

Public Consultation of the European Commission on High-Risk AI Systems: Use Cases

Answers by the Federation of German Consumer Organisations
(Verbraucherzentrale Bundesverband – vzbv) on high-risk AI use cases in
Annex III of the AI Act

18. Juli 2025

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

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

1. Answer in Row 1:

Name and description of the system

- **Chatbots in general and companionship bots inferring user emotions from biometric data** (if not prohibited under Art. 5 (1) a) and b))

Category of biometric system

- Emotion recognition (Annex III 1. c)),

The system is considered high-risk

- Yes, completely

Motivate your previous answer

The Commission guidelines on high-risk AI must clarify that all chatbots that infer users' emotional states or feelings from biometric data like voice or video interaction are considered as high-risk when they are not prohibited under Art. 5 (1) a) and b) of the AI-Act.

Many popular chatbots can interact with users in real time via voice or video. These bots increasingly have the capability to analyse biometric voice or video data from interactions with users and infer their emotional states in real time. The goal is to make the bots emotionally more appealing to users and increase user engagement. Such bots may also use biometric user data for biometric categorisation, according to sensitive or protected attributes (Annex III Point 1 (b)). There is a significant risk that chat bots cause psychological harm to users or induce users to actions leading to physical harm (e.g. by proposing dangerous "challenges" to minors). These risks are particularly pronounced in so-called companionship bots that are designed and marketed to build a personal relationship with users.

As the Commissions' guidelines on prohibited AI practices (C(2025) 884) on Art. 5 (1) a) and b) of the AI-Act states: The prohibition applies to chatbots that make "users emotionally dependent on the service incentivising addiction-like behaviour and potentially causing significant harms, such as suicidal behaviours and risks of harming other persons." Thus, the guidelines on high-risk AI must clarify that all chatbots that infer users' emotions based on biometric data, but fall short the threshold for prohibition under AI-Act Art. 5 (1) a) and b) of the AI Act (prohibited manipulation and exploitation of vulnerabilities) should be considered as high-risk AI systems falling under Annex III 1. c). Equivalently all chatbots engaging in biometric categorisation, according to sensitive or protected attributes, but fall short the threshold for prohibition under AI-Act Art. 5 (1) g) of the AI Act should be considered high-risk AI systems falling under Annex III 1. c).

The AI system performs profiling of natural person

- Unsure

The AI system meets at least one of the exception criteria of Article 6(3)

- No

Motivate your previous answer and specify any exception criteria that it meets, if applicable

Chatbots that interact with users and infer their emotional states or feelings based on biometric data like voice or video data for the purpose of appearing more appealing to users and increase user engagement do not fall within any of the exemptions in Art. 6(3): The analysis of user's feelings by chatbots is not preparatory or a narrow procedural task, nor does it serve to improve the result of a previously completed human activity. The analysis of users' biometric data to infer their emotions satisfies multiple criteria in Art. 7 (2) of the AI Act for classifying such systems as high-risk. Moreover, such chatbots are likely to perform profiling of natural person in relation to the users' personal preferences or interests. Equivalently this holds for chatbots engaging in biometric categorisation, according to sensitive or protected attributes and personality.

2. Answer in Row 2:

Name and description of the system

- **AI systems in call centres analysing the emotions of customers in real time through voice analysis** (if not prohibited under Art. 5 (1) a) and b))

Category of biometric system

- Emotion recognition (Annex III 1. c))

The system is considered high-risk

- Yes, completely

Motivate your previous answer

- More than 10% of German call centres use AI to analyse the emotions of customers in real time through their voice. Information on the callers emotional states may be used in order to guide call centre employees in real time or it could be processed by an AI systems that interacts with the callers directly via voice interface.

The emotions that such AI systems may detect in the customers voice may include current stress levels, anxiety, insecurity, happiness, sadness or anger. The guidelines on high-risk AI must consider such system as high-risk AI if the system is not prohibited under Art. 5 (1) a) of the AI Act for being used to exploit the vulnerability of customers and manipulating customer decisions, causing financial harm for example. The analysis of call center customers' voices to infer their emotions satisfies multiple criteria in Art. 7 (2) of the AI Act for classifying such AI systems as high-risk.

