Below are the answers from the AI Standards Lab on the consultation at: https://digital-strategy.ec.europa.eu/en/news/commission-launches-public-consultation-high-risk-ai-systems . For context we also reproduce most of the text of the consultation form.

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

Fields marked with * are mandatory.

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

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

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

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

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

AI systems that classify as high-risk must be developed and designed to meet the requirements set out in Chapter III Section 2, in relation to data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security.

Providers of high-risk AI systems must ensure that their high-risk AI system is compliant with these requirements and must themselves comply with a number of obligations set out in Chapter III Section 3, notably the obligation to put in place a quality management system and ensure that the high-risk AI system

undergoes a conformity assessment prior to its being placed on the market or put into service. The AI Act also sets out obligations for deployers of high-risk AI systems, related to the correct use, human oversight, monitoring the operation of the high-risk AI system and, in certain cases, to transparency vis-à-vis affected persons.

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

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

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

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

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

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

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

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

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

> AI systems in each use case under the 8 areas referred to in Annex III.
> The filter mechanism of Article 6(3) AI Act allowing to exempt certain AI systems from being classified as high-risk under certain conditions.
> If pertinent: Need for clarification of the distinction between the classification as a high-risk AI system

and AI practices that are prohibited under Article 5 AI Act (and further specified in the Commission's guidelines on prohibited AI practices[3] from 3 February 2025) and interplay of the classification with other Union legislation.

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

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

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

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

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

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

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

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

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689). [2] Article 1(1) AI Act.

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

Sections 1-2

Note: for legibility we provide the answers submitted in a table, instead of using the format of the consultation form itself.

Questions		
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**	
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 Yes/No	No
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'?	We checked the first 6 boxes: A component of a product or of a system which is intended to monitor and detect situations which may lead to physical harm to people or property (e.g. AI system detecting abnormal system behaviour); A component of a product or of a system which is intended to monitor and detect the need to schedule maintenance and inspections, which, if not conducted, may lead to physical harm to people or property (e.g. AI system detecting whether parts of a product are worn and may need replacement or maintenance); A component of a product or of a system which is intended to prevent a physical harm to people or property (e.g. AI system preventing a start of a system if an abnormal behaviour is detected); A component of a product or of a system which is intended to control or limit possible physical harm to people or property (e.g. AI system controlling specific behaviour or function of a system and adjusting its function accordingly); A component of a product or of a system which is intended to mitigate consequences of possible physical harm to people or property (e.g. AI system that triggers action such as safe-stop if dangerous condition occurs); A component of a product or of a system which controls or supervises another system that performs a safety function (e.g. AI systems supervisor through sensors an operation in real time of a safety component that directly performs the safety function);

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?	((below we use the characters ** to separate responses to survey form fields on the same line in the form)) 2013/53/EU ** Example: AI software that is used to help decide whether to perform safety related (preventive) maintenance in a watercraft, no matter whether this preventive maintenance is related to the watercraft functions that need to undergo mandatory third party conformity assessment, no matter whether the software is built into the watercraft itself, and no matter whether the software is sold or marketed separately. ** The AI Act definition of safety component lacks any test if the component is related to the safety functions that need to undergo mandatory third party conformity assessment under annex I regulations. To avoid outcomes where many actors believe they are not in fact subject to the AI Act, it would be good if Commission guidance stresses this part of the classification logic of the AI Act. 2017/745 ** Example: A set of interconnected software modules that includes at least one AI software module, around which, according to common reverse engineering practices, a boundary could be drawn, with this set inside the boundary being declared a 'component' of the system, where this set also performs a safety function in a medical device. The AI Act definition of safety component lacks any guidance on WHAT party has the power to declare that something is a component which then becomes subject to e.g. article 47 obligations. There is no legal certainty now about the possibility that some set might be declared to be a 'component' by a national regulator even though the original system designer did not consider it to be a component. ** We would welcome guidance that removes legal uncertainty on what counts as a component, and on who decides on that classification. Our suggestion is that if a set of modules is packaged, marketed, or released as a potential system component for third parties to integrate, this set must be treated as a component under the AI Act. In other cases where no downstream third parties are involved, designating a set of modules as (not an) an AI Act component should be a free choice of the integrator.

