EUROPEAN
COMMISSION

Brussels, 20.5.2026
COM(2026) 234 final

# REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

# REPORT ADOPTED PURSUANT TO ARTICLE 112(1) OF REGULATION (EU) 2024/1689 ON THE NEED TO REVIEW THE LIST OF PROHIBITED AI PRACTICES AND OF HIGH-RISK AI SYSTEMS LISTED IN ANNEX III

# REPORT FROM THE EUROPEAN COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

# REPORT ADOPTED PURSUANT TO ARTICLE 112(1) OF REGULATION (EU) 2024/1689 ON THE NEED TO REVIEW THE LIST OF PROHIBITED AI PRACTICES AND OF HIGH-RISK AI SYSTEMS LISTED IN ANNEX III

## 1. Context and background information

(1) Regulation (EU) 2024/1689 of the European Parliament and the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain regulations ('the AI Act'[1]) entered into force on 1 August 2024. This regulation lays down a comprehensive legal framework for the regulation of artificial intelligence ('AI') in the Union that aims to promote innovation and uptake of AI, while ensuring a high level of protection for health, safety, and fundamental rights in the European Union (EU), including democracy and the rule of law.

(2) The AI Act follows a risk-based approach, classifying AI systems into four different risk categories: (i) unacceptable risk; (ii) high risk; (iii) transparency risk; and (iv) minimal to no risk. For the unacceptable risk category, the AI Act lists specific AI practices that are prohibited in the EU (Article 5 AI Act). AI systems are classified as high-risk in accordance with Article 6 AI Act, in conjunction with Annex I (list of Union harmonisation legislation) and Annex III AI Act. Annex III covers eight areas and lists concrete use cases for each area that have been assessed by the European Parliament and Council as posing a high risk of harm to health and safety of persons or to fundamental rights.

(3) The AI Act is designed as a flexible and future-proof legal instrument that allows certain rules to be adapted to the rapid pace of technological developments, as well as to the potential changes in the use of AI systems and to emerging risks. For this purpose, the AI Act foresees continuous monitoring and revision, ensuring that the rules remain relevant and effective. This applies even before specific provisions enter into application, such as the rules for high-risk AI systems.

(4) Article 112 AI Act provides a specific monitoring instrument to evaluate and review the AI Act. Under Article 112(1) AI Act, the Commission is tasked with assessing the need to amend the list of high-risk AI systems set out in Annex III and the list of prohibited AI practices laid down in Article 5 AI Act, once a year following the entry into force of the AI Act, and until the end of the period of the delegation of power laid down in Article 97 AI Act. The Commission must submit the findings of that assessment to the European Parliament and the Council.

(5) This is the first report adopted under that provision. Its objective is to assess whether there is a need to amend the list of use cases set out in Annex III and the list of prohibited AI practices laid down in Article 5 AI Act in order to ensure that the AI Act remains relevant and effective in the face of rapidly evolving AI technologies. The review of the list of areas

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024).

covered by Annex III falls outside the scope of this report, as the Commission is only required to conduct that review by 2 August 2028, in accordance with Article 112(2) AI Act.

(6) This report begins by presenting the methodology used in its preparation. It then applies that methodology to present an assessment of the possible need to review the list of high-risk use cases set out in Annex III and of the list of prohibited AI practices laid down in Article 5 AI Act.

(7) The assessment in this report is limited by the short time that has elapsed since the AI Act entered into force and its limited entry into application at the time of adoption of this report. Chapter II of the AI Act (Prohibited practices) entered into application on 2 February 2025. However, the rules on the enforcement of that chapter will only apply as from 2 August 2026 and the national competent authorities are still in the process of being designated. The obligations regarding high-risk AI systems listed in Annex III AI Act will apply as from 2 August 2026, which is under consideration of possible prolongation[2]. Moreover, while Commission guidelines on prohibited AI practices were published in February 2025[3], guidelines on the classification of high-risk AI systems are still under preparation. Thus, clarity as to certain concepts and the classification of specific AI use cases remain to be provided in those guidelines, and further developed through the practical application of Annex III AI Act and related provisions.

## 2. Methodology adopted for the review under Article 112(1) AI Act

(8) In accordance with Article 112(11) AI Act, to guide the evaluations and reviews referred to in Article 112(1), the AI Office should develop an objective and participative methodology for the evaluation of risk levels based on the criteria outlined in the relevant Articles and the inclusion of new systems in the list set out in Annex III, including the extension of existing area headings or the addition of new area headings in that Annex, and the list of prohibited practices set out in Article 5 AI Act.

(9) This section of the report presents the methodological approach developed by the AI Office to ensure compliance with this obligation in the preparation of this report. First, it provides an overview of the legal criteria for the review of the list of prohibited AI practices laid down in Article 5 AI Act and the list of high-risk AI systems set out in Annex III (Section 2.1. below). These legal criteria inform the further assessment of the need for a potential review, in particular with regard to concrete AI systems that may fall into those two categories. Second, the report outlines the participatory methods employed for evidence

[2] The Commission proposed in the Digital Omnibus on AI to align the timeline for the high-risk AI rules to the availability of standards and other support tools. Once the Commission confirms these are sufficiently available, the rules will start to apply after a 6-month transition period for high-risk AI systems in Annex III and in any case no later than 2 December 2027. This remains under negotiation and is subject to agreement between the European Parliament and the Council. For more details, see Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). {SWD(2025) 836 final}, Brussels, 19.11.2025, COM(2025) 836 final, 2025/0359 (COD).

[3] Available at: Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act. | Shaping Europe's digital future

collection and analysis, as well as the approach followed throughout the assessment process (Section 2.2 below).