LINK: <https://www.tagesschau.de/investigativ/br-recherche/ki-callcenter-stimme-100.html>

The AI system performs profiling of natural person

- Partially

The AI system meets at least one of the exception criteria of Article 6(3)

- No

Motivate your previous answer and specify any exception criteria that it meets, if applicable

- The outcome of such real time evaluation of emotion may produce legal effects concerning the customer or similarly affect the customers by significantly. Analysing customer emotions in real can significantly influence the way customers are treated by call centre agents. It can influence the offers, prices and conditions customers receive as a result of their emotional states. Such AI systems may also contribute to profiling of known customers by evaluating, analysing or predicting customer emotions, preferences, and behaviour, reliability and significantly. In practice, customer emotion recognition systems in call centres are unlikely to merely fulfil preparatory tasks : a) When customers interact with an AI system acting as a call centre agent, the outcome of the emotion analysis will be taken as given by the AI system, thus it is not preparatory in nature. b) When customers interact with a human call centre agent, the agent will most likely follow the AI analysis and recommendation and not deviate from them (so-called 'automation bias').

3. Answer in Row 3:

Name and description of the system

- **Emotion recognition systems in Games detecting players emotional states and feelings on the basis of their biometric data**

Category of biometric system

- Emotion recognition (Annex III 1. c))

The system is considered high-risk

- Yes, completely

Motivate your previous answer

- AI systems embedded in video games may collect biometric data from players through, sensors, cameras, gaming googles, keyboard strokes or mouse/game controller data. Such biometric data may be used to infer emotional states of players such as excitement, anxiety, frustration, happiness and use such data to for example adjust the difficulty of the game to 'improve user experience' or personally target users by displaying/offering loot boxes or other in-game purchases. The guidelines on high-risk AI must classify such emotions analysis systems as high-risk AI if they do fall under the prohibitions of Art. 5 (1) a) or Art. 5 (1) b) of the AI Act.

The AI system performs profiling of natural person

- Yes

The AI system meets at least one of the exception criteria of Article 6(3)

- No

Motivate your previous answer and specify any exception criteria that it meets, if applicable

- In cases where such AI systems influence the display of loot boxes or in-game purchases to players, they may engage in profiling if they analyse players emotions or feelings to predict personal preferences or interests, behaviour, and can have legal implications, e.g. by influencing prices and encouraging players to spend money on loot boxes or in-game purchases.

Emotion recognition systems in games do not meet any of the exception criteria of Article 6(3). The analysis of user's feelings by games is not preparatory or narrow procedural task, nor does it serve to improve the result of a previously completed human activity.

4. Answer in Row 4:

Name and description of the system

- **Biometrics for age assessment of minors**

Category of biometric system

- *Biometric categorisation (Point 1(b))*

The system is considered high-risk

- Yes

Motivate your previous answer

- AI systems used for online age verification increasingly rely on biometric data, from users or may incorporate emotion recognition to infer maturity levels as indirect age indicators. The systems may employ facial recognition algorithms, but also behavioural pattern analysis with the aim to automatically categorize users into age groups for compliance purposes, grant or deny access to age-restricted content, and verify identity without requiring traditional documentation. If the systems do not fall within the scope of the prohibition of Article 5 (1) b) of the AI Act (exploiting vulnerabilities of minors) they should be considered as high risk.

The AI system performs profiling of natural person

- Yes

The AI system meets at least one of the exception criteria of Article 6(3)

- No

Motivate your previous answer and specify any exception criteria that it meets, if applicable

Age assessment systems using AI and biometric data may constitute profiling, when their use goes beyond simple age categorization for statistical purposes. These systems are intended to restrict, deny or grant access to content and services and cannot be considered to fall under the exception criteria of Article 6(3) as they do not perform a narrow procedural task, and are not intended to improve the result of a previously completed human activity. As such, they fulfil the conditions for high-risk classification and must be classified as high-risk.

5. Answer in Row 5:

Name and description of the system

- **Mental health apps**

Category of biometric system

- Emotion recognition Annex III Point 1 (c)

The system is considered high-risk

- Yes

Motivate your previous answer

- Mental health applications increasingly collect and process biometric data of users, e.g. through audio recordings of voice responses, voice diaries or physiological signals collected through connected devices such as smartwatches to make inferences about the users' mental health status. Where such systems are not already prohibited under Article 5(1)(b) or (a) of the AI Act, e.g. in cases involving the exploitation of vulnerabilities of protected groups or manipulation, they should be classified as high-risk. The processing of sensitive biometric and health-related data in this context carries significant risks, including inaccurate assessments, emotional and physical (self-)harm of consumers, as well as discriminatory outcomes.

