

*Contribution ID: 65ad54d7-6100-4d42-ba4d-dc7aa1665bc3

Date: 05/10/2025 11:18:04

Stakeholder consultation on transparency requirements for certain AI systems under Article 50 AI Act

Fields marked with * are mandatory.

General information

Disclaimer: The information in this consultation is provisional information of the AI Office for the purpose of consultation and does not prejudice the final decision that the Commission may take on the final guidelines or Code of Practice on transparency requirements under Article 50 AI Act. The responses to this consultation will provide input for the preparation of a Code of Practice and guidelines on the transparency requirements for certain AI systems under Article 50 AI Act.

This consultation is targeted to stakeholders of different categories, including, but not limited to, providers and deployers of interactive and generative AI models and systems, providers and deployers of biometric categorisation and emotion recognition systems, private and public sector organisations using such interactive and generative AI systems, as well as academia and research institutions, civil society organisations, governments, supervisory authorities and the general public.

The Artificial Intelligence Act ('the AI Act'), 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 [1]. It aims to promote innovation and the uptake of AI, while ensuring a high level of protection of health, safety and fundamental rights, including democracy and the rule of law.

Among various obligations, trustworthiness of AI systems is ensured by the AI Act through a set of requirements that aim to ensure transparency and to inform people when they are interacting with or being exposed to certain AI systems and their outputs. These transparency requirements are set out in Article 50 AI Act and will be applicable from 2 August 2026.

These transparency requirements aim to enable natural persons to recognise interaction with and content generated or manipulated by AI systems, thus reducing the risks of impersonation, deception or anthropomorphisation and fostering trust and integrity in the information ecosystem.

First, Article 50(1) AI Act obliges providers of AI systems that directly interact with natural persons to ensure that those persons are informed that they are interacting with an AI system and not a human, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use. Second, Article 50(2) AI Act aims to facilitate trustworthy detection and identification of AI-generated or manipulated content by requiring providers to mark such content in a machine-readable manner and enabling related detection mechanisms. Third, Article 50(3) AI Act requires deployers of emotion recognition or biometric categorisation AI systems to ensure that individuals exposed to these systems are informed about their operation. Fourth, Article 50(4) AI Act requires deployers of AI systems generating or manipulating deep fake content, or AI-generated or manipulated text publications intended to inform the public on matters of public interest to inform about the artificially generated or manipulated origin of the content, except in defined cases. Fifth, Article 50(5) AI Act imposes horizontal requirements on the above-mentioned transparency measures to ensure that the required information is provided to the natural persons concerned in a clear and distinguishable manner at the latest at the time of the first interaction or exposure, while respecting applicable accessibility requirements. Finally, Article 50(6) AI Act addresses the interaction between Article 50 and requirements applicable to high-risk AI systems under the AI Act and with other transparency obligations laid down in Union or national law for deployers of AI systems.

Pursuant to Article 96(1)(d) AI Act, the Commission shall issue guidelines on the practical implementation of transparency obligations laid down in Article 50 AI Act. Pursuant to Article 50(7) AI Act, the AI Office will encourage and facilitate the drawing up of codes of practice to facilitate the effective implementation of the obligations regarding the detection and labelling of artificially generated or manipulated content.

The purpose of the present targeted stakeholder consultation is to collect input from a wide range of stakeholders to inform the Commission guidelines and a Code of Practice on the detection and labelling of artificially generated or manipulated content. These topics will relate to specific practical examples on how the transparency requirements can be implemented, including issues that may require clarification whether they fall under the scope of Article 50 AI Act and under what conditions, information on state-of-the-art transparency and disclosure practices or other conceptual clarifications.

Since not all questions may be relevant for all stakeholders, respondents may reply only to the section(s) and the questions they deem relevant. Respondents are encouraged to provide specific, concise and concrete **explanations and concrete use cases**.

The consultation is available in **English only** and will be open for **5 weeks starting on 4 September until 9 October 2025, 23:59 CET**.

[1] Article 1(1) AI Act.

The questionnaire for this consultation is structured along 5 sections with several questions. Respondents may choose to provide answers only to some sections or only to some questions to which they wish to reply within the sections.

The sections of the survey are as follows:

Section 1. Questions in relation to Article 50(1) AI Act

This section includes questions on the concept of interactive AI systems, the applicable exception in case the direct interaction with persons could be considered obvious, their use for law enforcement activities and practical ways to design the systems in a way that individuals are notified about the interaction with AI systems.

Section 2. Questions in relation to Article 50(2) AI Act

This section includes questions related to the concept of synthetic content generating or manipulating AI systems, the applicable exceptions to marking AI-generated or manipulated content, their use for law enforcement activities, existing state-of-the-art technical solutions for marking and detecting AI-generated or manipulated content and the criteria for the assessment of marking techniques.

Section 3. Questions in relation to Article 50(3) AI Act.

This section includes questions on the concept of exposure to emotion recognition and biometric categorisation systems, their use for law enforcement activities and practical ways to inform natural persons of the operation of the system.

Section 4. Questions in relation to Article 50(4) AI Act

First, this section includes questions related to the concept of deep fake generating AI systems, the concept of evidently artistic, creative, satirical, fictional or analogous works or programmes, the system's use for law enforcement activities and best practices for disclosing the artificially generated or manipulated origin of deep fakes (including when part of artistic or creative works). Second, the section includes questions related to the concept of AI systems generating or manipulating text published for the purpose of informing the public on matters of public interest, the applicable exception in case the text is subject to human review or editorial control and a natural or legal person holds editorial responsibility, the exempted use for law enforcement activities and best practices for informing the public about the artificially generated or manipulated origin of such content.

Section 5. Other horizontal questions in relation to the implementation of Article 50 AI Act

This section covers a set of questions that relate to horizontal issues regarding Article 50 AI Act. First, it addresses the requirements from Article 50 (5) AI Act which apply horizontally when providing the information as required by paragraphs 1-4 of Article 50. Second, the section addresses Article 50(6) and the interplay between AI Act's requirements from Article 50(1)-(5) and other transparency obligations of the AI Act or other Union or national legislation. Finally, it also asks for recommendations and good practices for the Code of Practice.

All contributions to this consultation may be made publicly available. Therefore, please do not share any personal or confidential information in your contribution (Section 1-5). It is your responsibility to avoid including personal data in your contribution itself (any reference in your contribution itself that would reveal your identity, including together with the organisation you represent).

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 in the summary.

Introductory section - Information about the respondent

First name

James

Surname

Griffin

Email address

j.g.h.griffin@exeter.ac.uk

Do you represent an organisation (e.g., think tank or civil society/consumer organisation, provider or deployer of an AI system) or act in your personal capacity (e.g., independent expert or from a provider/deployer)?

- ☒ Organisation
☐ In a personal capacity

Name of the organisation

BILETA

Is your organisation headquartered in the EU?

- ☐ Yes
☒ No

Select the country where the organisation's headquarter is located

United Kingdom

If you selected "No" above and you are representing an organisation, do you have an office or other kind of representation in the EU?

- ☐ Yes, we have a subsidiary, branch office or similar in the EU
☐ Yes, other
☒ No

Select the size of the organisation

Medium (50-249 employees)

Which stakeholder category would you consider yourself in? If more than one category is applicable, please select the category that is best applicable in your situation / from the capacity you are responding.

- ☐ Deployer of an AI system
☐ Provider of a generative AI model
☐ Provider of an AI system
☐ Provider of transparency techniques
☐ Other operators (e.g. distributor, importer)
☐ Persons interacting with or exposed to AI systems and their outputs
☐ Rightholders
☐ Business association
☒ Academia
☐ Other independent expert or organisation with relevant expertise
☐ Civil society organisation
☐ Supervisory authority
☐ Other

In which sector do you operate?

- | | | |
|---|--|---|
| ☒ Information technology | ☐ Media | ☐ Energy |
| ☐ Public administration | ☐ Healthcare | ☐ Transport |
| ☐ Law enforcement | ☐ Employment | ☐ Telecommunications |
| ☐ Justice sector | ☒ Education and training | ☐ Retail |
| ☐ Legal services sector | ☐ Consumer goods or services | ☐ E-commerce |
| ☐ Civil society and non-profit organisations | ☐ Business services | ☐ Advertising |
| ☐ Security | ☐ Banking and finance | ☐ Other |
| ☐ Cultural and creative sector | ☐ Manufacturing | ☐ |

Please briefly describe the activities of your organisation or yourself.