### 2.1. Legal criteria for assessing the need to amend the list of prohibited AI practices laid down in Article 5 of the AI Act and the list of high-risk use cases set out in Annex III of the AI Act

(10) The assessment of the need to amend the list of prohibited AI practices under Article 5 AI Act, as well as the high-risk use cases set out in Annex III AI Act, is based on legal criteria. In the case of Annex III AI Act, these criteria are explicitly provided within the AI Act itself (Article 7 AI Act), while for Article 5 AI Act, they are inferred from the underlying rationale of the legislation.

#### 2.1.1. Criteria for reviewing the list of prohibitions in Article 5

(11) Article 5 AI Act prohibits the placing on the EU market, putting into service, or use of a limited number of AI systems for manipulative, exploitative, social control, surveillance and other practices, which by their inherent nature violate fundamental rights and EU values. Recital 28 AI Act clarifies that such practices are particularly harmful and abusive because they contradict EU values of respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights enshrined in the EU Charter of Fundamental Rights ('the Charter')[4]. Consequently, a review of Article 5 AI Act may be warranted whenever substantial evidence suggests that the current prohibitions do not adequately address new or emerging AI practices that effectively undermine EU values or fundamental rights enshrined in the Charter and qualify as especially harmful and abusive.

(12) Moreover, Article 5(8) AI Act provides that the AI Act does not affect existing prohibitions under other EU legislation. That provision emphasises the interplay of the AI Act with other legal frameworks, because of its horizontal nature[5]. Overall, the prohibitions in the AI Act primarily aim to focus on gaps that are not already addressed in other EU legislation and require AI-specific market-based rules. However, while other EU legal acts may apply in parallel, they inevitably approach issues from different angles, with different mechanisms of enforcement, and therefore might not sufficiently address the overall risks of certain unacceptable AI practices.

(13) As a result, the Commission's approach to reviewing the list of prohibited AI practices in Article 5 AI Act is to assess the need for review, subject to at least two cumulative conditions:

- there are new or emerging AI practices that undermine EU values or the rights and freedoms in the Charter which are not covered by the current list of prohibited practices in Article 5 AI Act; and

[4] Charter of Fundamental Rights of the European Union. OJ C 326, 26.10.2012, p. 391–407.
[5] See in this regard sections 2.8, 3.6, 4.4, 5.4, 6.4, 8.4 of the Guidelines on prohibited AI practices.

- regulatory gaps persist despite other applicable EU legislation, necessitating a review of the AI Act's prohibitions to ensure harmful AI practices are comprehensively covered.

(14) Article 5 may only be modified through a legislative amendment. Therefore, should the need to amend Article 5 AI Act be identified, the Commission will submit the findings of its assessment to the European Parliament and the Council and will consider the need to present a legislative proposal to that effect.

### 2.1.2. Criteria for reviewing the list of high-risk AI systems in Annex III

(15) Article 6 AI Act, in conjunction with Annex I and Annex III, addresses certain uses of AI systems that are classified as high-risk due to their significant risk of harm to the health and safety, or fundamental rights of persons. High-risk AI systems should only be placed on the market, put into service or used if they comply with certain mandatory requirements set out in the AI Act which aim to address those risks.

***Limitation of the review to use cases of high-risk AI systems listed in Annex III***

(16) The AI Act distinguishes between two categories of AI systems that are classified as 'high-risk' as set out in Article 6(1) and (2) AI Act. The first category is AI systems that are embedded as safety components in products or that themselves are products regulated by the EU harmonisation legislation listed in Annex I, which could have an adverse impact on health and safety of persons, and therefore classify as high-risk pursuant to Article 6(1) AI Act. The second category covers AI systems that in view of their intended purpose are considered to pose a significant risk to health, safety or fundamental rights and thus classify as high-risk according to Article 6(2) AI Act.

(17) Since Article 112(1) AI Act focuses on the possible need for a review of high-risk use cases listed in Annex III, the AI systems that are safety components of products, or which are themselves products, falling within the scope of certain EU harmonisation legislation listed in Annex I, are out of the scope of this report. The reference to high-risk AI systems in this report refers only to the stand-alone AI systems[6] falling within the pre-defined areas listed in Annex III.

***Criteria listed in Article 7 for amending high-risk AI systems use cases***

(18) Article 7 AI Act empowers the Commission, by means of delegated acts, to amend Annex III by adding, modifying or deleting use cases of high-risk AI systems to take account of the rapid pace of technological development, as well as the potential changes in the use of AI systems (see also Recital 52 and Recital 173 AI Act). This empowerment is subject to conditions set out in Article 7(1) to (3) AI Act.

(19) First, Article 7(1) AI Act establishes that the Commission may adopt delegated acts to add new use cases to Annex III or to modify the ones currently listed in that annex provided (i) the AI systems are intended to be used in one of the eight areas listed in Annex III and (ii) they pose a risk of harm equivalent to or greater than those already listed. This second

[6] High-risk AI systems other than those that are safety components of products, or that are themselves products classified as high-risk under Article 6(1).

condition sets a threshold of comparative risk assessment: a key condition for listing additional use cases of high-risk AI systems is that they must pose a risk to health and safety, or fundamental rights of persons equivalent to those already listed in Annex III. This ensures consistency and proportionality in the classification of high-risk AI systems.

(20) Article 7(2) outlines the criteria that must be considered when determining whether this threshold is met. These include inter alia the intended purpose of the AI system, the extent to which it is likely to be used, the nature of the data processed, the current and potential extent of harm. Recital 52 AI Act clarifies the rationale for these criteria by stating that it is appropriate to classify stand-alone AI systems as high-risk if, given their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence, and they are used in a number of specifically pre-defined areas specified in the AI Act. The Commission enjoys a certain margin of discretion in applying the criteria, provided that they are duly taken into account and considered fulfilled in the overall assessment.

