AUTORITEIT
PERSOONSGEGEVENS

Call for input

AI systems for making risk assessments regarding criminal offences

Prohibition clause in EU Regulation 2024/1689 (AI Act)

Autoriteit Persoonsgegevens - Department for the Coordination of Algorithmic Oversight (DCA)

February 2025
DCA-2025-01

Summary

The European AI Act (Regulation (EU) 2024/1689) has been in force since 1 August 2024 and regulates the use of Artificial Intelligence (AI) in the European Union (EU). The AI Act has a risk-based approach. As a result, certain AI systems that pose an unacceptable risk are prohibited from 2 February 2025.

It is up to the supervisors of the AI Act to explain how the prohibitions will be interpreted for the purpose of supervision. In order to prepare for this in the Netherlands, the Autoriteit Persoonsgegevens (AP) asks interested parties (citizens, governments, businesses and other organisations) and their representatives for their needs, information and insights. We can use all input that we receive to consider the necessary further clarification of the prohibited AI systems.

On 27 September 2024, the AP published the first call for input on the first two prohibitions of the AI Act, followed on 31 October by the second call for input on emotion recognition in the areas of workplace or education institutions. On 17 December, a third call for input was published on AI systems for social scoring. In this fourth call for input, we address the fourth prohibition: AI systems for *making risk assessments regarding criminal offences* (prohibition D). This document provides an outline of specific criteria for these prohibited AI systems while requesting (additional) input through a set of questions. Contributions can be submitted until 3 April 2025.

The AP makes this call for input based on its role as a coordinating supervisor on algorithms and AI. For the purpose of this new task, the Department for the Coordination of Algorithmic Oversight (DCA) was established within the AP. This call for input also aligns with the preparatory work being done in support of future supervision of AI systems that are prohibited under the AI Act. The Dutch government is currently working on the formal designation of national supervisory authorities for the AI Act.

These tasks are assigned to the Directorate Coordination Algorithms (DCA) within the AP. Also, the call for input is in line with the preparatory work being done for the supervision of prohibited AI systems under the AI Act. The government is currently working on the formal designation of national supervisors for the AI Act.

I. Background

1. **The European AI Act (2024/1689) has been in force since 1 August 2024.** This Regulation sets out rules for the provision and the use of artificial intelligence (AI) in the EU. The premise of the AI Act is that while there are numerous beneficial applications of AI, the technology also entails risks that have to be managed. The legislation follows a risk-based approach. More restrictive rules will apply to those AI systems that pose a greater risk. Some systems entail such an unacceptable risk that their placing on the market or use is completely prohibited. This is, for example, the case with AI systems that are used for social scoring. The prohibitions are set out in Article 5 of the AI Act.

2. **This call for input provides a preliminary basis for further clarification of the prohibitions in the AI Act.** To get there, this call for input aims to gather generic information and insights on, among other things, the functioning of AI technologies and the application possibilities that are relevant to the clarification of the prohibitions.

Prohibited AI applications as from February 2025

3. **The prohibitions in the AI Act will become applicable soon**. As from 2 February 2025, the prohibited AI systems listed in Article 5 may no longer be put on the European market or used. As from 2 August 2025, market surveillance authorities should be designated for prohibited AI systems, and sanctions may be imposed for violations of the prohibitions. Before this time, violation of one of the prohibitions could already lead to civil liability.

Supervision in the Netherlands on compliance with the prohibitions

4. **The Dutch government is currently working on legislation designating which supervisory authority will be responsible for overseeing compliance with the prohibitions**. The AP (from the Department for the Coordination of Algorithmic Oversight) and the Dutch Authority for Digital Infrastructure (RDI) have issued an advice on this matter in collaboration and coordination with other supervisory authorities. It has been recommended, among other things, that the AP could be designated as the market surveillance authority for most of the prohibitions in Article 5. Following these recommendations, the AP will closely cooperate with other relevant supervisors for the supervision of prohibited AI systems.

5. **Because the prohibitions in this call concern AI systems that also fall under other Union laws, this call has been coordinated within the AI and Algorithm group of the Dutch Cooperation Platform of Digital Supervisory authorities**. This is in the spirit of the requirement in Article 70(8) of the AI Act to consult relevant national competent authorities responsible for other Union law that covers AI systems.

II. About this call for input

Purpose: Why we ask for input

6. **It is up to the supervisors of the AI Act to explain how the prohibitions will be interpreted for the purpose of supervision.** In preparation for this, the AP is asking for information and insights from stakeholders (citizens, governments, companies and other organisations) and their representatives. All responses can be used for further explanation of the prohibited AI. Within the AP, the Department for the Coordination of Algorithmic Oversight is charged with this task.