1,300 character(s) maximum

Leading academic organisation in the UK and Ireland for IT and IP Law

Do you agree that we may publish your identity together with your contribution in the instance that all contributions are made publicly available?

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

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

- ☒ Yes
☐ No

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

- ☒ Yes
☐ No

For information on how we process your personal data, please see our privacy statement.

Privacy_statement_consultation_transparency.pdf

In which part(s) of the public consultation are you interested to contribute to? Multiple answers are possible. Please note that selecting a particular option will direct you to a set of questions specifically related to subject specified. If you do not select a specific option, you will be unable to respond to related questions.

- ☒ Section 1 - Questions in relation to Article 50(1) AI Act
☒ Section 2 - Questions in relation to Article 50(2) AI Act
☒ Section 3 - Questions in relation to Article 50(3) AI Act
☒ Section 4 - Questions in relation to Article 50(4) AI Act
☒ Section 5 - Other horizontal questions in relation to the implementation of Article 50 AI Act.

Section 1. Questions in relation to Article 50(1) AI Act

Article 50(1) AI Act targets providers of interactive AI systems, notably systems that are intended to interact directly with natural persons. Providers should ensure that such systems are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system.

Recital 132 AI Act clarifies that when implementing the transparency obligation for interactive AI systems, the characteristics of natural persons belonging to vulnerable groups due to their age or disability should be taken into account to the extent the AI system is intended to interact with those groups. Article 50(5) AI Act furthermore requires that the information shall be provided to the natural persons concerned in a clear and distinguishable manner at the latest at the time of the first interaction or exposure. In addition, such information shall conform to the applicable accessibility requirements. Regarding the latter, recital 132 confirms that such information and notifications should be provided in accessible formats for persons with disabilities.

Article 50(1) AI Act exempts providers from this obligation if the interaction with the AI system can be considered obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use.

Question 1. Please provide practical examples of AI systems that directly interact with natural persons, as well as examples for which there is doubt and you would seek clarification or consider out of scope.

For each AI system, determine whether the interaction with the AI system can be considered obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect. Consider in your answer how this interaction may be affected by the characteristics of natural persons belonging to vulnerable groups due to their age or disability.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

Name and description of the system	Is the AI system intended to interact directly with natural persons?	Motivate your answer	Specify if the interaction with the AI system can be considered obvious as specified in Article 50(1)?	Motivate your answer and provide practical example(s) of such circumstances and context of use
------------------------------------	--	----------------------	--	--

1	Name/description Deepfake video generator (e.g. face-swap app)	Select ☒ Yes	Explain 500 character(s) maximum It creates videos where a person's face/voice is replaced or altered. The output is synthetic because it does not reflect reality but is generated/manipulated media.	Select ☐ No	Explain 500 character(s) maximum Used for entertainment (parody videos). Not covered by exceptions. Transparency duties apply to avoid misleading the public.
2	Name/description AI image generator (e.g. DALL·E, Stable Diffusion)	Select ☒ Yes	Explain 500 character(s) maximum Generates images from text prompts. The content is synthetic as it is newly created and not captured directly from reality.	Select ☐ No	Explain 500 character(s) maximum General use (art, design). Not covered by Article 50(2). Requires labelling when presented as realistic
3	Name/description AI news text generator (e.g. automated financial news writer)	Select ☒ Yes	Explain 500 character(s) maximum Produces articles or summaries with human-like phrasing. Synthetic because the text is machine-generated, not authored by a journalist	Select ☐ No	Explain 500 character(s) maximum Used for rapid reporting. Not exempt: risk of misleading unless disclosed.
4	Name/description Law enforcement facial recognition (CCTV + AI matching system)	Select ☒ Yes	Explain 500 character(s) maximum The system processes and manipulates video/image data to compare against databases. Synthetic elements arise in "matches" produced.	Select ☒ Yes	Explain 500 character(s) maximum In the UK, use may be authorised under the Protection of Freedoms Act 2012 and common law policing powers, subject to human oversight, proportionality, and privacy safeguards.
5	Name/description Virtual assistant with synthetic voice (e.g. Alexa's voice responses)	Select ☒ Yes	Explain 500 character(s) maximum Produces synthetic audio responses in real time. Content is clearly synthetic as the "voice" is machine generated.	Select ☐ No	Explain 500 character(s) maximum Consumer use, not exempt. Must be obvious to users, though children may misinterpret it as human.
6	Name/description Fraud detection AI in banking	Select ☐ No	Explain 500 character(s) maximum Analyses data but does not generate synthetic content; outputs are alerts/flags.	Select ☒ Yes	Explain 500 character(s) maximum Falls under exemptions if authorised to detect/prevent crime (e.g. UK Proceeds of Crime Act 2002). Safeguards include regulatory oversight and proportionality tests.
7	Name/description 	Select ☐ Yes ☐ Not sure ☐ No	Explain 500 character(s) maximum 	Select ☐ Yes ☐ No ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum
8	Name/description 	Select ☐ Yes ☐ Not sure ☐ No	Explain 500 character(s) maximum 	Select ☐ Yes ☐ No ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum
9	Name/description 	Select ☐ Yes ☐ Not sure ☐ No	Explain 500 character(s) maximum 	Select ☐ Yes ☐ No ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum

	Name/description	Select	Explain	Select	Explain
		☐ Yes ☐ Not sure ☐ No	500 character(s) maximum	☐ Yes ☐ No ☐ Not sure ☐ Depends on the circumstances and context	500 character(s) maximum
10					

If you have more examples, please enter them in the section below, following the structure of question 1.

Furthermore, the transparency obligation under Article 50(1) AI Act does not apply if the interactive AI system is authorised by law to detect, prevent, investigate, or prosecute criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties unless those systems are available for the public to report a criminal offence.

Question 2. Please provide practical examples of AI systems that directly interact with natural persons and that can be authorised by law to detect, prevent, investigate, or prosecute criminal offences. For each system, provide the law that can authorise the use and describe appropriate safeguards for the rights and freedoms of third parties.

If you are aware of any AI systems available for the public to report criminal offences, please include them in your response.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

	Name and description of the system	Provide the law that can authorise the use to detect, prevent, investigate, or prosecute criminal offences and describe the appropriate safeguards	Is the AI system available for the public to report a criminal offence?	Motivate your answer
	Name/description	Describe 500 character(s) maximum	Select	Explain 500 character(s) maximum
1	AI facial recognition for law enforcement (used in public spaces to match suspects)	Authorised under Protection of Freedoms Act 2012 and common law policing powers. Safeguards: oversight by ICO, proportionality tests, judicial review.	☒ No	Used by police for detection, not by public. Citizens do not submit offences via this system.
2	Predictive policing system (AI analysing crime data to allocate patrols)	Use may be justified under Police and Criminal Evidence Act 1984. Safeguards: human oversight, local police governance, data protection law (GDPR/UK DPA 2018).	☒ No	Supports officers in decision-making but not available to the public for reporting crimes
3	Fraud detection AI in financial institutions	Authorised under Proceeds of Crime Act 2002 and Money Laundering Regulations 2017. Safeguards: reporting obligations, human review of suspicious activity.	☒ No	Used by banks to detect suspicious transactions, not a public-facing crime-reporting tool.
4	Online crime-reporting chatbot (e.g. UK police "report crime" portals enhanced by AI triage)	Authorised under general policing powers and Police Reform and Social Responsibility Act 2011. Safeguards: human follow-up by officers, secure handling of reports	☒ Yes	Members of the public can directly report offences via AI-assisted portals (e.g. cybercrime reporting websites).
5	Counter-terrorism monitoring system (AI scanning communications for threats)	Authorised under Investigatory Powers Act 2016. Safeguards: warrants, independent judicial commissioner oversight, proportionality	☒ No	Operates covertly; not available for public use.
6			☐ Yes ☐ No ☐ Not sure	
7			☐ Yes ☐ No ☐ Not sure	
8			☐ Yes ☐ No ☐ Not sure	

9	Name/description 	Describe 500 character(s) maximum 	Select ☐ Yes ☐ No ☐ Not sure	Explain 500 character(s) maximum
10	Name/description 	Describe 500 character(s) maximum 	Select ☐ Yes ☐ No ☐ Not sure	Explain 500 character(s) maximum

If you have more examples, please enter them in the section below, following the structure of question 2.