(21) As a result, the threshold for amending the list in Annex III AI Act is not merely technological novelty or public concern, but a demonstrable and comparable risk posed by AI systems to health, safety, or fundamental rights, similar to that of the AI systems currently listed in Annex III.

***Removal of use cases of high-risk AI systems from Annex III***

(22) Article 7(3) of the AI Act specifies the criteria for the removal of high-risk AI systems from Annex III. For this purpose, the Commission must demonstrate that the use case no longer poses a high risk of harm, and that its removal would not decrease the overall level of protection of the health and safety, or fundamental rights under EU law.

### 2.2. Methodology for objective and participatory evidence collection and analysis used in this report and the procedures followed

(23) According to Article 112(11) AI Act, the AI Office is required to undertake to develop an objective and participative methodology when assessing the need for the review covered by the report. Furthermore, pursuant to Article 112(8) and Article 112(9) AI Act, the Commission may request information from the European Artificial Intelligence Board ('the AI Board'), the Member States and national competent authorities in the preparation of its report and it has to take into account the positions and findings of the AI Board, of the European Parliament, of the Council, and of other relevant bodies or sources in carrying out its review and evaluation.

(24) In line with these provisions, the Commission applied the following methodology for the preparation of this report:

- **Engagement with the AI Board and consultation with Member States and national competent authorities**

  The Commission engaged with the Member States and their respective national competent authorities in the process of designation, submitting relevant questions through the AI Board. Several subgroups of the AI Board were involved in the process.

- **Stakeholder consultation**
  A multi-stakeholder consultation was conducted to collect feedback and perspectives from a broad range of stakeholders, including industry representatives, academia, civil society, and the general public.
- **Empirical research: analysing AI incident databases**
  The Commission also analysed relevant AI incident databases to ensure a comprehensive and evidence-based approach based on empirical evidence for harms caused by AI systems.

(25) The sections below discuss in more detail the methodology for the objective and participatory collection and analysis of evidence used in this report. They detail the approaches that were taken to ensure that the information gathered is comprehensive and inclusive of diverse stakeholder perspectives, thereby supporting a transparent, evidence-based and well-founded assessment.

## 3. Analysis of the information collected

### 3.1. Analysis of the input from the consultation with Member States and the AI Board

(26) The AI Office consulted the Member States via the relevant sub-groups of the AI Board[7] and invited them to provide their input directly during the meetings or in writing.

#### 3.1.1. Position of the Member States on the need to review the list of prohibited practices in Article 5 AI Act

***General position***

(27) During the consultation of the relevant AI Board subgroup, the majority of the Member States present stated that, at this stage, they do not see a need to amend the list of prohibited AI practices laid down in Article 5 AI Act. In addition, nine Member States submitted written statements via e-mail, similarly confirming that there is no perceived necessity to amend that list. Comparable responses were also received from the two observers to the subgroup.

(28) The respondent Member States' representatives repeatedly noted that, since the provisions of the AI Act concerning the definition of AI systems and prohibited practices only began to apply on 2 February 2025, the rules on enforcement will become applicable on 2 August 2026, and enforcement mechanisms are not yet operational, the evaluation of practices that are particularly harmful and abusive and that contradict EU values and

[7] In particular, questions on the need for review of the list of use cases set out in Annex III and of the list of prohibited AI practices laid down in Article 5 of the AI Act were submitted to the Member States during the Fourth meeting of the AI Board Sub-group on prohibitions, which took place on 13 May 2025; the Third meeting of the AI Board Annex III Subgroup on high-risk AI systems which took place on 16 May 2025; the Third meeting of the AI Board Annex III Subgroup on Law Enforcement and Security which took place on 5 June 2025; and the Second meeting of the AI Board AI in Financial Services Subgroup held on 13 May 2025.

fundamental rights is only starting. Due to the limited time since Article 5 AI Act entered into application, there is currently a lack of practical experience and concrete use cases on the basis of which the effectiveness of the AI Act's prohibitions can be evaluated. It was therefore assessed that a more meaningful input can be provided once the relevant provisions have been in effect for a longer period. For the time being, the Member States noted that there is little concrete data or analysis available to justify a revision.

(29) In light of these considerations, the general position of the Member States was that any efforts aimed at reviewing or amending the list of prohibited practices would be more appropriate at a later stage, once sufficient implementation experience has been gathered.

***Issues flagged for further monitoring***

(30) One Member State suggested that it might be relevant to assess for possible inclusion in the list of prohibited AI practices **AI systems intended to develop or distribute malware** that could harm critical infrastructure, compromise databases, or create risks to fundamental rights. After analysing that suggestion, the Commission considered that the risks such a prohibition would address seemed sufficiently covered by various EU legislation[8], but flagged the issue for further monitoring and assessment.

### 3.1.2. Position of the Member States on the need to amend the high-risk use cases in Annex III AI Act

***General position***

(31) The need to amend the list of high-risk use cases in Annex III AI Act was discussed in several meetings of the AI Board subgroups. During those meetings, many Member States present stated that they currently do not see a need to amend Annex III. Moreover, seven Member States submitted written statements via e-mail, confirming that that they do not see any need to amend Annex III at this stage.

(32) Similar to the considerations set out above in relation to possible amendments to the list of prohibited AI practices in Article 5 AI Act, the respondent Member States repeatedly noted that they are still assessing the implications of the legislative framework on the current high-risk AI use cases listed in Annex III. The rules concerning high-risk AI systems are not yet applicable, and corresponding Commission guidelines on the classification of high-risk AI systems are still forthcoming. In view of these considerations, the Member States generally considered it premature to make amendments to the current list of high-risk use cases in Annex III AI Act.

***Issues flagged for further monitoring***

(33) Two Member States raised concerns about some specific AI use cases[9].