4	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?	Please see, for a general remark on Q4, feedback item 1 under our answer to Q6
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?	2013/53/EU ** Example: A watercraft that has to undergo mandatory third party assessment under the Directive (e.g. it needs emissions testing), and which also has a built-in voice controlled entertainment system. The built-in voice controlled entertainment system uses AI modules as part of the voice control functionality, but note that the nature of the entertainment system has no safety implications. Many products are also AI systems according to article 3(1), and remain so when this article is clarified by the published guidance. Crucially, the AI Act logic in 3(1) and 6(1) does not contain any consideration on whether the AI related input/output functionality has any safety implications. ** See also https://datainnovation.org/2022/12/ai-acts-high-risk-obligations-unintentionally-apply-to-smartphones-and-iot-devices/ , but the fix proposed there, which would have to be done in the trilogue or earlier, is no longer applicable. We do not think it is possible to resolve this overreach issue, via guidance that gives some kind of tortured interpretation of the Act where the above example is not in fact a high-risk AI system. For our recommendation see the next box below. 2014/53/EU ** Example: Any modern smartphone, even if no AI based apps are installed. In all modern phones, built-in camera software uses AI based modules to recognise faces or other key elements of the picture and then determine camera focus. Many products are also AI systems according to article 3(1), and remain so when this article is clarified by the published guidance. Crucially, the AI Act logic in 3(1) and 6(1) does not contain any consideration on whether the AI related input/output functionality has any safety implications. ** We recommend that Guidance is written clarifying that the national regulators will only enforce the AI Act obligations for annex I products containing at least one AI sub-system that does fulfill a safety function, or alternatively that they define a very fast route to compliance with all Section 3 obligations for

		the various parties subject to them. We would also welcome future implementing acts or 'digital regulation simplification acts' that resolve the overreach.
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.	Feedback 1: Question 4 is somewhat strange: We consider that all 'components whose failure or malfunctioning may endanger the health and safety of persons or property' fulfill a safety function. If anything, the Commission should clarify if any 'components with a safety functions' exist which are not also members of the class of 'components whose failure or malfunctioning may endanger the health and safety of persons or property'. The preferred clarification is that some components offering safety will, if they fail, always cause the system to enter into or stay in a harmless operating mode: i.e. these safety components are designed to fail in a safe way, while still affecting safety when they are in operation. Feedback 2: As a party with people working in CEN-CENELEC JTC21, we foresee that the standards coming out of JTC21 will not have a lot to say about how makers of 'high-risk AI systems that are safety components in AI systems' will be able to comply with the obligations covered by the Standards Request – JTC21 is focussing on the obligations for full AI system providers, not safety component providers. So we would welcome guidance for AI system-as-a-safety-component providers, importers, and deployers to be written by the Commission.
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**	
2.A	**Questions in relation to biometrics**	
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.	
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?	
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,	We observe all the time that stakeholders somehow argue that in case of any overlap between the subject matter of two pieces of legislation, they only need to comply with the single regulation of their choosing that they like best. These

	please specify the practical provision in other Union or national law and where you see need for clarification of the interplay	arguments may come either from plain ignorance or wishful thinking, or they are made purely in bad faith by people who should know better, bad faith with the intent to preempt a more mature discussion of the law. We therefore would like to see the publication of very clear guidance confirming that the AI Act applies *in addition to* relevant annex I regulations, other Union law e.g. the GDPR and the general principle that companies and governments operating in Europe will always need to assess and manage the risks to fundamental rights of EU residents flowing from their operations. We also welcome specific guidance from the Commission on when complying with (some aspects of) one regulation also creates compliance with (some aspects of) another. A sample statement of such guidance: 'if you have already established that your AI system (of type T) complies with the GDPR (or some other piece of legislation relevant to type T), then you can validly conclude that it will also comply with AI Act articles A, however you still need to check if you will have to do extra work in light of articles B'.
2.B	**Questions in relation to critical infrastructure**	
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.	
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	See answers to Q3: these (New Legislative Framework/annex I/product related) concerns about ambiguities also apply to critical infrastructure.
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	
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	See answer to Q9.
2.C	**Questions in relation to education and vocational training (Annex III, point 3)**	
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.	
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.	
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	See answer to Q9.
2.D	**Questions related to employment, workers' management and access to self-employment**	
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.	
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?	
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	See answer to Q9.
2.E	**Questions in relation to the access to and enjoyment of essential private services and essential public services and benefits**	
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.	
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	
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	See answer to Q9.
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)**	
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.	
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?	
26	If you see the need for clarification of one of the various use-cases in Point 6 of Annex III to the AI Act and its interplay with other Union or national legislation, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay	
2.G	**Questions in relation to migration, asylum and border control management (Annex III, point 7)**	
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	
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.	
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?	
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	
2.H	**Questions in relation to administration of justice and democratic processes (Annex III, point 8)**	
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.	
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	

