facts directly related to criminal activity.

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

1500 character(s) maximum

-

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

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

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

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

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

1500 character(s) maximum

-

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

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

-

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

-

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

1500 character(s) maximum

-

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

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

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

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

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

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

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

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

Name/description	Category	High-risk	Explain	Profiling	Exception	Explain
A judge uses an	Assisting judicial	Unsure	It should be a high-risk use case in terms of its	No	Unsure	It could be a procedurally

AI chatbot to obtain a legal assessment of a case or a draft outline for a written brief.	authorities or used in similar ways in alternative dispute resolution (Point 8 (a))		specific application. Judges are also a judicial authority acc. to recital 61. However, it is unclear whether this is an AI system that is intended for use in this particular application. This would probably only be the case for AI systems that are explicitly developed/ marketed for use in the justice system.			narrow supportive use case, e.g., if only a summary of the case is created without application of legal text to the case.
An AI system used to determine where and to whom political advertisements are displayed in order to sway swing voters as much as possible.	Influencing election outcomes or voting behaviour (Point 8(b))	Unsure	According to the wording of lit. b, AI systems whose output is not directly exposed to natural persons, such as AI systems for the administration, logistics, or structuring of political campaigns, are expressly excluded from the scope of application. The use case could be seen as structuring because it does not directly create content that voters see.	Unsure	Unsure	Maybe it is arguable that the AI system is intended to only perform a preparatory task for an assessment that is relevant for the purposes of the use cases listed in Annex III.
Finding relevant case law, legal literature, and other	Assisting judicial authorities or used in	Yes, completely	A court uses an AI System that has the intended purpose to find relevant case law, legal literature, and other legal sources. The judge	No	Unsure	Unclear from the current wording of point 8 whether it is exempt pursuant to

legal sources	similar ways in alternative dispute resolution (Point 8 (a))		uses the findings of the AI system.			Article 6(3)(a) and (d) AI Act. One significant concern with the use of AI in judicial contexts is the potential overreliance on AI-generated legal references or case law. When AI systems are used to retrieve or suggest legal sources, there is a risk that judges or legal practitioners may begin to trust these outputs without critically reviewing the original materials themselves. This can lead to a situation where the AI system, rather than the human decision-maker, effectively shapes the legal reasoning and outcome of a case. If the AI system's suggestions are accepted at face value—without thorough human

						scrutiny—its influence on judicial decisions becomes substantial, even though it lacks true understanding or accountability. Such a dynamic could undermines the independence and depth of legal reasoning, especially if the AI system introduces subtle biases, omits relevant counterarguments, or misinterprets legal nuances. It is therefore essential to maintain a strong culture of critical engagement with AI outputs and to ensure that human oversight remains central in all stages of legal decision-making.
Use of AI by a court-appointed expert	Assisting judicial authorities or used in similar ways in	Yes, completely	A court-appointed expert is tasked with producing a report on factual findings for the court. The expert uses an AI system to examine the documentation and	Unsure	Unsure	Perhaps profiling if the court expert evaluates the state of health of a natural person. Unclear whether it could be exempted

	alternative dispute resolution (Point 8 (a))		prepares an expert report about the factual findings. The expert then submits the report to the court. Acc. to recital 61 (2) "it is appropriate to qualify as high-risk AI systems intended to be used by a judicial authority or on its behalf to assist judicial authorities in researching and interpreting facts".			pursuant to Article 6(3)(a) and (d) AI Act. As the parties are normally able to ask questions to the court-appointed expert (in writing and during oral testimony) and present factual evidence, the risk of unquestioned use of AI research facts does not in general seem high.
Like above but a party appoints the expert.	Assisting judicial authorities or used in similar ways in alternative dispute resolution (Point 8 (a))	No	Like above but a party appoints the expert. This is not covered acc. to recital 61 (2) "on the courts behalf to assist [the court] in researching and interpreting facts and the law and in applying the law to a concrete set of facts".	No	No	
Like above but the AI system is used by a witness.	Assisting judicial authorities or used in similar ways in alternative dispute resolution (Point 8	No	Like above but the AI system is used by a witness called to give testimony before a court. In its private preparation for the testimony, the witness prompts an AI System with reviewing relevant materials available to	No	No	