[8] E.g. EU cybersecurity legislation (from recent legal acts, see EU Cyber Solidarity Act), Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[9] As noted above, the Commission guidelines on high-risk AI systems will only be issued in 2026. As a result, assessments of concrete high-risk AI systems that were identified by the Member States, stakeholders or AI incidents' databases, are based on the AI Act text only. Due to limited guidance available at the current stage, concrete assessments were not always possible, and these cases have been flagged for further monitoring.

(34) One concern involved the regulation of **self-help (therapy) AI chatbots**[10] not falling under the Medical Device Regulation[11]. Self-help (therapy) AI chatbots are digital tools powered by AI and designed to provide users with mental health support and emotional guidance through conversational interfaces. Although presented as wellbeing tools, rather than as medical devices, they nevertheless affect users' mental health-related decisions and may process sensitive personal data. Consequently, there is a risk that the support and emotional guidance that such chatbots provide could negatively impact individuals' mental health. In light hereof, one Member State raised the question whether such systems ought to be classified as high-risk AI systems.

(35) After analysing this question, the Commission considers that when self-help chatbots fulfil the definition of a medical device they are subject to the strict requirements and controls under the Medical Device Regulation. Furthermore, the most harmful self-help AI chatbots potentially fall under the prohibitions laid down in Article 5(a) and (b) AI Act. As for classification of other self-help AI chatbots as high-risk, most of such AI systems could not be placed under one of the currently listed Annex III use cases, with some specific exceptions already covered by the use cases[12]. In addition, at least to a certain extent, the disclosure obligations set out in Article 50 AI Act may serve as a mitigation for addressing some of the risks associated with self-help AI chatbots, particularly those related to informed decision-making and the potential psychological impact of the interaction on individuals. The Commission will therefore assess how these provisions address the aforementioned risks in practice before considering any amendments to Annex III. The Commission nevertheless recognises that, at this stage, the use and potential risks associated with this type of AI system should be subject to close monitoring and the collection of further evidence in the coming years, especially once the provisions of the AI Act on high-risk AI systems start to apply.

(36) Another concern focused on **AI-driven personalised learning**. Current analysis based on the criteria listed in Article 7 AI Act lead the Commission to conclude that self-taught (independent) learning AI systems do not in most cases pose risks equivalent to or greater than those posed by AI systems listed in Annex III AI Act. In particular, there is limited empirical evidence of a high risk of harm in relation to such systems and no incidents involving those systems have been identified. A similar conclusion applies to AI systems that are used to develop personalised-content learning materials in the context of self-taught (independent) learning. Other use cases for AI-driven personalised learning are identified for further clarification in the forthcoming Commission guidelines on the classification of high-risk systems.

(37) Lastly, there was a suggestion from one Member State to extend Annex III AI Act to cover AI use cases for **granting authorisations by public authorities** in cases where a person applies for, for instance, a driver's license, firearms' and ammunition licenses, or a permit for handling chemical substances or for working with explosives. At this stage, there

[10] Similar concerns were also expressed by various stakeholders (see Section 3.2 below).

[11] If a chatbot is marketed as addressing specific mental health conditions or guiding users through therapeutic interventions, it would likely fall within the scope of the Medical Devices Regulation, since it can be considered as software intended for the treatment or alleviation of disease (Article 2(1) of the Medical Devices Regulation). Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. OJ L 117, 5.5.2017, pp. 1–175.

[12] For instance, AI self-help chatbots with functionalities of emotion recognition. AI systems intended to be used for emotion recognition are classified as high-risk pursuant to Annex III point 1(c).

is scant evidence that such use cases justify high-risk classification based on the criteria laid down in Article 7 AI Act. In light of this, the Commission considers that these risks merit further monitoring.

### 3.2. Analysis of the input from the stakeholder consultation

(38) From 6 June to 18 July 2025, the Commission organised a multi-stakeholder consultation[13] to gather input on implementing the AI Act's rules on high-risk AI systems. This consultation also included several questions with regard to the potential need for amendment of the list of high-risk use cases set out in Annex III AI Act and of the list of prohibited AI practices in Article 5 AI Act.

(39) In total, 547 responses were received from various stakeholders, including businesses, civil society organisations, academia, public institutions, and persons acting in private capacity[14].

#### 3.2.1. Stakeholders' views as to the need to review the list of prohibitions in Article 5 AI Act

(40) While a significant number of stakeholders considered the current list to be sufficient,[15] others proposed inclusion of additional prohibitions[16]. The majority of the respondent stakeholders did not advocate for the removal of any of the existing prohibitions.

(41) The suggestions of the stakeholders to include additional prohibitions were evaluated by the Commission by applying the methodology and the criteria outlined in Section 2.1.1 above. In particular, the Commission sought to identify, from the suggestions received, those practices that can be considered particularly harmful and abusive, contradicting EU values and fundamental rights, and not sufficiently addressed by existing EU legislation. This approach informed the assessment of whether proposed additions warranted inclusion in the list of prohibited AI practices or were more appropriately addressed through other regulatory mechanisms within the AI Act or possibly other EU legislation.

(42) A considerable number of suggestions were assessed as being sufficiently addressed by the existing provisions of the AI Act, either through the prohibitions set out in Article 5 AI Act, the classification of certain AI systems as high-risk under Annex III or Annex I AI Act, or the transparency requirements in Article 50 AI Act. Some of the suggestions, when

[13] Commission launches public consultation on high-risk AI systems | European e-Justice Portal.

[14] A total of 409 respondents indicated that they are representing an organisation. Among those, the largest group of respondents represented companies (150 responses), followed by associations (93 responses) and those respondents that selected 'other organisation' (81 responses). Civil society organisations or associations accounted for 56 responses, while research institutes (11 responses), universities (7 responses), think tanks (6 responses) and consumer organisations (5 responses) made out the minority of organisations. A total of 138 respondents indicated that they are acting in an individual capacity. Among the latter, the largest groups were those describing themselves as other independent experts or organisations with relevant expertise (35), providers of an AI system (34), and academia (28), while 14 selected "other" and 13 identified as deployers of an AI system. Some other respondents who marked that they are acting in a personal capacity indicated a link to a civil society organisation (7), other operators (3), a business association (2), or a supervisory authority (2).