The AI system performs profiling of natural person

- Yes

The AI system meets at least one of the exception criteria of Article 6(3)

- No

Motivate your previous answer and specify any exception criteria that it meets, if applicable

Mental health AI systems intended to detect emotional states through biometric indicators and interact with or support users in sensitive domains such as mental wellbeing, meet the required criteria for classification as high-risk AI systems. In terms of risk assessment under Article 7(2), these systems process special categories of personal data, act with a high degree of autonomy, and can significantly affect vulnerable individuals' health, access to support, or self-perception. They qualify as high-risk systems, as they carry significant risks due to their potential for causing harm to the psychological and physical wellbeing of users due to over-reliance by users and erroneous outputs as users may receive feedback or guidance that appears authoritative or therapeutic in nature.

These systems do not fall under the exemption criteria of Article 6(3). The emotion recognition does not constitute a narrow or preparatory procedural activity, nor does it merely support a previously completed human decision. Rather, it is a central functionality of the health application.

AI systems used in sensitive areas such as mental health, especially where they use biometric and emotional inference data, must be subject to the highest level of regulatory scrutiny. These applications can directly affect users' autonomy and wellbeing. Therefore, they clearly warrant classification as high-risk under the AI Act. These systems may also engage in profiling users.

6. Answer in Row 6:*Name and description of the system*

- **Smart mirrors on with emotion recognition**

Category of biometric system

- Emotional recognition (Annex III Point 1 (c)) and/or Biometric categorisation (Annex III Point 1(b))

The system is considered high-risk

- Yes

Motivate your previous answer

- Smart mirrors equipped with sensors and cameras are increasingly used in the retail sector and can be installed people's at home. They intend to offer virtual try-on functions by measuring body dimensions, analyse skin conditions as well as facial expressions. Their aim is to offer users personalized product recommendations e.g. for clothing or make up based on biometric and/or emotional data. These mirrors are widely used in retail already and the forecasts indicate a growing market (see: [Smart Mirror Market Size to Worth USD 1,299.83 Million by 2034](https://www.precedenceresearch.com/smart-mirror-market) <https://www.precedenceresearch.com/smart-mirror-market>). If these systems do not already fall under the prohibition of Article 5(1) (a) or (b) of the AI Act for manipulating consumers or exploiting consumer vulnerabilities, they should be classified as high-risk AI. They rely on biometric categorisation and emotion recognition to influence purchasing behaviour in real time. In terms of risk assessment under Article 7(2) they pose significant risks to consumer autonomy, privacy, personal data protection and fairness, especially in environments that create pressure to make appearance-based or impulsive choices. They also carry risk for financial harm, as they have the potential to push consumers to conduct impulsive purchases.

The AI system performs profiling of natural person

- nsure

The AI system meets at least one of the exception criteria of Article 6(3)

- No

Motivate your previous answer and specify any exception criteria that it meets, if applicable

These systems do not fall under the exception criteria of Article 6(3) as they do not perform a narrow procedural task, nor are they intended to improve the result of a previously completed human activity. They could be used for user profiling, e.g. when they are installed at home or when users log in to such systems with personal accounts when they are installed in retail stores.

7. Answer in Row 7:

- **Facial recognition used at commercial stores, retail chains or shopping malls to identify customers**

Category of biometric system

- *Remote biometric identification (Annex III Point 1(a))*

The system is considered high-risk

- Yes

Motivate your previous answer

- Such system use biometric identification to link a customer to a purchasing profile, preload past orders, or offer personalised prices. This a high-risk practice due to the asymmetry of power between consumers and retailers, the absence of meaningful consent.

The AI system performs profiling of natural person

- Yes

The AI system meets at least one of the exception criteria of Article 6(3)

- No

Motivate your previous answer and specify any exception criteria that it meets, if applicable

- The system goes beyond narrow identity verification. Deployers use it for personalised service delivery and consumer profiling. Therefore, it should not be exempt under Article 6(3) AI Act.

8. Answer in Row 8:

Name and description of the system

- **Smart toys using facial expression and/or voice analysis to detect and respond to a child's emotions**

Category of biometric system

- Emotion recognition (Annex III Point 1 (c))

The system is considered high-risk

- Yes

Motivate your previous answer

- Smart toys marketed as emotionally intelligent often use facial biometrics and/or voice analysis to infer children's' emotions like "happy," "bored," or "engaged." Such applications can be highly manipulative and exploitative. Children are a vulnerable group, and these AI systems risk influencing emotional development, encouraging dependency, and collecting sensitive data. These systems should be considered as being high-risk under Annex III Point 1 (c) if they are not designated as high risk AI under Art. 6 (1) in conjunction with Annex I of the AI Act.