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

The phrase “promotional or sales materials and statements” needs to be clarified, especially when a statement is promotional. For example, suppose an educational chat-bot whose answers are constrained to educating children about languages. If a child asks the bot what its intended usage is and the bot responds “to educate children in the following three languages and more soon”, is

this the intended usage of the product? Is the phrase “more soon” assumed to be a promotional statement on behalf of the provider?

Also, there should be a hierarchy among the different documents or communications mediums that expresses the intended purpose of the system, in the case where the stated intended purpose may be contradictory depending on the medium of expression. We believe that technical documentation and explicit instructions of use should take precedence over other mediums to ground intended usage on measurable specifications. For example of a situation we want to avoid, a promotional material may claim a new use-case for the system when in fact the documentation has not described safe usage for the new use-case.

We emphasize that prioritization is meant to clarify the actual intended usage and not to absolve the provider of blame for producing confusing information. With the above, we are avoiding the case where a downstream user is accused of using a model different from its intended usage because of some contradictory statements on the part of the provider.

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

We do not agree with the observation made in the consultation form text, just above this question that article 6(1) and 6(2) define two categories with the intent that ‘The two categories are in principle intended not to overlap.’ We see no such intent by the legislator.

Indeed a 6(1) AI system-that-is-a-safety component is unlikely to not overlap with any system classified as high-risk under 6(2).

However, it is easy to image products getting a high-risk AI system classification under 6(1), e.g. certain machinery, medical devices, or products containing WiFi or Bluetooth (so that they get a high-risk classification via 6(1) and directive 2014/53/EU (radio equipment)), where the intended use of these products is to support one of the activities in annex III, e.g. ‘AI systems intended to be used to evaluate learning outcomes’. An example would be a digital toy used in an educational setting where interactions are AI based and where learning results can be downloaded out of the toy via WiFi. Another would be a medical diagnostic device used in a setup where medical students are trained and graded on the use of it.

We do not consider this classification of some systems as being high-risk AI via two routes, 6(1) and 6(2) both, to be problematic. Any guidance given should just clarify that this can happen. If there is any problem here worthy of note, it is the problem of the overreach described in our answer to Q5.

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*

As the JTC21 standards are expected to be published somewhat late, compared to the entry into force deadlines of the EU AI Act, it would be useful if the Commission publishes guidance on how ISO 42001 might be used as a vehicle to inform attempts to achieve compliance with the AI Act high-risk AI provider requirements. The AI Office has done an on-line webinar on this question in 2024 (https://ai-watch.ec.europa.eu/news/eu-ai-office-webinar-risk-management-ai-act-and-related-standards-2024-06-05_en), and the content from that webinar might be adapted into guidance. Guidance about existing standards beyond ISO 42001 would also be nice, but we note that ISO 42001 is the main one that is in play, in societal conversations we are aware of about getting IT departments more ready for the AI Act.

We repeat the following point 2 that we included under Q6: As a party with people working in CEN-CENELEC JTC21, we foresee that the standards coming out of JTC21 will not have a lot to say about how makers of 'high-risk AI systems that are safety components in AI systems' will be able to comply with the obligations covered by the Standards Request: JTC21 is focusing on the

obligations for full AI system providers, not safety component providers. So we would welcome guidance for AI system-as-a-safety-component providers, importers, and deployers to be written by the Commission.

While we cannot provide specific details about JTC21 internal status in this consultation input (because of confidentiality reasons), we note that it is well possible that the JTC21 standards will fall short of providing full explanations creating a presumption of conformity with all aspects of Articles 9-15, and also fall short of explaining how conformity with these articles is affected by the text of Article 8. We recommend that the Commission is not shy about creating guidance that fills gaps it is anticipating.