[15] Both respondents who explicitly expressed this view in their answers and those who did not comment on the relevant question were understood to consider the current list of prohibitions sufficient.

[16] Slightly more than 10% of respondents.

assessed in light of the current stage of AI development and deployment, as well as taking into account the AI incidents registered, did not appear to meet the threshold for prohibition under the AI Act[17].

(43) The following concerns repeatedly expressed by the stakeholders were marked for further monitoring and evaluation of practice:

- In the area of biometrics, numerous suggestions focused on broadening the prohibition on the use of **emotion recognition technologies** in Article 5(1)(f) AI Act. Such use is prohibited when used in the areas of workplace and education institutions[18]. The use of such systems in all other areas are classified as high-risk AI systems under point 1 of Annex III AI Act. Moreover, Article 50(3) AI Act requires that deployers of emotion recognition systems inform the natural persons exposed thereto of the operation of the system. However, several respondents expressed concerns regarding their deployment in sensitive contexts, such as migration, and proposed that, rather than being subject to high-risk regulatory requirements, their use in these specific areas should be explicitly prohibited. Due to the lack of empirical evidence that classifying such systems as high-risk does not suffice to ensure fundamental rights are protected, the Commission does not see an immediate need to amend Article 5 AI Act in this respect. However, this area is flagged for further consideration.

- The question of classification of **AI systems enabling dark patterns and addictive design** was raised by several stakeholders. The current assessment of the Commission is that the most harmful instances of such practices are already covered by the existing prohibitions, in particular those listed in Article 5(a) and (b) AI Act. Moreover, those practices may be covered in other EU legislation such as the Unfair Commercial Practice Directive[19] and the Digital Services Act[20], regardless of whether they are AI-enabled. Nonetheless, such practices remain an important area of concern. It is considered important to closely monitor their evolution to assess whether existing EU legislation continues to provide adequate protection in particular where AI systems enable dark patterns and addictive design.

- Several stakeholders drew attention to AI systems **facilitating scams** and **generating nude images and other malicious and degrading deepfakes**. These harmful practices were also identified in the incident analysis and are further discussed in the Section 3.3.3. below.

[17] Such as, for instance, suggestions to prohibit AI systems used in the management of migration; voice clones in consumer-facing AI applications; or AI generated personas used for political messaging.

[18] Except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons.

[19] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'). OJ L 149, 11.6.2005, pp. 22–39.

[20] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). OJ L 277, 27.10.2022, pp. 1–102.

### 3.2.2. Stakeholders' views as to the need to amend the use cases in Annex III AI Act

(44) While a substantial number of stakeholders considered the existing list of high-risk use cases in Annex III AI Act to be adequate[21], others suggested adding new use cases to the area headings, extending current use cases, or questioned whether new area headings should not be added to the annex[22]. The majority of stakeholders did not support removing any of the current use cases from Annex III.

(45) A considerable number of suggestions were assessed by the Commission as being sufficiently addressed by the existing provisions of the AI Act[23]. The remaining suggestions to include additional use cases and area headings were evaluated, taking into account the criteria listed in Article 7 AI Act (see Section 2.1.2. above). Several proposed use cases were examined, but they were not deemed to pose a risk of harm equivalent to or greater than those already listed in Annex III AI Act[24]. Some of the concerns raised by stakeholders were assessed as likely already covered by the list of high-risk use cases in Annex III AI Act and noted to be further clarified in the guidelines on classification of high-risk AI systems that are currently being drafted by the Commission[25].

(46) The following concerns, repeatedly raised by stakeholders, have been identified by the Commission for ongoing monitoring and assessment in light of evolving practices:

- A significant number of suggestions concerned **point 5 of Annex III AI Act**. With regard to point 5(a), several stakeholders questioned lack of an explicit reference to AI systems used in public administration for managing access to social welfare benefits and social housing. Regarding point 5(b), stakeholders noted that AI systems used in tenant screening and private service (e.g., telecoms, utilities) eligibility are not clearly covered. As to point 5(c), concerns were expressed that the current high-risk use case is limited to life and health insurance, without a mention of other essential insurances (e.g., motor vehicle, professional liability, homeowners', disability insurance). There were also suggestions to extend point 5(d) to include AI systems that influence emergency response decisions affecting safety and rights (e.g. forced evacuation, lockdowns). While many of the suggestions were noted for further clarification in the forthcoming Commission guidelines on the classification of high-risk systems, the AI Office will closely monitor the deployment of AI systems in the area covered by point 5 of Annex III AI Act, and in particular in situations where no relevant high-risk use case exists in Annex III with regard to specific AI systems. Particular attention will be given to gathering empirical data on actual harms and identifying any regulatory gaps that may emerge, which could warrant amending or supplementing the list of high-risk use cases in point 5 of Annex III or the heading of the area more generally.

[21] Both respondents who explicitly expressed this view in their answers and those who did not comment on the relevant question were understood to consider the current list of high-risk AI use cases in Annex III as adequate.
[22] Around 20% of the respondents.
[23] Such as, for instance, suggestions to include specific biometric systems as high-risk (already covered under point 1 of Annex III).
[24] For instance, AI systems designed for online service providers to make sure that audiovisual media services of public interest are given suitable visibility; certain AI systems used in livestock farming.
[25] Such as concerns expressed with regard to specific AI systems used in employment and emotion recognition.