Question 3. If you are aware of any examples of notification techniques that can be employed with interactive AI systems, including embedded in their design, to duly inform natural persons that they are interacting with an AI system, please provide them in your response.

For each notification technique, determine whether the type and the content of the technique used for notifying a natural person is appropriate, including considering the characteristics of natural persons belonging to vulnerable groups due to their age or disability, the need for a clearly distinguishable and accessible manner and the timing of the notification.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

	Description of the notification technique	Determine whether the type and the content of the technique used for notifying a natural person is appropriate	Motivate your answer and, where available, provide practical examples with links and further information
1	Describe On-screen disclosure banner (e.g. "You are now chatting with an AI system")	Select Appropriate	Explain 500 character(s) maximum Clear, immediate, and accessible. Helps users distinguish AI from human operators. Widely used in customer service chatbots (e.g. HMRC chatbot explicitly labels itself as automated).
2	Describe Audio disclosure in synthetic voice (e.g. "I am an AI assistant")	Select Appropriate	Explain 500 character(s) maximum Accessible for visually impaired users. Works well for voice assistants like Amazon Alexa or Google Assistant, which already self-identify when activated.
3	Describe Icon or watermark displayed (e.g. small AI logo during video call when AI transcription is active)	Select Depends on the circumstances and context	Explain 500 character(s) maximum Effective if consistently applied, but not always clear to vulnerable groups. Example: Zoom live transcription displays "AI-generated captions" tag.
4	Describe Terms & conditions disclosure only (buried in documentation)	Select Not appropriate	Explain 500 character(s) maximum Not accessible or timely. Users often do not read long terms. This fails transparency standards under EU consumer law.
5	Describe Colour-coded frames or borders (e.g. red frame during AI surveillance interaction)	Select Appropriate	Explain 500 character(s) maximum Visually striking and accessible, though must be adapted for colour-blind users. Example: experimental AI-assisted interview tools highlight active analysis.
6	Describe Haptic feedback or vibration alert (on mobile reporting apps when AI system takes over)	Select Depends on the circumstances and context	Explain 500 character(s) maximum Supports users with limited vision/hearing. Example: crime-reporting apps could notify through vibration when AI categorises the report before human review.
7	Describe 	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum
8	Describe 	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum

9	Describe	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum
10	Describe	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum

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

Question 4. Are there aspects related to the scope or practical implementation of the transparency obligation for interactive AI systems under Article 50(1) for which you would seek further clarification?

- ☐ Yes
- ☒ No

Section 2. Questions in relation to Article 50(2) AI Act

Article 50(2) AI Act targets providers of AI systems, including general-purpose AI systems, capable of generating synthetic text, audio, image, and video content. Providers of such systems are required to employ technical solutions to ensure that the outputs of their systems are marked in a machine-readable format and enable detection that the content has been generated or manipulated by an AI system and not a human (see also recital 133).

AI systems that perform an assistive function for standard editing or that do not substantially alter the input data provided by the deployer or the semantics thereof are exempt from this obligation. Furthermore, Article 50(2) AI Act does not apply if the generative AI system is authorised by law to detect, prevent, investigate, or prosecute criminal offences.

Question 5. Please provide practical examples of AI systems that generate synthetic text, audio, image, or video content as well as examples of systems for which there is doubt and you would seek clarification or consider them out of scope.

If you are aware of any AI systems that may fall under one or more of the exceptions of Article 50(2), such as AI systems that perform an assistive function for standard editing or that do not substantially alter the input data or the semantics thereof, or systems that can be authorised by law for law enforcement purposes, please include them in your response.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

	Name and description of the system	Is the AI system generating or manipulating synthetic audio, image, video or text content?	Motivate your answer, including whether and why the content should be considered synthetic	Does the AI system fall within one or more of the exceptions of Article 50(2)?	Motivate your answer and provide practical examples(s). For the law enforcement exemption provide the law that can authorise the use and describe if it includes any appropriate safeguards
1	Name/description Computer Vision and GANs Diffusion Probabilistic Models (DPMs)	Select Yes	Explain 500 character(s) maximum Computer Vision and GANs are employed to produce a variety of ID cards, simulate genuine examples, introduce texture noise, and create composite scenarios to assist with fraud detection network training whilst improving accuracy of fraudulent activities. DPMs are utilised to generate and augment document data, particularly identity documents, that has the capability to integrate optical character recognition, layout understanding, face detection, and text layout generation.	Select ☐ Yes – the system performs primarily an assistive function for standard editing ☐ Yes – the system does not substantially alter the input data provided by the deployer or the semantics thereof ☐ Yes – the system is authorised by law to detect, prevent, investigate, or prosecute criminal offences ☐ No ☐ Not sure ☒ Depends on the circumstances and context	Explain 500 character(s) maximum Synthetic media maybe used to translate eyewitness descriptions into visual representations of potential suspects. This can aid law enforcement investigations by providing leads and helping to identify and locate potential suspects. Similarly synthetic media helps law enforcement capabilities through its roles in undercover operations and covert surveillance. By using synthetic media, undercover officers can modify their appearances to achieve their objectives.

2	Name/description	Select ☐ Yes ☐ No ☐ Not sure
---	---	---

5	Name/description	Select ☐ Yes ☐ No ☐ Not sure	Explain 500 character(s) maximum	Select ☐ Yes – the system performs primarily an assistive function for standard editing ☐ Yes – the system does not substantially alter the input data provided by the deployer or the semantics thereof ☐ Yes – the system is authorised by law to detect, prevent, investigate, or prosecute criminal offences ☐ No ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum
6	Name/description	Select ☐ Yes ☐ No ☐ Not sure	Explain 500 character(s) maximum	Select ☐ Yes – the system performs primarily an assistive function for standard editing ☐ Yes – the system does not substantially alter the input data provided by the deployer or the semantics thereof ☐ Yes – the system is authorised by law to detect, prevent, investigate, or prosecute criminal offences ☐ No ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum
7	Name/description	Select ☐ Yes ☐ No ☐ Not sure	Explain 500 character(s) maximum	Select ☐ Yes – the system performs primarily an assistive function for standard editing ☐ Yes – the system does not substantially alter the input data provided by the deployer or the semantics thereof ☐ Yes – the system is authorised by law to detect, prevent, investigate, or prosecute criminal offences ☐ No ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum

8	Name/description	Select ☐ Yes ☐ No ☐ Not sure
---	---	---

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

Article 50(2) AI Act specifies that the technical marking and detection solutions implemented by the provider should be effective, interoperable, robust and reliable as far as this is technically feasible taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art, as may be reflected in relevant technical standards.

Recital 133 AI Act gives examples of such marking techniques based on watermarks, metadata identifications, cryptographic methods for proving provenance and authenticity of content, logging methods, fingerprints, or a combination of such techniques. Furthermore, Recital 133 also clarifies that such techniques and methods can be implemented at the level of the AI system or at the level of the AI model, including general-purpose AI models generating content, thereby facilitating fulfilment of this obligation by the downstream provider of the AI system. Recital 133 also clarifies that the detection methods can be made accessible, as appropriate, to enable the public to effectively distinguish AI-generated content.