	(a))		the witness (e.g. exhibits involving the witness) and asking the witness relevant factual questions. The AI system inadvertently hallucinates facts and manipulates the witness to change her recollection of events. A witness is not a judicial authority and is not acting on behalf of the court.			
Like above but an attorney representing a party uses the AI system to review documents or to research relevant legal sources/ case law or to draft a motion.	Assisting judicial authorities or used in similar ways in alternative dispute resolution (Point 8 (a))	No	Like above but an attorney representing a party uses the AI system to review documents or to research relevant legal sources/ case law or to draft a document to the court. An attorney is not a judicial authority and is not acting on behalf of the court". Also e.g. if an attorney is appointed by the court as the trustee in a bankruptcy estate.	Unsure	No	Perhaps profiling in case of mandates relating to employment or family law. Perhaps profiling if attorney is appointed by the court as the trustee in a bankruptcy estate and if the previous managing director of the insolvent company is evaluated
AI use by a judge to proof read	Assisting judicial authorities or used in similar ways in alternativ	No	A judge uses an AI system to review his draft judicial decision for errors in translations, spelling and grammar. The use case does not involve any "researching	No	Yes	The AI system is intended to improve the result of a previously completed human activity.

	e dispute resolution (Point 8 (a))		and interpreting facts and the law and in applying the law to a concrete set of facts", and involves little or no real risk to fundamental rights.			
AI-based transcription and translation of language of witness testimonies	Assisting judicial authorities or used in similar ways in alternative dispute resolution (Point 8 (a))	No	Parties to an arbitration agree that all witness testimony will be with AI-based transcription and translation of language (instead of an appointed court reporter and translator) in order to save costs. The use case is not encompassed by the intent and wording of the EU AI Act's Article 6(2) and Annex III, item 8(a). In particular, the arbitral tribunal does not use the AI System "in researching and interpreting facts and the law and in applying the law to a concrete set of facts".	No	No	
AI dual use by a judge to proof read and to give hints on legal aspects	Assisting judicial authorities or used in similar ways in alternative	Unsure	A judge uses an AI system to review his draft judicial decision for errors in translations, spelling, grammar but also asks to give an assessment whether he has overlooked relevant aspects in his legal assessment.	No	No	

	dispute resolution (Point 8 (a))		Partly applying the law to a concrete set of facts”,			

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

1500 character(s) maximum

-

Section 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

How are AI systems regulated, that can be used for a variety of purposes, such as GPAI systems? Will the specification of purposes not be purely theoretical and essentially an invitation to providers to avoid regulation by simply specifying the narrowest possible purpose that does not entail high-risk regulation, knowing full well

that there are no technical barriers to using the system for such purposes? Does Article 6(3) of the AI Act provide an exhaustive list of cases in which self-assessment is permitted, or should the listed cases be understood as examples (i.e., non-exhaustive)?

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 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

What happens if an emotion recognition function (according to Art. 6 para. 2, Annex III no. 1 (c) is used in a vehicle for passenger transport, such as a city bus or private vehicle, to which according to Art. 2 para. 2 in conjunction with Annex I Section B no. 18 the AI-Act is not applicable). In this case, the emotion recognition system falls under the AI Act, but the vehicle falls under Annex I Section B of the AI Act. Is that correct? Or is there a blocking effect, i.e., for an AI system that falls within the scope of Art. 6 (1) AI Act in conjunction with Annex I, Section B AI Act, the application of Art. 6 (2) AI Act is excluded on the basis of specialty? This is backed by the wording of Article 2 (2), first sentence: “only Article 6 (1) shall apply ...”.

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

According to Article 8(1) of the AI Act, the implementation of Articles 9 to 15 of the AI Act must always take into account the intended purpose and the generally accepted state of the art in relation to AI and AI-related technologies.

Is it correct that therefore, unlike in the original Commission proposal, Articles 9-15 no longer provide for uniform ("one size fits all") regulation of high-risk systems, but should rather be read as basic principles?

Is it correct that the requirements clarify that the provider does not have to consider all conceivable misuse scenarios when fulfilling the high-risk obligations, but only has to take measures that are generally known and recognized at the time of market introduction? On the other hand, according to Art. 9(2) of the AI Act, the risk management system must be reviewed and updated regularly and systematically.

According to Article 9(3) of the AI Act, the risk assessment may also be limited to aspects that can be mitigated or eliminated appropriately through the development and design of the high-risk AI system or through the provision of sufficient technical information. Is it correct that the provider is therefore not required to anticipate and take into account all conceivable risks that may arise on the operator side?

Art. 10: Due to the central role played by machine learning and, in particular, deep learning in the development of current AI systems, as well as the central role of training data in development, Art. 10 AI Act is a key provision of the AI Act. Problematic is that there is no generally accepted definition of the term bias. The same applies to the quality requirements for data sets in Art. 10(3) and (4). The terms are not defined in the AI Act or in the recitals. Will there be clarification on this?

According to Article 12(2), the logging functions should enable the recording of events that are relevant for the following: The identification of situations that could lead to the high-risk AI system posing a risk within the meaning of Article 79(1) of the AI Act (“risk at national level”) or to a significant change in the AI system. This is the case if the AI system adversely affects the health, safety, or fundamental rights of data subjects to an extent that is unreasonable and unforeseeable in light of the intended purpose. This reference is very broad, and it is difficult to determine when an unreasonable risk arises. Is it true that to be on the safe side, providers should log all events that occur outside the scope defined by the intended purpose? It remains unclear what type of logging is suitable for monitoring. Choosing the right logging function is therefore associated with uncertainty for the provider. Specific log content is only provided for in Art. 12(3) for AI systems for real-time remote biometric identification. Will there be clarification?