- Reiterating the concern expressed by one Member State (see Section 3.1. above), a recurring issue in the stakeholder consultation concerned **AI companions and AI mental support chatbots.** These AI systems were noted by stakeholders both in the context of the potential need to amend prohibited AI practices and the Annex III use cases. As noted above, if such systems exert subliminal, manipulative, or deceptive influence, or exploit vulnerabilities in a harmful way, they may fall under the prohibitions of Article 5(a) and (b) AI Act. When designed with elements for emotion recognition, they may be classified as high-risk under point 1(c) of Annex III AI Act. Transparency obligations also apply to ensure users are aware they are interacting with an AI chat box or subjected to emotion recognition or biometric categorisation systems. Additional safeguards are provided by the Digital Services Act[26] and the EU data protection law when applicable[27]. Nevertheless, in light of the increasing proliferation of AI companions and AI mental support chatbots, the Commission considers it important to closely monitor their development in the coming years to collect further evidence and assess whether the existing legislative framework remains adequate to address the risks they may pose.

- Some stakeholders suggested classifying **AI systems used in debt collection and enforcement** as high-risk, noting their growing use by energy, telecom, and financial providers. Such AI systems could potentially fall under the area heading of points 5 or 8 of Annex III AI Act. These systems will be further monitored by the Commission to see how intensively they are deployed and the harms that may arise, particularly in relation to vulnerable consumers.

- Several stakeholders proposed extending the scope of point 2 of Annex III AI Act, which concerns AI systems used in the area of **critical infrastructure**. They suggested that this area should cover not only AI systems functioning as safety components but also a broader range of systems integral to infrastructure reliability and continuity. Given these suggestions, further monitoring of AI systems in this area is needed to assess the intensity of deployment and harms to which such systems may give rise in practice.

### 3.3. Empirical research: analysing AI incident databases and other sources

[26] The Digital Services Act (DSA) prohibits manipulative interface design (dark patterns) and obliges providers of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) to identify, assess, and analyse any systemic risks stemming from the design or functioning of their services and its related systems, including algorithmic systems (Art. 34 DSA). Providers are also required to put in place reasonable, proportionate and effective mitigation measures, including testing and adapting their algorithmic systems (Art. 35 DSA). The DSA also requires providers of online platforms accessible to minors to put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security of minors, on their service (Art. 28.1 DSA). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). OJ L 277, 27.10.2022, pp. 1–102.

[27] Such as data processing principles and data subjects' rights established by the GDPR which would be applicable in connection with an AI system, e.g. either because personal data are used to develop an AI system or are input or output during the deployment. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, pp. 1–88.

(47) For the purposes of this report, information in relevant AI incidents databases was also consulted and analysed. This desk research was conducted to identify dangerous practices and past incidents caused by AI systems that could provide empirical evidence of risks to health, safety and fundamental rights that have materialised to inform the assessment of the review. While providing an additional source of mapping available data of harms and incidents caused by AI systems, the empirical research done in the next section has its inherent limitations considering that the incident databases analysed do not contain complete and verified information on all AI incidents. Many of the incidents are also global and not limited to Europe and detailed information for the proper categorisation of the incidents under the AI Act is not always available.

### 3.3.1. Databases and timeline

(48) The main database on which this desk research relied was the AI Incidents and Hazards Monitor (AIM)[28] of the Organisation for Economic Cooperation and Development (OECD). This database is a free and open-source project dedicated to indexing the history of harms or near harms that have materialised in the real world by the deployment of AI systems. The database is AI-driven and collects information about AI incidents from public sources (mostly AI incidents covered by the media). Another database the Commission consulted was the AI Risk Repository[29] of the Massachusetts Institute of Technology (MIT)[30]. This database was mainly analysed for devising the methodology of incident analysis.

(49) Due to the nature of the incidents databases, which publish only brief summaries of reported events, the analyses relying on these sources was to a certain extent limited. Concise descriptions do not consistently permit a precise evaluation of the incidents' characteristics, nor do they always enable accurate categorisation according to the methodological framework employed in this report, as specified in Section 2.1. above. Due to these limitations and constraints, this report refers to generalised quantifying terms (such as 'substantial part' or 'small part'), instead of providing precise proportions of incidents.

(50) To enable sufficient time for the analysis of the incidents, the time frame covered was limited to incidents reported from 1 January 2024 (after finalising the negotiations of the AI Act) to 31 May 2025. In total, 3 791 incidents were reported in the OECD AI Incidents and Hazards Monitor (AIM) during this period.

[28] Available at https://oecd.ai/en/incidents?search_terms=%5B%5D&and_condition=false&from_date=2014-01-01&to_date=2025-05-27&properties_config=%7B%22principles%22:%5B%5D,%22industries%22:%5B%5D,%22harm_types%22:%5B%5D,%22harm_levels%22:%5B%5D,%22harmed_entities%22:%5B%5D%7D&only_threats=false&order_by=date&num_results=20

[29] Available at https://airisk.mit.edu/

[30] This repository has three parts: (i) the AI Risk Database; (ii) the Causal Taxonomy of AI Risks (classifying how, when, and why AI risks occur); and the Domain Taxonomy of AI Risks (classifying AI risks into 7 domains (e.g., "Misinformation") and 24 subdomains (e.g., "False or misleading information").

### 3.3.2. Categorisation of reported incidents

(51) The first step of the analysis was the categorisation of all reported 3 791 incidents in six categories. These categories included:

1. incidents falling outside the scope of the AI Act;
2. incidents likely addressed by Annex I AI Act;
3. incidents likely covered by Article 50 AI Act;
4. incidents, which present hypothetical risks, without having caused any harm as of the time of reporting;
5. incidents that are (or may be) potentially addressed by Article 5 AI Act; and
6. incidents that are (or may be) potentially addressed by Annex III AI Act.