Question 6. Please provide examples of marking and detection solutions, including combinations of techniques, that can be employed to mark in a machine-readable format AI-generated or manipulated content and enable detection whether the content has been generated or manipulated by AI.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

	Technology's name	Type of solution, one or combination of multiple techniques	Application field per modality	Technology maturity	Link to the source (e.g. paper, journal)	Concise description of the technique and how it works, along with its specificities and potential limitations for modalities and costs of implementation if known
1	Technology Class Activation Mapping (CAM)	Select ☒ Watermarks ☐ Metadata identifications ☐ Cryptographic methods ☐ Logging methods ☐ Fingerprint ☐ Other	Select ☐ Text ☐ Image ☐ Audio ☐ Video ☒ Multi-modal	Select Wide market adoption	Insert link Interpol, 'Beyond Illusions: Unmasking the threat of synthetic media for law enforcement' (2024)	Description 500 character(s) maximum CAM offers a generalised approach to enhance interpretability of AI decisions.
2	Technology Detection Typology	Select ☐ Watermarks ☒ Metadata identifications ☒ Cryptographic methods ☐ Logging methods ☐ Fingerprint ☐ Other	Select ☐ Text ☐ Image ☐ Audio ☐ Video ☒ Multi-modal	Select Wide market adoption	Insert link Interpol, 'Beyond Illusions: Unmasking the threat of synthetic media for law enforcement' (2024)	Description 500 character(s) maximum Detection Typology helps identify synthetic media models which can provide insights into origins or creator identity, similar to tracing cybercriminal trends.
3	Technology Digital Fingerprinting	Select ☐ Watermarks ☐ Metadata identifications ☐ Cryptographic methods ☐ Logging methods ☒ Fingerprint ☐ Other	Select ☐ Text ☐ Image ☐ Audio ☐ Video ☒ Multi-modal	Select Wide market adoption	Insert link Interpol, 'Beyond Illusions: Unmasking the threat of synthetic media for law enforcement' (2024)	Description 500 character(s) maximum Digital Fingerprinting traces synthetic media to their originating GAN through unique digital fingerprints.
4	Technology Biometric analysis	Select ☐ Watermarks ☐ Metadata identifications ☐ Cryptographic methods ☐ Logging methods ☐ Fingerprint ☒ Other	Select ☐ Text ☐ Image ☐ Audio ☐ Video ☒ Multi-modal	Select Wide market adoption	Insert link Interpol, 'Beyond Illusions: Unmasking the threat of synthetic media for law enforcement' (2024)	Description 500 character(s) maximum Biometric analysis - despite potential for spoofing, when applied correctly, this method can be highly important for flagging synthetic media.
5	Technology	Select ☐ Watermarks ☐ Metadata identifications ☐ Cryptographic methods ☐ Logging methods ☐ Fingerprint ☐ Other	Select ☐ Text ☐ Image ☐ Audio ☐ Video ☐ Multi-modal	Select ☐ Early research ☐ Advanced research ☐ Testing phase ☐ Beta version ☐ Recently released on the market ☐ Limited market adoption ☐ Wide market adoption	Insert link	Description 500 character(s) maximum
6	Technology	Select ☐ Watermarks ☐ Metadata identifications ☐ Cryptographic methods ☐ Logging methods ☐ Fingerprint ☐ Other	Select ☐ Text ☐ Image ☐ Audio ☐ Video ☐ Multi-modal	Select ☐ Early research ☐ Advanced research ☐ Testing phase ☐ Beta version ☐ Recently released on the market ☐ Limited market adoption ☐ Wide market adoption	Insert link	Description 500 character(s) maximum

7	Technology	Select ☐ Watermarks ☐ Metadata identifications ☐ Cryptographic methods ☐ Logging methods ☐ Fingerprint ☐ Other	Select ☐ Text ☐ Image ☐ Audio ☐ Video ☐ Multi-modal	Select ☐ Early research ☐ Advanced research ☐ Testing phase ☐ Beta version ☐ Recently released on the market ☐ Limited market adoption ☐ Wide market adoption	Insert link	Description 500 character(s) maximum
8	Technology	Select ☐ Watermarks ☐ Metadata identifications ☐ Cryptographic methods ☐ Logging methods ☐ Fingerprint ☐ Other	Select ☐ Text ☐ Image ☐ Audio ☐ Video ☐ Multi-modal	Select ☐ Early research ☐ Advanced research ☐ Testing phase ☐ Beta version ☐ Recently released on the market ☐ Limited market adoption ☐ Wide market adoption	Insert link	Description 500 character(s) maximum
9	Technology	Select ☐ Watermarks ☐ Metadata identifications ☐ Cryptographic methods ☐ Logging methods ☐ Fingerprint ☐ Other	Select ☐ Text ☐ Image ☐ Audio ☐ Video ☐ Multi-modal	Select ☐ Early research ☐ Advanced research ☐ Testing phase ☐ Beta version ☐ Recently released on the market ☐ Limited market adoption ☐ Wide market adoption	Insert link	Description 500 character(s) maximum
10	Technology	Select ☐ Watermarks ☐ Metadata identifications ☐ Cryptographic methods ☐ Logging methods ☐ Fingerprint ☐ Other	Select ☐ Text ☐ Image ☐ Audio ☐ Video ☐ Multi-modal	Select ☐ Early research ☐ Advanced research ☐ Testing phase ☐ Beta version ☐ Recently released on the market ☐ Limited market adoption ☐ Wide market adoption	Insert link	Description 500 character(s) maximum

If you have more examples, please enter them in the section below, following the structure of question 6.

Question 7. For each of the solutions included in the previous question, please clarify whether there is relevant information that can help you competently assess their effectiveness, interoperability, robustness and reliability as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art. Please also assess to what extent the detection mechanisms are accessible and enable people exposed to the AI generated or manipulated content to identify its origin.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

	Technology's name	Assessment of effectiveness based on the grade below: - N/A (Not known/not sure) 1. Very low 2. Low 3. Moderate 4. High 5. Very high	Assessment of interoperability based on the grade below: - N/A (Not known/not sure) 1. Very low 2. Low 3. Moderate 4. High 5. Very high	Assessment of robustness based on the grade below: - N/A (Not known/not sure) 1. Very low 2. Low 3. Moderate 4. High 5. Very high	Assessment of reliability based on the grade below: - N/A (Not known/not sure) 1. Very low 2. Low 3. Moderate 4. High 5. Very high	Assessment of transparency and accessibility to people based on the grade below: - N/A (Not known/not sure) 1. Very low 2. Low 3. Moderate 4. High 5. Very high	Motivate your answer, including by providing sources, further information and evidence that supports the assessment
--	-------------------	---	--	--	---	--	---

[illegible]

7	Technology	Select ☐ Effective - 1 ☐ Effective - 2 ☐ Effective - 3 ☐ Effective- 4 ☐ Effective - 5 ☐ Effective - N/A
---	-----------------------------------	--

☐ Interoperable - 1

☐ Interoperable - 2

☐ Interoperable - 3

☐ Interoperable - 4

☐ Interoperable - 5

☐ Interoperable - N/A

☐ Robust - 1

☐ Robust - 2

☐ Robust - 3

☐ Robust - 4

☐ Robust - 5

☐ Robust - N/A

☐ Reliable - 1

☐ Reliable - 2

☐ Reliable - 3

☐ Reliable - 4

☐ Reliable - 5

☐ Reliable - N/A

☐ Transparent and accessible - 1

☐ Transparent and accessible - 2

☐ Transparent and accessible - 3

☐ Transparent and accessible - 4

☐ Transparent and accessible - 5

☐ Transparent and accessible - N/A

If you have more examples to assess, please enter them in the section below, following the structure of question 7.

They are all existing, those technologies, but none can accomplish what is aimed for in Article 50.

Question 8: Are you aware of technical standards or ongoing standardisation activities relevant in the context of the obligation for generative AI systems in Article 50(2) AI Act?

- ☒ No
☐ Yes

Question 9. Are there any other aspects related to the scope or the practical implementation of the transparency obligation for generative AI systems under Article 50(2) for which you would seek clarification?

- ☐ No
☒ Yes

Please, specify.

500 character(s) maximum

- a. Why would you mandate a technology that is functionally unproven.
b.How could you implement e.g. a watermarking mandate that is not surveillant

Section 3. Questions in relation to Article 50(3) AI Act

Article 50(3) AI Act requires deployers of emotion recognition systems or biometric categorisation systems to inform the natural persons exposed thereto of the operation of the system. This obligation does not apply if the system is permitted by law to detect, prevent or investigate criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, and in accordance with Union law.

The concepts of emotion recognition and biometric categorisation systems are defined by, respectively, Article 2(39) and (40) AI Act and have been clarified in the Commission Guidelines on Prohibited Artificial Intelligence Practices. (<https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>)

Article 50(5) AI Act furthermore requires that the information shall be provided to the natural persons concerned in a clear and distinguishable manner at the latest at the time of the first interaction or exposure. In addition, such information shall conform to the applicable accessibility requirements. Regarding the latter, recital 132 confirms that such information and notifications should be provided in accessible formats for persons with disabilities.

Question 10. Please provide practical examples of AI systems that may be considered emotion recognition and biometric categorisation systems.