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

If the high-risk AI system is embedded in a product that is subject to a harmonization requirement in Annex 1, Section A, the sectoral harmonization requirements must also always be observed in accordance with Art. 9 (2) AI Act. The provider must then comply fully with the applicable harmonization provisions, but may integrate the requirements set out in Articles 9-15 of the AI Act into existing procedures. This is to prevent double regulation. Recital 46, sentence 3 of the AI Act refers in this regard to the so-called Blue Guide on the implementation of EU product rules from 2022, according to which the specific implementation of the harmonization rules is at the discretion of the provider. According to Art. 11 (2) if a high-risk AI system is embedded in a product listed in Annex 1 Section A, only a single set of technical documentation needs to be produced, containing both the requirements of the AI act and the information required by those legal acts. Will there be clarification on how the interplay with existing harmonization legislation will work?

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

According to Art. 72, providers must also establish a system for monitoring the high-risk AI system after it has been placed on the market, which collects and analyses relevant data throughout the entire lifetime of the system. Is it true that a plan for this monitoring is part of the technical documentation?

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

If so, please elaborate which specific aspects require clarification regarding their interplay with other Union legislation and point to concrete provisions of specific other Union law.
3000 character(s) maximum
-

C. Obligations for deployers of high-risk AI systems

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

Yes, the implementation of the following obligations should be specified:

- Pursuant to Art. 26 (2) of the AI Act, the obligation to ensure, by means of technical and organizational measures, that they use the AI system in accordance with the accompanying instructions for use. What could those measures be?
- That operators must use relevant and representative input data (para. 4) and log the data processing (para. 6). How should be determined whether data is representative?
- The natural person exercising supervision on behalf of the operator should also have the necessary competence. Is that part of AI competence acc. to art. 4 AI Act?

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

-

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 model questionnaire in accordance with Article 27(5) and recital 96 (12) of the AI Act is likely to become defacto mandatory as soon as it is available, because Article 27(3) of the AI Act stipulates that the results of the fundamental rights impact assessment must be sent to the market surveillance authority together with the questionnaire in accordance with Art. 27 (5). Can alternatives be used, e.g., the Canadian government's "Algorithmic Impact Assessment" from 2019 and the European Law Institute's "ELI Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration" from 2022?

Algorithmic Impact Assessment tool, available at: https://www.canada.ca/en/government/system/digital-government/digitalgovernment-innovations/responsible-use-ai/algorithmic-impact-assessment.html;

Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration Available at: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Impact_Assessment_of_ADMSs_Used_by_Public_Administration.pdf.

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
-

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

How does the right interplay with the case law clarifying the right acc. to art. 13 (2f) 14 (2g), 15 (1h) and 22 GDPR and the relevant case law (e.g. ECJ 27 ruling from February 2025, Case C-203/22) in case of an exclusively automated decision-making?

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

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

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

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

distributor, importer, deployer or other third-party shall be considered to be a provider of a high-risk AI system and shall be subject to the obligations of the provider, in any of the following circumstances:

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

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

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

Question 44. Do you have any feedback on issues that need clarification as well as practical examples on the application of the concept of 'substantial modification' to a high-risk AI system.
3000 character(s) maximum

The AI Act does not regulate how to deal with excessive use by employees, i.e., when an employee uses an AI system on their own initiative for a high-risk application. Example: A school provides its teachers with an AI chatbot developed for the education sector, which, according to the school's usage policy, may only be used to create teaching content. However, a teacher decides on their own to also use the chatbot for grading and report card creation, which is a high-risk use according to Article 6(2) in conjunction with Annex 3 No. 3 of the AI Act.

Article 43(4) second sentence describes the circumstances under which the change does not qualify as a substantial modification: 'For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined by the provider at the

moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.'