The AI system performs profiling of natural person

- Yes

The AI system meets at least one of the exception criteria of Article 6(3)

- No

Motivate your previous answer and specify any exception criteria that it meets, if applicable

- These systems do not fall under the exception criteria of Article 6(3) as they do not perform a narrow procedural task, nor do they improve the result of a previously completed human activity. It performs emotional inference and profiling on children, a protected group, and therefore must not benefit from the exemptions under Article 6(3) of the AI Act.

9. Answer in Row 9:

Name and description of the system

- **Biometric verification systems for unlocking residential smart door locks**

Category of biometric system

- Remote biometric identification (Annex III Point 1 (a))

The system is considered high-risk

- Yes

Motivate your previous answer

Biometric verification systems for unlocking residential smart door locks may appear to perform a narrow procedural function, but their deployment in the context of housing raises significant concerns from a consumer and fundamental rights perspective. Access to one's home is an essential service and linked to the right to respect for private and family life, which is protected under Article 7 of the EU Charter of Fundamental Rights. When such biometric systems are implemented without offering genuine, non-biometric alternatives, they may leave tenants or residents with no meaningful choice, effectively coercing acceptance of biometric surveillance.

Moreover, it is important to distinguish between active and passive biometric verification systems. In active systems, users deliberately initiate the process of identification (for instance, by placing a finger on a scanner or positioning themselves in front of a camera). In contrast, passive systems may rely on proximity sensors and remote facial recognition, capturing biometric data of anyone approaching the door, often without their knowledge or meaningful consent. E.g. smart door locks may record and store video footage, including the pavement in front of the house or the path to the front door. In such cases, any person approaching the home (e.g. postal workers, neighbours, guests) could be subject to biometric surveillance who could be biometrically identified without consent. This brings such system closer to remote biometric identification and pose risks of incidental biometric surveillance, undermining the purpose of the current exemption. Such systems should not be exempted under Article 6(3) of the AI Act, as they do not merely perform a neutral, narrow task; rather, they determine access to a vital space based on the processing of biometric data, often under asymmetric conditions. Such systems should therefore be classified as high-risk AI.

The AI system performs profiling of natural person

- No

The AI system meets at least one of the exception criteria of Article 6(3)

- No

Motivate your previous answer and specify any exception criteria that it meets, if applicable

- The system does not fulfill a narrow procedural or preparatory task, operates outside full user control, governs access to an essential service, processes sensitive data and may compel individuals to accept biometric processing as a condition for entry, therefore disqualifying it from the exemption criteria under Article 6(3) AI Act.

10. Answer in Row 10:

Name and description of the system

- **Face-scanning filters in social media and beauty apps that adjust appearance and recommend cosmetic products**

Category of biometric system

- *Biometric categorisation (Point 1(b))*

The system is considered high-risk

- Yes

Motivate your previous answer

- Face-scanning filters in beauty and social media apps may appear harmless, serving a cosmetic or entertainment purpose. Nonetheless they have raised serious concerns about their deeper impact on consumer rights and psychological wellbeing. These systems go beyond merely enhancing user experience, when they analyse facial features to adjust appearance and recommend (cosmetic) products; especially when combined with persistent profiling or personalised advertising. They contribute to the promotion of unattainable beauty ideals, reinforce gendered and appearance-based pressure, and may exploit personal insecurities for commercial gain. Such systems pose a serious risk, as they may cause or contribute to psychological harm of users, especially minors, over time. E.g. by reinforcing insecurities of minors about their appearance or other mental problems. Such systems perform biometric categorisation by processing facial characteristics to infer user traits and tailor commercial content accordingly. If the biometric data is retained or used to build profiles for marketing purposes, their function shifts from experimenting with cosmetic possibilities to active, data-driven commercial influence. This goes far beyond a narrow or preparatory task and must be regulated accordingly. These systems meet the classification criteria under Art. 7 (2) and should be fall under AI Annex III Point 1(b).

The AI system performs profiling of natural person

- Unsure

The AI system meets at least one of the exception criteria of Article 6(3)

- No

Motivate your previous answer

- If the system involves commercial profiling, data retention, or personalised advertising based on biometric categorisation, it should not qualify as a narrowly scoped or low-risk application.

At least in such cases, the system should be disqualified from exemption and classified as high-risk under the AI Act.