(52) Whilst categories 1-4 were collected for the purpose of better understanding the overall landscape of AI incidents, only incidents falling under categories 5 and 6 were further analysed according to the methodology employed for this report and the above-mentioned criteria (Section 2.1).

(53) The analysis demonstrated that almost half of all reported incidents in the relevant timespan fell outside the scope of the AI Act or were sufficiently covered by other EU instruments[31]. In addition, approximately 10% of the reported incidents were likely to be addressed by Annex I AI Act[32] and, thus, expected to be mitigated once these rules of the AI Act start to apply. Part of the reported incidents appeared to be addressed by Article 50 AI Act[33] and, therefore, can similarly be expected to be mitigated when this part of the AI Act starts to apply. Finally, some of the reported incidents were hypothetical incidents and thus excluded from further analysis, which was limited to actual damage that has or has been reasonably likely to occur due to the incident.

(54) Around 30% of reported incidents were identified by the Commission as relevant for a more detailed analysis. Approximately two thirds of these incidents either fell within the scope of Article 5 AI Act or were considered sufficiently relevant to warrant an assessment of whether they meet the criteria for inclusion in the list of prohibited AI practices (Section 2.1.1 above). The remainder, i.e. one third of the incidents identified for a more detailed analysis, were likely to fall under the high-risk area headings listed in Annex III AI Act[34]. However, it had to be verified whether those incidents were captured by the high-risk use cases currently listed in Annex III or, if not, whether they satisfy the criteria for inclusion in Annex III AI Act (criteria discussed in Section 2.1.2. above).

[31] These incidents generally concerned issues that are addressed by other relevant EU legislation, such as data privacy violations, which are regulated by the GDPR. Moreover, many of these incidents concerned copyright disputes, addressed by instruments such as the EU copyright law. Furthermore, many incidents resulted from areas which fall under the competences of the Member States, such as the use of AI in military applications.

[32] Such incidents concerned primarily damage arising from AI used in medical devices or self-driving vehicles.

[33] These incidents concern deepfakes lacking appropriate watermarks or other transparency measures.

[34] Most commonly, these incidents concerned the use of AI in biometric identification in law enforcement, border control management, essential services, educational and vocational institutions, as well as in the administration of justice and democratic processes

### 3.3.3. Assessment of incidents identified for further assessment

(55) The second step of the analysis involved assessing whether the 30% of reported incidents identified as relevant for a more detailed analysis were covered by the prohibitions in Article 5 or use cases listed in Annex III AI Act. If not, the subsequent assessment aimed to determine the potential need to amend these provisions by adding or removing relevant use cases.

*Incidents potentially falling under prohibited AI practices listed in Article 5 AI Act*

(56) Concerning incidents that could potentially fall under the prohibitions set out in Article 5 AI Act, part of incidents assessed appeared to be already covered by this provision[35]. Some of the incidents could neither be considered as covered by, nor excluded from the prohibitions of Article 5 AI Act, due to a lack of sufficient information to make a concrete assessment.

(57) However, the Commission identified a considerable number of incidents as potentially relating to the prohibited practices in Article 5 AI Act or as amounting to similar practices with particularly harmful and abusive effect which were not clearly covered by that provision. Those incidents were assessed according to the criteria discussed in Section 2.1.1. above. This analysis resulted in the following areas flagged by the Commission:

- AI systems intended or capable of generating **non-consensual nude and sexually explicit deepfakes**, depicting real people, including minors. The Commission has analysed whether the existing prohibitions of AI systems that deploy purposefully manipulative or deceptive techniques (Article 5(1)(a) AI Act), or exploit vulnerabilities due to age, disability, or a specific socio-economic situation (Article 5(1)(b)) causing significant harm could cover AI systems producing child sexual abuse material (CSAM) and non-consensual sexually explicit images. The Commission conclusion is that these practices are not covered by the Article 5(1)(a), nor Article 5(1)(b) of the AI Act, since they do not manipulate children and victims to engage them in harmful behaviour.

- AI systems intended for **facilitating scams and financial fraud** may potentially be covered by Article 5(1)(a) and (b) AI Act, if the conditions of these provisions are fulfilled, including the threshold of significant financial harm. This also necessarily requires a plausible causal link between the financial harm that has occurred or is reasonably likely to occur and the use of the AI system (e.g. a deepfake content impersonating a family member). The Commission considers it important to evaluate how the Member States' practice with regard to interpreting the requirement of significant financial harm evolves and how this will impact the coverage of such harmful and fraudulent AI practices by the prohibitions in Article 5 AI Act.

[35] Such incidents, which were potentially covered by Article 5 AI Act, spanned a range of topics, such as the real-time biometric identification or emotion recognition at the workplace.

*Incidents relating to high-risk use cases in Annex III*

(58) The analysis of incidents falling under the high-risk area headings of Annex III AI Act indicated that a substantial portion were already likely covered by the specific use cases listed in that annex[36]. In addition, some reported incidents were evaluated as not posing a level of risk of harm equivalent to that associated with the use cases already listed in Annex III AI Act[37]. A smaller proportion of incidents could not be conclusively categorised due to insufficient information.

(59) A considerable number of incidents were identified as falling within the area headings listed in Annex III AI Act; however, these were not clearly covered by the specific use cases currently set out therein. These incidents were assessed based on the criteria discussed in Section 2.1.2. above. The analysis led to the identification of the following areas flagged for further monitoring and data collection:

- A significant number of incidents involved **political disinformation campaigns**, which thematically fall under the area of administration of justice and democratic processes listed in point 8 of Annex III, but do not clearly appear in the use cases listed therein. These disinformation campaigns largely concerned deepfake videos and images, whose risks are already addressed to a certain extent by Article 50 AI Act. Moreover, part of such AI systems may be covered by the prohibitions in Article 5(1)(a) or (b) AI Act, provided all the conditions laid down therein are fulfilled. In addition, the Digital Services Act and the Regulation on the Transparency and Targeting of Political Advertising[38] address some of the issues linked to political disinformation. Additional measures and initiatives are foreseen in the recently adopted Communication on the European Democracy Shield[39]. The Commission will further assess and clarify in the forthcoming guidelines on classification of high-risk AI systems whether part of such AI practices could be classified as AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda.