Guidance on how Article 12 (record keeping) interacts with the data minimisation and informed consent principles of the GDPR would be welcome, including guidance in the form of specific examples that cover use cases that are expected to occur frequently. We believe it is unlikely that the JTC21 standards will touch on this topic.

For more suggestions see our answer to Q36.

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

As they are expected to be 'horizontal' standards, the JTC21 standards may also fail to answer many questions about compliance that specific verticals may have, e.g. on the vertically specific methods that might be available to them to determine levels of acceptable risk (Article 9), and appropriate levels of accuracy and robustness (Article 15). We expect that in specific verticals, often there will be vertical-specific union legislation, legislation potentially supported by vertical-specific standards or guidance, that may define vertical-specific methods to determine levels of acceptable risk, and appropriate levels of accuracy and robustness. Guidance by the commission could remove legal uncertainties about the status of these methods with respect to requirements in the AI Act.

Some methods spanning multiple verticals may also be available, e.g. the GDPR and related guidance could be read as defining methods to achieve accessible outcomes with respect to the fundamental rights on privacy and the protection of personal data – article 9 requires that risks to those rights are assessed and mitigated. In general, the JTC21 standards might not go into much detail for specific fundamental rights, so guidance from the Commission with respect to specific fundamental rights, published as soon as possible, would be welcome and we do not expect it to be very duplicative of what will be in JTC21 standards.

See our answers to questions 50 and 53 for some input on fundamental rights, and/or additional aspects requiring clarification, our answer to Q9.

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;

80

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*

A clarification of Article 16 and 17 (and other articles referenced by them) for providers who are 'component' providers, providers of high-risk AI systems which are in fact safety components of other high-risk AI systems, would be welcome. For example, clarifying whether component providers would often have to do nothing in order to comply with the logging and accessibility requirements, under the assumption that the provider of the surrounding AI system will handle them.

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

(this seems to be something of a repeat of Q36, but then with different articles in mind? Could use it so that we have more character budget)

We have touched on this topic in several other answers to more specific questions, e.g. Q9, we will not repeat the text of these answers here

C. Obligations for deployers of high-risk AI systems

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

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

Take appropriate technical and organisational measures to ensure that AI systems are used in accordance with the instructions accompanying the AI systems;
Assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support;
Ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system;
Monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Article 72;
Keep the logs automatically generated by that high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system of at least six months.

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

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

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

If so, please elaborate on which specific questions you would seek further clarification. *3000 character(s) maximum*

Article 6(1) defined a class of high-risk AI systems which are in fact safety components of other high-risk AI systems. A machine vision AI module that is intended to be used as a safety component in an elevator might, for example, fit the description. It is somewhat unclear who the 'deployer' of that module would be, to which the Article 26 obligations apply. Is it a) the elevator maker integrating the safety component into their elevator, so the provider or the elevator, because they can be said to be 'using the component under their authority', to paraphrase the deployer definition 3(4), or b) or the deployer of the elevator, e.g. the building owner who paid for installing the elevator in their building, because they can likewise be said to be using the module, or c) both? Guidance to remove legal uncertainties would be welcome – maybe the correct answer is also different for different parts of article 26. Similar concerns apply to importers and distributors.

A clarification of how to sufficiently inform workers' representatives and the affected workers in the case that the high-risk AI system is a lift, a piece of machinery, or one any of the other products and systems in annex I, would be welcome.

In case that a high-risk AI system (e.g. a lift or machinery) is part of a building being rented by an employer as a workplace, it should be clarified who, if any, has the obligation to inform employees: the landlord or the tenant.

In many situations, for example, a subcontractor of an employer using a high-risk AI system to perform human resource activities for the employer, it may be unclear which party exactly counts as the 'deployer' of the system: the subcontractor or the employer. We recommend that guidance is given saying that in organizational situations where it is unclear exactly what organisational entity might be the deployer, these organizations can decide among themselves who assumes deployer responsibilities. Some guidance might however be given to inform such decisions. It should be clarified that to resolve any ambiguities, article 26(1) requires that the eventual deployer documents the decision that they are in fact the deployer. It should also be clarified that if the deployer position is not allocated at all, the market regulator may decide who counts as the deployer who might then be subject to fines, etc.

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

With respect to logging, the interaction with the GDPR could be clarified – see our answer to Q36 for more details.