If you are aware of any such systems that can be authorised by law to detect, prevent or investigate criminal offences, please include them in your response. For each of these systems, provide the law that can authorise their use and describe the appropriate safeguards for the rights and freedoms of third parties.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

	Name and description of the system	Is the AI system an emotion recognition system or a biometric categorisation system to which natural persons are exposed?	Motivate your answer	Is the AI system authorised by law to detect, prevent or investigate criminal offences?	If yes, provide the law that can authorise the use to detect, prevent, or investigate criminal offences and describe the appropriate safeguards
	<i>Name/description</i>	<i>Select</i>	<i>Explain</i> <i>500 character(s) maximum</i>	<i>Select</i>	<i>Describe</i> <i>500 character(s) maximum</i>
1	Amazon Rekognition https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html Amazon Rekognition https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html Amazon Rekognition https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html Amazon Rekognition https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html Amazon Rekognition https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html Amazon Rekognition	Yes, the system is emotion recognition system	This is an application programming interface (API) providing users with a facial analysis system for images and videos. It can estimate emotions such as 'Happy', 'Sad', 'Angry', 'Surprised', and others. Performs biometric categorisation by analysing faces to estimate an apparent age range (e.g., 25-34) and gender ('Male' or 'Female').	Not sure	It does contemplate law enforcement use
2	Microsoft Azure AI Vision	Yes, the system is emotion recognition system	500 character(s) maximum It can detect and analyse human faces. Its capabilities include the detection of a range of emotions, providing a confidence score for each (e.g., happiness: 98%, sadness: 2%).	Not sure	500 character(s) maximum
3	FaceReader by Noldus	Yes, the system is emotion recognition system	500 character(s) maximum A specialized software tool primarily used in academic and commercial research to automatically analyse facial expressions.	Not sure	500 character(s) maximum Is used worldwide at more than 1,000 universities, research institutes, and companies—from consumer and psychology research to usability studies. It could be used in crime prevention and detection.

4	Name/description 	Select ☐ Yes, the system is emotion recognition system ☐ Yes, the system is biometric categorisation system ☐ Not sure ☐ No	Explain 500 character(s) maximum 	Select ☐ Yes ☐ No ☐ Not sure	Describe 500 character(s) maximum
5	Name/description iMotions (platform)	Select Yes, the system is emotion recognition system	Explain 500 character(s) maximum A multimodal biometric research platform (facial expression, eye tracking, GSR, EEG) with a facial emotion-analysis	Select Not sure	Describe 500 character(s) maximum No evidence of being used in law enforcement directly but, it is used by academic researchers studying how police officers behave. In a peer-reviewed research context, the platform is used to analyse officers' physiological and emotional responses during training simulations.
6	Name/description Realeyes – "Emotion AI"	Select Yes, the system is emotion recognition system	Explain 500 character(s) maximum Facial coding for attention and emotion analysis	Select Not sure	Describe 500 character(s) maximum No evidence of working with law enforcement.
7	Name/description Clarifai	Select Yes, the system is biometric categorisation system	Explain 500 character(s) maximum The 'Demographics' model analyses faces in images or videos to predict apparent age, gender, and 'multicultural appearance'.	Select Yes	Describe 500 character(s) maximum Law enforcement solutions include: Computer vision technology for image analysis in investigations. Automated face recognition to help identify suspects. Behavioral analysis and pattern recognition by merging large quantities of data from disparate sources. Crowd detection to monitor crowd density, which can trigger real-time alerts for public safety. Privacy protection tools (redaction etc)
8	Name/description Live Facial Recognition (LFR) by the Metropolitan Police and South Wales Police	Select Yes, the system is emotion recognition system	Explain 500 character(s) maximum Scans faces in a live camera feed and compares them against a "watchlist" of individuals sought by the police.	Select Yes	Describe 500 character(s) maximum Combination of sources – many legally challenged. (i.e. R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058)
9	Name/description Smart Eye	Select Yes, the system is emotion recognition system	Explain 500 character(s) maximum Analyses facial expressions and voice tonality from video and audio streams to detect complex human emotions (e.g., joy, anger, surprise), cognitive states (e.g., drowsiness, distraction), and reactions. It is widely used in automotive safety systems and market research.	Select Not sure	Describe 500 character(s) maximum
10	Name/description 	Select ☐ Yes, the system is emotion recognition system ☐ Yes, the system is biometric categorisation system ☐ Not sure ☐ No	Explain 500 character(s) maximum 	Select ☐ Yes ☐ No ☐ Not sure	Describe 500 character(s) maximum

If you have more examples, please enter them in the section below, following the structure of question 10.

Question 11. If you are aware of any examples of transparency measures that can be employed with emotion recognition or biometric categorisation systems to duly inform natural persons exposed thereto of the operation of the system, please provide them in your response.

For each transparency measure, determine whether the type and the content of the measure used for informing the natural person of the operation of the system is appropriate, including as regards the need for a clearly distinguishable and accessible manner and the timing of the notification.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

	Description of the transparency measure	Determine whether the type and the content of the measure used for informing the natural person of the operation of the system is appropriate	Motivate your answer and, where available, provide practical examples with links and further information
1	Describe 500 character(s) maximum Amazon Rekognition	Select Not sure	Explain 500 character(s) maximum Provides guidance on best practice and use. Technical limitations are explained. For law enforcement use, they published a moratorium and subsequent guidelines.
2	Describe 500 character(s) maximum Microsoft Azure AI Vision	Select Not sure	Explain 500 character(s) maximum Transparency Notes are provided for all Microsoft services. Intended use and limitations are presented. Microsoft publishes research and documentation on the performance of its Face API across different demographic subgroups (e.g., by gender and skin tone) and provides guidance on how to mitigate fairness-related harms.
3	Describe 500 character(s) maximum Smart Eye	Select Not sure	Explain 500 character(s) maximum Operates on a principle of "opt-in" data, meaning they only analyse data from individuals who have given explicit consent. A strong public stance against using emotion AI for surveillance or lie detection, clearly defining the intended purpose of their technology for improving driver safety
4	Describe 500 character(s) maximum	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure	Explain 500 character(s) maximum
5	Describe 500 character(s) maximum	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure	Explain 500 character(s) maximum
6	Describe 500 character(s) maximum	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure	Explain 500 character(s) maximum
7	Describe 500 character(s) maximum	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure	Explain 500 character(s) maximum
8	Describe 500 character(s) maximum	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure	Explain 500 character(s) maximum
9	Describe 500 character(s) maximum	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure	Explain 500 character(s) maximum
10	Describe 500 character(s) maximum	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure	Explain 500 character(s) maximum

If you have more examples, please enter them in the section below, following the structure of question 11.

Question 12. Are there any other aspects related to the scope or the practical implementation of the transparency requirement for emotion recognition and biometric categorisation systems for which you would seek clarification?

- ☐ No
- ☒ Yes

Please, specify.

500 character(s) maximum

- Timeliness of the provision of the information. Should the point at which the information is provided be specified (i.e. before use? Only after informed consent obtained? Etc)
- Guidance as to the detail required in the information provided - technical data etc?
- Information post-use - the ability of the subject to correct or ask for data to be deleted?

Section 4 – Questions in relation to Article 50(4) AI Act

Article 50(4), subparagraph 1, AI Act requires deployers of AI systems generating or manipulating image, audio or video content constituting a deep fake to disclose that the content has been artificially generated or manipulated. The definition of a deep fake is provided in Article 3(60) AI Act, which defines 'deep fakes' as AI-generated or manipulated image, audio, or video content that resembles existing persons, objects, places, entities, or events and would falsely appear to a person as authentic or truthful.

If the deep fake content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme, the transparency requirement is limited to the disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work.

The transparency obligation in Article 50(4), subparagraph 1, does not apply if the AI system is authorised by law to detect, prevent, investigate, or prosecute criminal offences.

Question 13. Please provide practical examples of generative AI systems that produce 'deep fake' AI-generated or manipulated image, audio, or video content that resembles existing persons, objects, places, entities, or events and would falsely appear to a person as authentic or truthful.