[36] The incidents in the area of biometrics (point 1 of Annex III) often concerned AI systems used in surveillance cameras for remote facial recognition to identify suspects. In the area of employment, the identified incidents related to AI systems used to optimise the hiring and firing processes, such as the scanning of CVs, or the surveillance of employees on platforms used at work. In the area of access to and enjoyment of essential services, reported incidents often concerned the use of an AI based algorithm to flag people receiving housing benefits for fraud, leading to unnecessary investigations and rights violations. Concerning the area of law enforcement, relevant incidents include the use of AI to assess the risks faced by victims of domestic violence. When it came to border control management, relevant incidents related to the tracking and facial identification of migrants through cameras.

[37] Several incidents involved the use of AI cameras used to detect traffic offenses or to track crowd density and ensure safety during public events. Such applications of AI pertain to law enforcement; however, they do not appear to post risk of harm equivalent to, or greater than, the risk of harm or of adverse impact posed by other high-risk AI systems already listed under Annex II point 6. This is mainly due to the fact that they typically concern administrative offences, whose consequences are less intrusive than those linked to criminal offences or are used to ensure safety without direct effect on fundamental rights. Accordingly, such AI use cases do not currently require amendment to Annex III.

[38] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising. OJ L, 2024/900, 20.3.2024.

[39] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Democracy Shield: Empowering Strong and Resilient Democracies. Brussels, 12.11.2025. JOIN(2025) 791 final.

## Conclusion

(60) This report is prepared by the Commission and addressed to the European Parliament and the Council to fulfil the Commission's obligations as set out in the Article 112(1) AI Act. The findings set out in this report are submitted for the consideration of these institutions.

(61) Following the assessment performed applying the objective and participatory methodology for the review required under Article 112(1) AI Act, the Commission notes and further analyse a potential regulatory gap regarding AI systems generating CSAM and non-consensual intimate content, which are not prohibited by Article 5 AI Act. Since the provisions of the AI Act relating to prohibited AI practices entered into application on 2 February 2025 and the rules on enforcement are not yet applicable, the assessment of other AI practices that are particularly harmful and abusive and that contradict EU values and fundamental rights is still at an early stage, and there is a lack of practical experience with the prohibitions. A more substantive evaluation of the application of Article 5 AI Act will only become possible after the prohibitions have applied for at least a year and common challenges or regulatory gaps begin to emerge. Similarly, evaluating how the rules on high-risk AI systems function and identifying any potential gaps in the use of such systems that pose a high risk of harm to health and safety or fundamental rights will be facilitated once the Commission guidelines on the classification of high-risk AI systems are published and practical experience has been acquired. It is also expected that regulatory sandboxes established in accordance with the AI Act will serve as a mechanism for regulatory learnings and evidence collection that will help to identify possible regulatory gaps and challenges in interpretation. Based on the evidence collected and the assessment made in this report, the Commission has nevertheless flagged specific AI systems for monitoring and further analysis in subsequent reviews.

(62) In the coming years, market surveillance authorities supervising the application of the AI Act are encouraged to consider whether the prohibitions set out in Article 5 AI Act adequately address malicious and specific applications with a high potential for misuse, drawing from their practical supervisory and enforcement experience. Similarly, once the rules on high-risk AI systems start to apply and enforcement begins, particular attention should be given to AI systems that could fall under one of the areas listed in Annex III, but are not explicitly mentioned among the current list of high-risk use cases. These efforts will provide evidence-based input for future Commission reports adopted on the basis of Article 112(1) AI Act and assist the Commission in assessing whether the scope of Article 5 and Annex III AI Act remains adequate over time, thereby paving the way for a well-informed, objective, and evidence-based review and potential revision of the relevant provisions of the AI Act.

(63) In accordance with Article 112(1) AI Act, the list of prohibited AI practices laid down in Article 5 AI Act and the list of use cases of high-risk systems set out in Annex III AI Act are subject to annual review until the end of the period of the delegation of power laid down

in Article 97 AI Act. The next assessment of the Commission pursuant to Article 112 AI Act is therefore due in 2026 and, once finalised, the Commission will publish its findings in a report.

(64) To ensure a consistent and systematic collection of relevant data prior to the 2026 assessment, the Commission intends to coordinate ongoing monitoring efforts at national and EU level. For this purpose, the AI Office will cooperate with the AI Board and national competent authorities of the Member States, as well as consult, as appropriate, already established cooperation frameworks of national contact points in the relevant areas. Particular attention will be paid to the areas flagged for further monitoring and evidence collection identified in this report. However, monitoring of technological developments, as well as potential relevant changes in the use of AI systems, their impacts and emerging risks will also be performed.

(65) In assessing whether risks associated with AI are adequately addressed by existing EU legislation, once the enforcement of the AI Act has begun and practical experience has been gained, the analysis will examine how the AI Act interacts with and complements other EU frameworks in addressing risks to health, safety, and fundamental rights. Particular attention will be given to the coherence and practical interplay between the AI Act and instruments such as the Digital Services Act, the Data Governance Act, the Regulation on the Transparency and Targeting of Political Advertising, as well as the consumer protection and free movement of goods *acquis*. Such analysis should seek to establish the extent to which horizontal rules, sector-specific obligations, data governance mechanisms and product-related safeguards collectively mitigate the relevant risks, thereby informing whether further regulatory intervention is necessary.