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*

See the aspects mentioned in a provider context in our answer to Q36. These same aspects are relevant for deployers, and some of these aspects might be clarified by the AI Office providing one or more templates that deployers can fill out prior to their deployment of a high-risk AI system.
information may need to be gathered.

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

We note that the AI Act does not seek to be complementary with an absolute avoidance of overlap: while we would welcome guidance that helps parties to avoid duplicate assessment work, we would not like to see guidance that effectively relinquishes parties from certain assessment obligations just because there might sometimes be a possibility of overlap.

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*

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*

We would like the Commission to give guidance for the following example scenarios, where P is the provider that developed an AI system and placed it on the market, and E is an entity using the system without any modification:
1): P states that the system is not intended for annex III uses, E uses it in an area under Annex III.
2): P states that the system is intended for annex III uses, E uses it in an area under Annex III.
3): P is silent on intended uses of its system, E uses it in an area under Annex III.

In our interpretation of the Act, P would be considered the provider of the high-risk AI system in scenario 2, while E would be considered the provider of the high-risk AI system in scenario 1. Scenario 3 creates an ambiguity, so we would like to see guidance that P should avoid ever being in scenario 3 by writing clear documentation.

In further scenarios, E would make 'substantial' modifications to the system, which will make E the provider of the modified system, or 'non-substantial' ones so that P would remain the provider of the modified system. Currently, the meaning of 'substantial modification' is dependent on the interpretation of the term 'conformity assessment', which has been defined but has no practical examples of. Additional guidance should contain a working example for 'conformity assessment' as defined by Article 3 (20). We would also like to see guidance that disambiguates (or instructs how P could disambiguate in documentation) what 'foreseen and planned' (according to Article 3(23)) is, and therefore not a substantial modification. Do 'foreseen and planned' events refer to the scenarios handled in the initial conformity assessment?

Additional guidance should target open source providers, who are rightly concerned that they may end up being classified as high-risk AI system providers if somebody downstream uses their software in a high-risk AI use case as defined by annex III, or as a safety component in an annex I product or system. The concern about the legal consequences of such use is particularly acute for GPAI model and GPAI system providers, because these have such broad potential applications. Most open source licenses cannot restrict the allowed uses of the software or an included software component downstream: any such restriction would be met by broad accusations from the open source community that the license is no longer really open source.

The Commission guidance should make it clear that open source providers can address this concern by including in the documentation the information that the software has been developed and released with certain intended purposes in mind, and specifically that the intended purposes exclude any use in high-risk AI systems as defined by the EU AI Act. The guidance should confirm that, as long as this statement of intended purpose is truthful, making the statement will shield the open source provider from being classified as a high-risk AI system provider.

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

The Commission should remind providers who expect downstream modifications that they should write documentation that clearly specifies allowed and forbidden modifications. For those pre-determined modifications that are allowed, the provider

must be reminded that they are held liable if they specify an allowed modification that later causes or is a factor to a harm that was not considered in the system's conformity assessment. This is to avoid the situation where a provider unknowingly provides a loophole where a dangerous modification is made downstream that will be held liable for.

For example, in the case of a system that involves continual learning, the provider can specify what are the allowed range of statistical properties of the inputs to prevent data drift or when to trigger an assessment to verify if the provider's guidelines are still valid.

For many types of machine learning systems that continuously update a model, a few new adversarial inputs may significantly change the behavior of the model. Providers should clearly specify how they intend the system to be used if this type of vulnerability exists. For example, who will be responsible for ensuring the security and trustworthiness of the model inputs.

There is an ambiguity in the case of in-context learning on whether it is a type of continual learning. One can argue that while it does not modify the weights, the fact that it modifies the internal activations given new information imply it is a type of learning. Guidance should be provided in this case or encourage providers to handle this case in their terms of use.

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

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*

The AI Act is pretty clear about allocating legal responsibilities.

We now give further feedback related to a scenario where latest-generation LLM (GPAI) providers upstream in the value chain are all unwilling to provide sufficient information or support to downstream SMEs and startups, sufficient so that these SMEs and startups can actually use these models to build safe high-risk AI systems while they also fulfilling e.g. their article 9 obligations to assess and ensure acceptable risk from their systems. Such unwillingness may arise because of a combination of technical factors and independently made choices in business strategy – it would not necessarily be a violation of antitrust laws.