If you are aware of any AI systems for which the deep fake content may be considered to form part of an evidently artistic, creative, satirical, fictional or analogous work or programme, please include them in your response.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

	Name and description of the system	Is the AI system generating or manipulating image, audio or video content constituting a deep fake?	Motivate your answer	Can the deep fake content form part of an evidently artistic, creative, satirical, fictional or analogous work or programme?	Motivate your answer and provide practical example(s)
	Name/description	Select	Explain 500 character(s) maximum	Select	Explain 500 character(s) maximum
1	DeepSwap / Nudify.Online / XPicture.ai	☒ Yes	They manipulate real photos to swap faces or remove clothing, producing false but realistic portrayals of people. Why? These outputs resemble real individuals and could easily appear authentic.	☒ No	use is typically deceptive or abusive.
2	Midjourney, Stable Diffusion, DALL·E	☐ Not sure	o Is it deepfake? Sometimes - when used to generate hyper-realistic portraits of non-existent people or mimic celebrities. o Why? Images can falsely appear as photographs of real persons/events.	☒ Yes	Yes - often used for art, satire, or fictional works.
3	Speechify, Play.ht, Resemble AI	☒ Yes	o Is it deepfake? Yes - they enable voice cloning from short audio samples. o Why? Outputs can convincingly imitate real people's voices for audiobooks, interactive bots, or scams.	☐ Depends on the circumstances and context	Sometimes - Resemble AI is also used in film/creative works, with watermarking safeguards.
4	Argil AI / AI Studios / Synthesia / HeyGen	☒ Yes	o Is it deepfake? Yes - they generate avatars or clones of real people for presentations, YouTube content, or video calls. o Why? The avatars closely resemble real people and can appear truthful.	☒ Yes	Yes - film production increasingly uses them to edit or recreate scenes.

5	Name/description Reface.ai, Avatarify, DeepFaceLive	Select ☒ Yes	Explain 500 character(s) maximum o Is it deepfake? Yes - they allow real-time face swapping in videos or calls. o Why? The manipulated content appears authentic in social media or streaming contexts.	Select Depends on the circumstances and context	Explain 500 character(s) maximum Sometimes - can be used for parody, satire, or entertainment
6	Name/description Vidnoz Face Swap / Deepfakes Web	Select ☒ Yes	Explain 500 character(s) maximum o Is it deepfake? Yes - they support synthetic avatars and face swapping at scale. o Why? They produce realistic videos without requiring technical skills.	Select ☒ No	Explain 500 character(s) maximum Mostly no - often marketed for personal/entertainment use but sometimes applied creatively.
7	Name/description 	Select ☐ Yes ☐ No ☐ Not sure	Explain 500 character(s) maximum 	Select ☐ Yes ☐ No ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum
8	Name/description 	Select ☐ Yes ☐ No ☐ Not sure	Explain 500 character(s) maximum 	Select ☐ Yes ☐ No ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum
9	Name/description 	Select ☐ Yes ☐ No ☐ Not sure	Explain 500 character(s) maximum 	Select ☐ Yes ☐ No ☐ Not sure ☐ Depends on the circumstances and context	Explain 500 character(s) maximum

If you have more examples, please enter them in the section below, following the structure of question 13.

Question 14. Please provide practical examples of AI-generated or manipulated content for which you would seek clarification regarding its classification as a 'deep fake'.
400 character(s) maximum

Clarification sought on whether these qualify as 'deep fakes': AI stock photos of non-existent people (Levi's virtual models); virtual influencers not impersonating real people (Noonouri); celebrity voice-cloning for satire (Sassy Justice); AI retouching (Photoshop Generative Fill); film de-aging (Indiana Jones); synthetic data for LLM training; AI music/virtual bands.

Question 15. If you are aware of any generative AI systems producing deep fakes that can be authorised by law to detect, prevent, investigate or prosecute criminal offences, please provide practical examples thereof in your response. For each of these systems, provide the law that can authorise the use and if it includes any appropriate safeguards for the rights and freedoms of third parties.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

	Name and description of the system	Is the AI system generating or manipulating image, audio or video content constituting a deep fake and can the system be authorised by law to detect, prevent, investigate, or prosecute criminal offences?	If yes, describe the law that can authorise the use of the AI system for law enforcement purposes and if it includes any appropriate safeguards
1	Name/description Deepfake video generator (e.g. faceswapping apps)	Select ☒ Yes	Describe 500 character(s) maximum Fraud Act 2006 (s.1, s.2) Malicious Communications Act 1988 Communications Act 2003 (s.127) Protection from Harassment Act 1997 Perverting the Course of Justice (common law) Copyright, Designs and Patents Act 1988

2	Name/description AI image generator (e.g. DALL·E, Stable Diffusion)	Select Yes	Describe 500 character(s) maximum Copyright, Designs and Patents Act 1988 Malicious Communications Act 1988 Communications Act 2003 (s.127) Obscene Publications Act 1959 Protection of Children Act 1978 / Sexual Offences Act 2003 (indecent images) Public Order Act 1986 (racial hatred) Terrorism Acts (terrorist publications) Data Protection Act 2018 / UK GDPR
3	Name/description AI grammar/spell checker (e.g. MS Word Editor, Grammarly)	Select No	Describe 500 character(s) maximum
4	Name/description AI video enhancement (e.g. frame interpolation, noise reduction)	Select Not sure	Describe 500 character(s) maximum
5	Name/description Police AI voice cloning for undercover ops	Select Yes	Describe 500 character(s) maximum Investigatory Powers Act 2016 Regulation of Investigatory Powers Act 2000 Data Protection Act 2018 (Part 3 - Law Enforcement Processing) Human Rights Act 1998 (Article 8 ECHR)

If you have more examples, please enter them in the section below, following the structure of question 15.

Recital 134 clarifies that deployers of AI systems generating deep fake content should clearly and distinguishably disclose that it has been artificially created or manipulated by labelling the output accordingly and disclosing its artificial origin. Regarding deep fake content that is part of evidently creative, satirical, artistic, fictional or analogous works or programmes, that recital clarifies that disclosure of the existence of such generated or manipulated deep fake content should occur in an appropriate manner that does not hamper the display or enjoyment of the work, including its normal exploitation and use, while maintaining the utility and quality of the work.

Article 50(5) AI Act furthermore requires that the information shall be provided to the natural persons concerned in a clear and distinguishable manner at the latest at the time of the first interaction or exposure. In addition, such information shall conform to the applicable accessibility requirements. Regarding the latter, recital 132 confirms that such information and notifications should be provided in accessible formats for persons with disabilities.

Question 16. If you are aware of any examples of disclosure practices that can be employed with deep fake content to duly disclose the artificially generated or manipulated origin of such content to natural persons exposed thereto, please provide them in your response.

For each disclosure practice, determine whether the type and the content of the disclosure practice is appropriate for clearly, distinguishably and accessibly informing natural persons about the artificially generated or manipulated origin of the content and the timing of the notification.

In cases where the disclosure practice is used on deep fake content that forms part of an evidently creative, satirical, artistic, fictional or analogous work or programme, determine whether the disclosure is done in an appropriate manner that does not hamper the display or enjoyment of the work.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

	Description of the disclosure practice	Specify to which type of deep fake it applies	Determine whether the type and the content of the disclosure practice is appropriate for clearly, distinguishably and accessibly informing natural persons	Motivate your answer and, where available, provide practical examples with links and further information	For deep fake content part of evidently creative satirical, artistic, fictional or analogous works, determine whether the disclosure does not hamper the display or enjoyment of the work	Motivate your answer and provide practical example(s)
--	--	---	--	--	---	---

1	Describe . Visible watermarks (image/video)	Select ☐ Audio ☒ Image ☒ Video ☐ Not sure	Select Appropriate	Explain 500 character(s) maximum - Practice: Embedding a visible symbol or label ("AI-generated") directly into the image/video. - Appropriateness: Appropriate - clear, immediate, and accessible to most users. - Timing: Shown at the point of exposure. - Creative exemption: If subtle and non-intrusive (e.g., corner label), it does not hamper artistic or satirical works.	Select ☐ Hampers the display or enjoyment ☐ Does not hamper the display or enjoyment ☐ Not sure ☐ Not applicable	500 character(s) maximum
2	Describe Metadata / tagging (all modalities)	Select ☒ Audio ☒ Image ☒ Video ☐ Not sure	Select Not sure	Explain 500 character(s) maximum - Practice: Attaching machine-readable tags indicating whether content is AI- or human-generated. - Appropriateness: Partially appropriate - useful for platforms and researchers, but not always visible to end-users unless platforms surface it. - Timing: Depends on platform implementation; risk of delayed disclosure. - Creative exemption: Neutral - invisible to most viewers, so no impact on enjoyment.	Select ☐ Hampers the display or enjoyment ☐ Does not hamper the display or enjoyment ☐ Not sure ☐ Not applicable	500 character(s) maximum
3	Describe Audio cues or disclaimers (audio/video)	Select ☒ Audio ☐ Image ☒ Video ☐ Not sure	Select Appropriate	Explain 500 character(s) maximum - Practice: Pre-roll audio messages ("This voice/video has been generated by AI"). - Appropriateness: Appropriate - direct and understandable. May need adaptation for accessibility (subtitles for hearing-impaired). - Timing: Best placed at start or at first exposure. - Creative exemption: Could disrupt immersion in artistic works unless kept brief and outside the main performance.	Select ☐ Hampers the display or enjoyment ☐ Does not hamper the display or enjoyment ☐ Not sure ☐ Not applicable	500 character(s) maximum