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

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

The Commission should use its powers under Article 7(1) and expand the list of high-risk use cases in Annex III. Several AI use cases not named in Annex III meet multiple criteria under Article 7(1)(b) and Article 7(2), including their widespread deployment, processing of sensitive personal data, autonomous decision-making, irreversibility of harm, and the vulnerability of affected individuals. These systems fall within the areas in Annex III, but are not yet covered.

1. AI systems used in underwriting and pricing of non-life or -health insurance

Currently Annex III covers only life and health insurance. vzbv has called for including all AI used in insurance pricing and risk assessment for all consumer-facing forms in insurance. These systems can introduce unfair discrimination and financial exclusion, and their omission in Annex III 5. (c) leaves a significant gap in consumer protection.

2. AI systems used in payment and debt collection

vzbv has called for AI systems employed in debt collection to be classified as high-risk. These systems process sensitive data and have severe adverse consequences on individuals' and their access to basic services. They can exacerbate financial hardship for vulnerable consumers.

3. AI systems used in determining access to the housing market

AI systems are already used by landlords to prioritise potential tenants. Access to the housing market should be fair and unbiased. Housing is an essential service provided by private and public actors that fits the criteria to be added to Annex III (5) ('Access to and enjoyment of essential private services and essential public services and benefits'). AI systems that prioritise potential tenants for landlords or buyers of property influence decisions that determine the life chances of those affected.

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

Yes, there are use cases in Annex III that should be amended. These use cases require adaptation to fulfil the conditions under Article 7(1 and 2) of the AI Act. They need to be better specified to reflect emerging consumer harms in areas such as profiling, opaque scoring practices, and emotion recognition.

1. Emotion recognition (Annex III, point 1(c))

The current use case of emotion recognition is too vague and risks inconsistent interpretation. Annex III 1(c) of the AI Act should cover all AI systems that infer users' emotional states. Currently, Annex III 1(c) of the AI Act classifies AI systems as high risk only if they infer users' emotional states from *biometric data*, such as voice or video. This is because the definition of 'emotion recognition system' holds that emotion recognition must be inferred on the basis of users' biometric data. This scope is too narrow. The precondition that emotion recognition only falls within the scope of Annex III 1(c) if it uses biometric data only should be removed. Annex III 1(c) should be amended to explicitly state that it covers all AI systems that infer emotions or intentions of natural persons, not only those using biometric data, but also those that use non-biometric data, like behavioural data.

Critical examples that currently fall out of the scope of Annex III 1 (c) include companion chatbots that infer users' emotions from text typed into chat interfaces. These can be very harmful to users if they encourage dangerous behaviour or cause psychological harm, especially to minors. Other examples include text-based chatbots in online casinos or gambling websites, which could be used to infer gamblers' emotional states in order to encourage them to place more bets.

2. Insurance pricing and underwriting (Annex III, point 5(c))

Annex III refers narrowly to AI systems used for pricing and risk assessment in life and health insurance. However, vzbv has argued that a broader range of insurance-related AI applications in other areas of insurance meet the criteria for high risk and should be included.

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

No, vzbv opposes the removal of any use cases listed in Annex III. All use cases of consumer-facing AI systems currently listed in Annex III continue to meet the criteria set out in Article 7(2). From a consumer perspective, the use cases in the areas 'Biometrics' (Annex III point 1) and 'Access to and enjoyment of essential private services and essential public services and benefits' (Annex III point 5) remain highly sensitive and impactful in daily life. AI systems deployed in these areas regularly affect people's fundamental rights, opportunities, and access to fundamental goods and services.

Rather than removing use cases vzbv urges the Commission to strengthen and clarify existing categories and use cases to ensure effective enforcement, avoid ambiguity, and prevent circumvention. Several use cases (e.g. emotion recognition, underwriting and pricing of insurance) need clearer definitions and a broader scope to close current gaps. Removing existing high-risk use

cases risks weakening the level of protection offered to individuals under the AI Act and undermines the goal of building consumer trust in AI technologies. It could also lead to legal fragmentation and increase enforcement difficulties across Member States.

Impressum

Herausgegeben von:

Verbraucherzentrale Bundesverband e.V.

Rudi-Dutschke-Straße 17, 10969 Berlin

T +49 30 25800-0

info@vzbv.de

vzbv.de

Für den Inhalt verantwortlich:

Dr. Miika Blinn, Referent

Redaktion und Text:

Dr. Miika Blinn, Referent

Stand:

Monat, Jahr

Der Verbraucherzentrale Bundesverband e.V. ist im Deutschen Lobbyregister und im europäischen Transparenzregister registriert. Sie erreichen die entsprechenden Einträge [hier](#) und [hier](#).