Question 45. Do you have any feedback on issues that need clarification as well as practical example of pre-determined changes which should not be considered as a substantial modification within the meaning the Article 43(4) of the AI Act.
3000 character(s) maximum
-

E. Questions related to the value chain roles and obligations

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

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

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

Question 46. From your organisation's perspective, can you describe the current distribution of roles in the AI value chain, including the relationships between providers, suppliers, developers, and other stakeholders that your organisation interacts with?
3000 character(s) maximum

To our knowledge law firms primarily work with ready-made, off-the-shelf AI systems. These are often complex, integrated solutions where it is difficult to determine how the provider of the AI system has coordinated with the developer of the underlying GPAI (General Purpose AI) model—particularly regarding critical issues such as whether personal data was used during training (c.f. EDPB guidelines 28/2024). This lack of transparency can pose challenges because of the distribution of responsibilities along the AI value chain, e.g., the client (law firm) approaches the AI system provider to obtain details about the training data and risk scenarios. The AI system provider refers to the provider of the underlying GPAI model. Of course, the AI system provider should have sufficient information considering the guidelines and the Code of Practice on GPAI models, but this reflection of responsibility nevertheless describes the status quo quite well. In other words, it can be difficult to obtain truly reliable and precise information, e.g. on the question of which data was used to train an AI model and whether this data contained personal data. This causes difficulties assessing the compliance with data protection and ethical standards.

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

From our perspective, one of the most critical dependencies in the AI value chain lies in the relationship between AI system providers and the developers of general-purpose AI (GPAI) models. In many applications, the GPAI model constitutes the "secret sauce"—the core component that drives the system’s capabilities. As such, a significant portion of the transparency obligations under the AI Act hinges on how openly and responsibly these GPAI developers operate.

This dependency creates challenges, especially for SMEs and start-ups, who often rely on third party GPAI models integrated into off-the-shelf solutions. These smaller actors

typically lack the leverage or resources to audit or negotiate detailed transparency commitments from upstream providers. As a result, they may be held accountable for compliance obligations without having full visibility into the model's training data, risk mitigation strategies, or alignment with ethical and legal standards.

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

To ensure effective compliance with the AI Act, especially for providers of high-risk AI systems, it is essential that concrete and technically feasible guidance is made available in a timely manner. This guidance must take into account real-world limitations —such as the lack of explainability in many AI models—and avoid imposing theoretical or overly ambitious requirements that cannot be met in practice.
Support measures should include:

- Clear technical documentation standards that are achievable and reflect current capabilities.
- Modular compliance toolkits that can be adapted to different system architectures and risk profiles.
- Best practice collections, particularly around AI literacy and competence, which would help organisations build internal capacity and understand how others have successfully implemented compliance strategies.
- Templates for written agreements that clarify roles and responsibilities across the value chain, especially between GPAI developers and downstream providers.
- The use of soft language in the AI Act—such as "where technically feasible"—is helpful, but it must be backed by actionable examples and practical interpretations to avoid uncertainty.

Question 49. Please specify the challenges in the application of the value chain obligations in your organisation for compliance with the AI Act's obligations for high-risk

AI systems and the issues for which you need further clarification; please provide practical examples.

1500 character(s) maximum

-

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

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

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

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

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

(a) the intended purpose of the AI system;

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

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

(d) the extent to which the AI system acts autonomously and the possibility for a human to override a decision or recommendations that may lead to potential harm;

(e) the potential extent of such harm or such adverse impact, in particular in terms of its intensity and its ability to affect multiple persons or to disproportionately affect a particular group of persons;

(f) the extent to which the use of an AI system has already caused harm to health and safety, has had an adverse impact on fundamental rights or has given rise to significant concerns in relation to the likelihood of such harm or adverse impact, as demonstrated, for example, by reports or documented allegations submitted to national competent authorities or by other reports, as appropriate;

(g) the extent to which persons who are potentially harmed or suffer an adverse impact are dependent on the outcome produced with an AI system, in particular because for practical or legal reasons it is not reasonably possible to opt-out from that outcome;

(h) the extent to which there is an imbalance of power, or the persons who are potentially harmed or suffer an adverse impact are in a vulnerable position in relation to the deployer of an AI system, in particular due to status, authority, knowledge, economic or social circumstances, or age;

(i) the extent to which the outcome produced involving an AI system is easily corrigible or reversible, taking into account the technical solutions available to correct or reverse it, whereby outcomes having an adverse impact on health, safety or fundamental rights, shall not be considered to be easily corrigible or reversible;

(j) the magnitude and likelihood of benefit of the deployment of the AI system for individuals, groups, or society at large, including possible improvements in product safety;

(k) the extent to which existing Union law provides for:

- *effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages;*

– *effective measures to prevent or substantially minimise those risks.*

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

If so, please specify the concrete AI system that fulfils those criteria as well as evidence and justify why you consider that this system should be classified as high-risk.
3000 character(s) maximum
-

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

O Yes
X No

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

O Yes
X No

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

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

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

3000 character(s) maximum

-

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**?

O Yes

X No

Mailing List

Europe

European Commission

- Directorate-General Justice and Consumers
- Directorate-General Communication Networks, Content and Technology

European Parliament

- Committee on Internal Market and Consumer Protection
- Committee on Legal Affairs

Council of the European Union

Ständige Vertretung der Bundesrepublik Deutschland bei der EU

Justizreferenten der Landesvertretungen

Council of Bars and Law Societies of Europe (CCBE)