4	Describe Provenance/ fingerprinting tools (image/ audio/video)	Select ☒ Audio ☒ Image ☒ Video ☐ Not sure	Select Appropriate	Explain 500 character(s) maximum - Practice: Embedding cryptographic signatures or fingerprints traceable via blockchain or C2PA standards. - Appropriateness: Appropriate for long-term verification, but not always clear to lay users unless platforms translate signatures into simple labels. - Timing: Disclosure occurs when the content is displayed with verified provenance info. - Creative exemption: Does not hamper enjoyment - invisible to end- users unless surfaced.	Select ☐ Hampers the display or enjoyment ☐ Does not hamper the display or enjoyment ☐ Not sure ☐ Not applicable	500 character(s) maximum
5	Describe Platform-level labels (all modalities)	Select ☒ Audio ☒ Image ☒ Video ☐ Not sure	Select Appropriate	Explain 500 character(s) maximum - Practice: Platforms display "Generated by AI" badges or contextual disclaimers when users encounter synthetic content. - Appropriateness: Highly appropriate - visible, user- friendly, and scalable. - Timing: Should be displayed immediately at or before exposure. - Creative exemption: If shown outside the main artwork (e.g., in a description box), does not interfere with enjoyment.	Select ☐ Hampers the display or enjoyment ☐ Does not hamper the display or enjoyment ☐ Not sure ☐ Not applicable	500 character(s) maximum
6	Describe 	Select ☐ Audio ☐ Image ☐ Video ☐ Not sure	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure	Explain 500 character(s) maximum 	Select ☐ Hampers the display or enjoyment ☐ Does not hamper the display or enjoyment ☐ Not sure ☐ Not applicable	500 character(s) maximum
7	Describe 	Select ☐ Audio ☐ Image ☐ Video ☐ Not sure	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure	Explain 500 character(s) maximum 	Select ☐ Hampers the display or enjoyment ☐ Does not hamper the display or enjoyment ☐ Not sure ☐ Not applicable	500 character(s) maximum
8	Describe 	Select ☐ Audio ☐ Image ☐ Video ☐ Not sure	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure	Explain 500 character(s) maximum 	Select ☐ Hampers the display or enjoyment ☐ Does not hamper the display or enjoyment ☐ Not sure ☐ Not applicable	500 character(s) maximum

9	Describe 	Select ☐ Audio ☐ Image ☐ Video ☐ Not sure	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure	Explain 500 character(s) maximum 	Select ☐ Hampers the display or enjoyment ☐ Does not hamper the display or enjoyment ☐ Not sure ☐ Not applicable	500 character(s) maximum
10	Describe 	Select ☐ Audio ☐ Image ☐ Video ☐ Not sure	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure	Explain 500 character(s) maximum 	Select ☐ Hampers the display or enjoyment ☐ Does not hamper the display or enjoyment ☐ Not sure ☐ Not applicable	500 character(s) maximum

If you have more examples, please enter them in the section below, following the structure of question 16.

Article 50(4), subparagraph 2, AI Act requires deployers of AI systems generating or manipulating text published with the purpose of informing the public on matters of public interest to disclose that the content has been artificially generated or manipulated.

This obligation does not apply if the AI system is authorised by law to detect, prevent, investigate, or prosecute criminal offences or where the AI-generated content has undergone a process of human review or editorial control and a natural or legal person holds editorial responsibility for the publication of the content.

Question 17. Please provide practical examples of AI systems generating or manipulating text published with the purpose of informing the public on matters of public interest, including by providing examples of such publications.

If you are aware of any AI systems that may fall under one or more of the exceptions, such as AI systems for which the AI-generated or -manipulated text has undergone human review or editorial control and where a natural or legal person holds editorial responsibility for the publication of the content, or the use can be authorised by law to detect, prevent, investigate, or prosecute criminal offences, please include them in your response. If applicable, provide the law that can authorise the use for law enforcement purposes.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

	Name and description of the system	Is the AI system generating or manipulating text published with the purpose of informing the public on matters of public interest?	Motivate your answer, including as regards the type of the publication	Does the AI system fall within one or more of the exceptions of Article 50(4) subparagraph 2?	Motivate your answer and provide practical example(s). For the law enforcement exemptions, provide the law that can authorise the use for law enforcement purposes and if it includes any appropriate safeguards
1	Name/description Judicial or prosecutors' offices using AI to evaluate reliability of evidence	Select ☒ Yes	Explain 500 character(s) maximum For "evaluating reliability of evidence" in investigations.	Select ☒ Yes – the system is authorised by law to detect, prevent, investigate, or prosecute criminal offences	Explain 500 character(s) maximum
2	Name/description Police using AI analysers for predictive risk of reoffending	Select ☒ Yes	Explain 500 character(s) maximum Even though predictive risk is controversial, it's covered under "AI systems ... used by or on behalf of law enforcement ... to assess risk of a natural person re offending" in the Act.	Select ☒ Yes – human review or editorial control is guaranteed, and there is a person holding editorial responsibility for the publication	Explain 500 character(s) maximum
3	Name/description Media organisation using AI assisted writing/translation with human editors in control	Select ☒ Yes	Explain 500 character(s) maximum Where a news outlet uses AI to draft articles, which are ultimately edited by journalists and the editor, they may not have to clearly label each article, although the public interest requirement is still very relevant.	Select ☒ Yes – human review or editorial control is guaranteed, and there is a person holding editorial responsibility for the publication	Explain 500 character(s) maximum

4	<i>Name/description</i>	<i>Select</i> ☐ Yes ☐ No ☐ Not sure	<i>Explain</i> 500 character(s) maximum	<i>Select</i> ☐ Yes – human review or editorial control is guaranteed, and there is a person holding editorial responsibility for the publication ☐ Yes – the system is authorised by law to detect, prevent, investigate, or prosecute criminal offences ☐ No ☐ Not sure ☐ Depends on the circumstances and context	<i>Explain</i> 500 character(s) maximum
5	<i>Name/description</i>	<i>Select</i> ☐ Yes ☐ No ☐ Not sure	<i>Explain</i> 500 character(s) maximum	<i>Select</i> ☐ Yes – human review or editorial control is guaranteed, and there is a person holding editorial responsibility for the publication ☐ Yes – the system is authorised by law to detect, prevent, investigate, or prosecute criminal offences ☐ No ☐ Not sure ☐ Depends on the circumstances and context	<i>Explain</i> 500 character(s) maximum
6	<i>Name/description</i>	<i>Select</i> ☐ Yes ☐ No ☐ Not sure	<i>Explain</i> 500 character(s) maximum	<i>Select</i> ☐ Yes – human review or editorial control is guaranteed, and there is a person holding editorial responsibility for the publication ☐ Yes – the system is authorised by law to detect, prevent, investigate, or prosecute criminal offences ☐ No ☐ Not sure ☐ Depends on the circumstances and context	<i>Explain</i> 500 character(s) maximum
7	<i>Name/description</i>	<i>Select</i> ☐ Yes ☐ No ☐ Not sure	<i>Explain</i> 500 character(s) maximum	<i>Select</i> ☐ Yes – human review or editorial control is guaranteed, and there is a person holding editorial responsibility for the publication ☐ Yes – the system is authorised by law to detect, prevent, investigate, or prosecute criminal offences ☐ No ☐ Not sure ☐ Depends on the circumstances and context	<i>Explain</i> 500 character(s) maximum

8	Name/description	Select ☐ Yes ☐ No ☐ Not sure
---	---	---

If you have more examples, please enter them in the section below, following the structure of question 17.