In such a scenario, all these SMEs and startups will simply have to conclude that they are in fact unable to legally build and release high-risk AI systems with any kind of latest-generation LLM technology inside. SMEs and startups who want to make trustworthy non-high-risk AI systems based on this technology would also be seriously impaired in their ambitions.

We would consider it entirely undesirable if, in this scenario, the Commission would start publishing guidance or implementing acts that would somehow allow SMEs and startups to release (potentially unsafe) high-risk AI systems with latest-generation LLM technology in the EU anyway.

Other tools of industrial policy (e.g. subsidies, promoting education, enforcing market competition law) should be used instead to try to achieve long-term technical and market outcomes that help SMEs and startups release innovative systems based on this technology, without endangering EU citizens and residents.

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 help providers of high-risk AI systems, specifically SMEs, we would like the Commission to publish guidance containing the following points.

Point 1: The level of information, capabilities, and mutual assistance needed across the value chain, in order for the AI system provider to comply with e.g. Article 9 obligations to assess and mitigate risk to an acceptable level, can vary considerably based on the use case and the AI

technology used. It is up to the AI system provider to make an assessment for their particular AI system, and obtain the required information and technical access as necessary. When they incorporate GPAI models into their high-risk system, AI system providers shall not blindly make the assumption that the GPAI documentation that GPAI model providers are minimally required to deliver under Article 53 will be sufficient for their particular needs.

Point 2. While it is not necessary that the high-risk AI provider to negotiate or write all contracts governing mutual behaviors and responsibilities among parties in the value chain use to create and maintain their AI system, it is definitely a responsibility of the provider to assess and ensure that sufficient contracts are in place in their value chain, such that they can fulfill all their Article 16 obligations. The provider also needs to check and ensure that the parties involved can be expected to implement their duties under these contracts in practice.

Point 3: If some party in the value chain makes a mistake or breaks their contract, then the AI Act makes the high-risk AI provider responsible for the possible consequences: the provider could potentially be fined under the AI Act, or required to take certain remedial actions, depending on the findings of the regulators. When it comes to taking remedial actions, it is wise for the provider to ensure beforehand that other parties in the value chain are bound by their contracts to help: if not then the only possible remedial action left might be to take the entire system off the market.

Point 4. If a GPAI-SR model is used in the high-risk AI system, then Article 55 may make model providers and/or modifiers of that GPAI-SR model, who may be organisations upstream from the high-risk AI system provider, co-responsible for ensuring that certain specific safety outcomes are achieved when the high-risk AI system is put on the market or onto service. This co-responsibility exists because the 'systemic risk' related safety outcomes required by Article 55 overlap to some extent with the 'health, safety, and fundamental rights' outcomes that need to be achieved by the high-risk AI system provider under Chapter 3 Section II (Articles 8-15). Co-responsibility means that both parties may potentially be fined for failing to uphold their responsibilities. Providers should be aware that when they themselves modify a GPAI-SR model, they can also become co-responsible for ensuring Article 55 outcomes.

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

Below, we discuss potential challenges for various organizations, not necessarily specifically relevant to our organization. Much of this has been described in our responses to the other questions in this consultation, but we summarize several key concerns here.

- In situations where an entity takes a GPAI with systemic risk and uses it as a component in their high-risk system, there may be overlap between the risk management performed by the model provider (Article 55) and the system provider (Article 9). It can be a challenge to understand which entity is liable for which of the potentially overlapping scope. We discuss this further in Q48.
- In situations where an entity places on the market a general-purpose AI system, they may inadvertently be classified as a high-risk AI system provider if another downstream entity uses it in areas classified under Annex III. It can be challenging to see what the best

course of action for the developer of the open-source AI system is, on how they can adhere to open source principles while not being inadvertently classified as a high-risk AI system provider, where Article 2(12) does not exempt them from obligations. We discuss this further in Q44.

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 fulfills those criteria as well as evidence and justify why you consider that this system should be classified as high-risk.