Question 18. Please provide practical examples of AI-generated or manipulated textual content for which you would seek clarification regarding whether or not such content is published with the purpose of informing the public about matters of public interest, or whether or not such content has undergone human review or editorial control.

400 character(s) maximum

In cases of pandemics, calamities or e.g. info related to health it is helpful to know from who the information is coming and what the aim of the information is. Human review is in case of AI generated content is not really meaningful because humans normally lack the capability to critically assess this. In case of editorial control you can say the same but also that then the text becomes the resp

Question 19. If you are aware of any examples of disclosure practices that can be employed for AI-generated or manipulated text published with the purpose of informing the public on matters of public interest to duly disclose the artificially generated or manipulated origin of the publication to natural persons exposed thereto, please provide them in your response.

For each disclosure practice, determine whether the type and the content of the disclosure practice is appropriate for clearly, distinguishably and accessibly informing natural persons about the artificially generated or manipulated origin of the publication and the timing of the notification.

If needed, please use the horizontal scroll bar located at the bottom of the table in order to view all the columns.

	Description of the disclosure practice	Determine whether the type and the content of the disclosure practice is appropriate for clearly, distinguishably and accessibly informing natural persons	Motivate your answer and, where available, provide practical examples with links and further information
1	Description 1. Visible Labelling This entails placing a clear, upfront label at the beginning of content indicating whether and to what extent AI was involved (e.g., for research, editorial assistance, data analysis). As highlighted by Wittenberg et al visible content warnings alert users to AI origin, helping reduce confusion and over-trust in synthetic media . Furthermore, empirical research also shows that disclosure of source (AI vs human) reduces perceived accuracy of the content	Select Appropriate	Explain 500 character(s) maximum This method ensures visibility, immediate awareness, and accessibility. It helps reduce user confusion and over-trust in synthetic media. Research shows that source disclosure (AI vs human) reduces perceived accuracy and prompts critical reading¹. Example: The Guardian has used such labels in experimental AI-generated content.
2	Description AI Attribution in Byline	Select Not sure	Explain 500 character(s) maximum Justification: While the byline is a familiar way to indicate authorship, attributing authorship to AI is controversial. As Moffatt et al. argue, AI systems and large language models cannot take legal or ethical responsibility and arguably do not meet authorship standards .
3	Description Visual Iconography--- Description: Displaying a recognisable AI icon (e.g., a robot head) near titles or headlines.	Select Appropriate	Explain 500 character(s) maximum Justification: Icons are intuitive and work across languages and literacy levels. Platforms like YouTube and Meta have tested these. When paired with a tooltip, they enhance clarity
4	Description Watermarking and/or Pop-Up Notification Description: Embedding imperceptible watermarks or using pop-up alerts when users access AI-generated content.	Select Appropriate	Explain 500 character(s) maximum Justification: Pop-ups ensure real-time visibility. Watermarks can support verification and traceability. However, designing publicly detectable and robust watermarks is technically challenging and currently limited in practice .
5	Description Footer Disclosure Description: Including a note at the end of the article about AI involvement.	Select Not appropriate	Explain 500 character(s) maximum Justification: Footers are often missed, especially on mobile or in reposted content. This placement fails to meet clarity and accessibility standards.
6	Description	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure ☐ None	Explain 500 character(s) maximum
7	Description	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure ☐ None	Explain 500 character(s) maximum
8	Description	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure ☐ None	Explain 500 character(s) maximum
9	Description	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure ☐ None	Explain 500 character(s) maximum
10	Description	Select ☐ Appropriate ☐ Not appropriate ☐ Not sure ☐ None	Explain 500 character(s) maximum

If you have more examples, please enter them in the section below, following the structure of question 19.

Question 20. Are there any other aspects related to the scope or the practical implementation of the transparency requirement for deployers of AI systems that generate deep fakes and text publications on matters of public interest under Article 50(4) for which you would seek clarification?

- ☐ No
☒ Yes

Please, specify.

500 character(s) maximum

Clarity is needed on four points: (1) Editorial responsibility—what qualifies as human oversight and legal accountability, and how this varies by sector. (2) Public interest—what types of content count, including niche, social media, or internal communications. (3) Human review—whether light editing suffices or deeper evaluation is required. (4) Disclosure detail—whether a simple AI-use statement is enough or fuller explanation is needed, ideally via standard templates.

Section 5. Horizontal questions in relation to the implementation of Article 50 AI Act

Article 50(5) AI Act requires that the information to be provided under the various transparency requirements from Article 50 shall be provided to the natural persons concerned in a clear and distinguishable manner at the latest at the time of the first interaction or exposure. In addition, such information shall conform to the applicable accessibility requirements. Regarding the latter, recital 132 confirms that such information and notifications should be provided in accessible formats for persons with disabilities.

Question 21. Are there aspects related to the AI Act's horizontal requirements in Article 50(5), including their interplay with the requirements in Article 50(1)–(4), for which you would seek clarification?

- ☐ No
☒ Yes

Please, specify.

500 character(s) maximum

Article 50(5) enhances transparency but key issues need clarification: (1) Timing—what counts as “first interaction” in passive, active, or iterative use. (2) Clear and distinguishable—balance between detail and vagueness; model notices would help. (3) Accessibility—should standards follow EU law or new AI-specific rules? (4) Overlap—can one notice cover multiple Article 50 duties? (5) Responsibility—who ensures compliance and how is it enforced?

Article 50(6) AI Act states that paragraphs 1 to 4 of Article 50 shall not affect the requirements and obligations set out in Chapter III of the AI Act (i.e. the chapter containing the rules applicable to high-risk AI systems) and shall be without prejudice to other transparency obligations for deployers of AI systems under other Union or national law.

Question 22. Are there any further aspects related to the transparency obligations under Article 50(1)–(5) for which you would seek clarification regarding their interplay with other obligations in the AI Act?

- ☐ No
☒ Yes

Please, specify which aspects require clarification and point to specific provisions in the AI Act.

500 character(s) maximum

Transparency rules need clearer links to other AI Act duties: (1) Direct interactions—definition is vague beyond obvious chatbot cases; unclear for assistants or recommenders. (2) Reasonably well-informed user test—may be inconsistently applied and burdensome. (3) Undisclosed synthetic materials—no removal mechanism for harmful deepfakes or false political content. (4) Rights of notified persons—no complaint, redress, or substantive protections, leaving gaps for individuals.

Question 23. Are there any further aspects related to the transparency obligations under Article 50(1)–(5) for which you would seek clarification regarding their interplay with obligations in other Union or national legislation (e.g. data protection regulation such as Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, Regulation (EU) 2024/900 on the transparency and targeting of political advertising or Regulation (EU) 2022/2065 on a Single Market For Digital Services)?

- ☐ No
☒ Yes

Please, specify which specific aspects require clarification and point to specific provisions in Union or national legislation.

500 character(s) maximum

The AI Act overlaps with GDPR and DSA but leaves gaps. GDPR duties may clash with Art. 50 disclosure, e.g. in data retention, suggesting a right to opt out could help. Under the DSA, only “illegal material” must be removed; unmarked deepfakes or false content fall outside. Arts 50(2) and 50(4) create non-compliance but no removal duty. Platforms face unclear moderation roles, highlighting the need for clearer, harmonised rules.

Question 24. Are there any recommendations or good practices you would like to share as input for the Code of Practice to operationalise the implementation of the transparency obligations regarding interactive and generative AI systems?

- ☐ No
☒ Yes

Please, specify.

750 character(s) maximum

Key steps: (1) Label all synthetic/AI content under Art. 50(2) with watermarks or similar and disclose clearly per Art. 50(1). (2) Interpret “direct human interaction” broadly to ensure robust transparency and future compliance. (3) Provide substantive rights (e.g., opt-outs) for those notified of exposure. (4) Align policies with GDPR/DSA, managing undisclosed synthetic content proactively to reduce risk. (5) Clarify and strengthen provider duties, using the DSA as a model, so responsibility falls on platforms, not end-users.

Contact

Contact Form (/eusurvey/runner/contactform/ConsultationArt50AIATransparency)