3000 character(s) maximum

We want to put some emphasis on the dangers of three different kinds of AI systems:

1 Highly addictive AI systems trained to maximize user engagement
Relevant to Area 5 (essential services) and Area 8 (democratic processes): The company character.ai claims to have an average of two hours/day of user engagement: https://qz.com/a-startup-founded-by-former-google-employees-claims-tha-1850919360

2 Persuasive or addictive AI systems, which may be used in communication or other platforms that are necessary to access essential services (Annex III, Area 5), such as messaging applications, which are not easy to avoid since many services depend on having access to such platforms. AI systems could influence public discourse and the democratic process (Annex III, Area 8) beyond electoral contexts, possibly by subliminal influence, sycophancy leading to political polarization. Current AI systems, as they become larger, get more persuasive: https://www.anthropic.com/news/measuring-model-persuasiveness; and there are many examples of AI systems deceiving humans in e.g. game environments: https://arxiv.org/abs/2308.14752

3 Agentic AI systems with little human oversight. Relevant to Area 2 (critical infrastructure), Area 5 (essential services) and Area 8 (democratic processes): Software engineering AI systems like https://mentat.ai/, Claude Code or Cascade by Windsurf already perform autonomous tasks, and we expect those to become longer-range.

We propose to add to area 3 (Education), the following:

(e) AI systems intended to be used to increase or preserve student engagement with an educational or training task, via methods including AI based or AI supported gamification, AI based determination of rewards or the timing of rewards, and AI based persuasive feedback.

We propose to add to area 4 ('Work') the following:

(c) AI systems intended to be used to increase or preserve worker engagement with a task or line of work, via methods including AI based or AI supported gamification, AI based determination of rewards or the timing of rewards, and AI based persuasive feedback.

For area 8 we propose 'AI systems intended to be used to increase political engagement, via methods including AI based or AI supported gamification and AI based persuasive feedback

We propose to add to area 5 (services) the following:

(3) AI systems intended to be used, without any high-risk alternative being available, by vulnerable persons to apply for, access, or enjoy essential private services, essential public services, or benefits, where these AI systems provide open-ended natural language interactions.

We propose to add to area 2 ("Critical infrastructure") the following:

(b) Agentic AI systems deployed in critical infrastructure, such as in smart energy grids, traffic and transportation, digital infrastructure (and especially the digital backbone), and water or gas systems, where these systems display long-range autonomy.

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

- Yes

No

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

3000 character(s) maximum

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

Yes

X No

Please justify why you consider that this system should no longer be classified as high-risk *3000 character(s) maximum*

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*

1. We are entering a technical phase where AI systems are increasingly capable of performing open-ended ‘automated R&D’ activities to create new software, followed by ‘automated marketing and sales’ activities for that software, with the whole chain being completely free of human oversight. Resulting AI systems could easily end up implementing dark patterns that are incompatible with human dignity by for example driving addiction loops. Also it is generally impossible to predict whether such systems will stray into banned or high-risk AI application areas as they interact with humans or their environment.

It will be tempting for companies to leverage the above full automation capabilities to flood the market with ‘slop’ AI products that will then overwhelm the regulator and lead to unsafe situations. We believe that this potential market failure is not sufficiently mitigated by the current form of the AI Act or other Union legislation.

We therefore propose to add to prohibited practices: ‘the use of an AI system to automatically create an artifact which is an AI system or software, with the resulting artifact being automatically made available on the market or put into service, automatically without any human oversight steps being present in the process.’

2. Regulatory gaps also exist for ‘narrow AI’ tools, special purpose AI models and AI systems that are powerful enough to raise concerns about their dual-use nature, because they could lower barriers to biological, chemical, or cyberweapons development, as considered in recital 110. Such tools are not covered by the high-risk AI classification, nor by the GPAI-with-systemic-risk rules. We also do not believe that current dual-use and export control law is scoped to sufficiently regulate the release of these tools. The problem is explored mor deeply in https://arxiv.org/pdf/2311.15936 . We do not expect that a full airtight solution is possible; going by section 4.4 of the paper we are mainly looking for a ban that has the effect of allocating responsibilities to parties.

So we suggest that article 5 is amended to ban the AI practice of ‘developing, bringing to market, or putting into service special-purpose AI models or AI systems in the areas of biology, biochemistry, or cybersecurity, where these models or systems can be expected to lower barriers to biological, chemical, or cyber weapons development, without putting appropriate access control and know-your-customer measures in place’. To avoid some ambiguity about banning a net-positive technology, the text should also say ‘this prohibition shall not apply to the release of quality checking tools that can be used to find security issues in software under development’.

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

- ( ) Yes
- (X) No

87

Please justify how other Union legislation already sufficiently addresses this AI practice *3000 character(s) maximum*

88