7. **This call for input discusses the prohibition of AI systems *for making risk assessments regarding criminal offences* in the AI Act.** In addition to this call for input, the AP already published a first call on 27 September 2024 on two other prohibitions, namely the prohibition on manipulative and deceptive AI systems and the prohibition on exploitative AI systems. On 31 October 2024, the second call for input, on emotion recognition in the workplace or in education institutions, was published. And on 18 December 2024, a third call for input on AI systems for social scoring was published, together with a summary and follow-up steps in relation to the first call.

8. **The legislation and recitals serve as the foundation for this call for input.** Given the scope and possible impact of this prohibition, a call for input is issued for this prohibition. Please refer to the Annex to this document for an overview of all prohibitions in the AI Act.

9. **This call for input highlights specific aspects of this prohibition.** The focus is on those specific criteria that determine whether or not an AI system is within the scope of this prohibition. Each criterion is briefly explained based on the legislator's recitals of the AI Act. On 4 February 2025, the European Commission published the adopted 'Guidelines on Prohibited AI Practices, as defined in the AI Act' (hereinafter: Guidelines)[1] The explanations provided by the European Commission have been taken into account in this document. In some cases, we provide an interpretation of our own. If we do so, this is explicitly mentioned. We then pose several questions, the answers to which will contribute to a better understanding of the prohibition.

Process: This is how you send your input to us.

10. **You decide which questions you answer.** You can also provide us with other relevant input in addition to the questions asked. Please send your input to **dca@autoriteitpersoonsgegevens.nl** by 3 April 2025. Please mention the subject "call for input DCA-2025-01 ('AI systems *for making risk assessments regarding criminal offences*') and your name and/or your organisation in your email. If desired, you can provide us with your contact details so that we can reach you in case we have further questions. When we have received your input, we will send you a confirmation by email.

Follow-up: What do we do with your input?

11. **After the closure of this call for input, the AP will publish a summary and appreciation of the input on AI systems *making risk assessments regardig criminal offences*.** In this summary, we will refer in generic terms to the input received (e.g., "several sectoral representative organisations have indicated that', "a developer of AI systems points out that", "organisations advocating fundamental rights note that"). If preferred and

[1] European Commission 'Guidelines on Prohibited Artificial Intelligence practices established by Regulation (EU) 2024/1689 (AI Act)'. (2025).

indicated by you, we may explicitly name your organisation or group. Through our summarised and evaluative response, we can also share the acquired insights with other (European) AI supervisory authorities. For instance, the summary and appreciation of the contribution may be utilised in the drafting of Guidelines on the prohibitions.

12. **We will only use your input for our task to obtain information and insights about the prohibitions in the AI Act.** We will delete your personal data after publication of our summary and evaluation of the input, unless you have given permission for further use. For more information about how we process personal data, see: The AP and privacy.

More calls for input

13. **Following this call, there may be more calls for input on other parts of the AI Act, including the prohibitions.** The AP has previously called for input on manipulative, misleading and exploitative AI systems as well as on AI systems that are used for emotion recognition in the areas of workplace or education institutions.

III. Definition of the prohibition on AI systems "for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence"

General scope of prohibited AI systems

14. **The AI Act (and its prohibitions) apply to 'AI systems'.** Thus, in order to determine whether the Regulation applies, the first question is whether the product falls within the definition of an AI system:

> 'A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;'

15. **The prohibitions are addressed to providers (e.g. developers), users, importers, distributors and other operators.** They shall not place on the market, put into service or use the prohibited AI systems. It is therefore important for the above operators to ensure that they do not place on the market or use a prohibited AI system. To do so, they will have to verify whether the AI system in question is covered by the prohibitions in the AI Act.

Content of the prohibition

16. **This call for input focuses on the prohibition of AI systems used for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence.** In the remainder of this call for input, we will refer to this prohibition as 'prohibition D'. The Regulation defines this prohibition as follows:

> **Article 5(1)(d) ('prohibition D'):**
>
> 'the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity;'

17. **The AI Act identifies other AI systems for risk assessment and profiling for law enforcement purposes as high-risk systems. Such systems may be placed on the market and used if the rules set out in the AI Act are complied with.** Point 6(d) of Annex 3 of the Regulation defines such high-risk systems as 'AI systems intended to be used by law enforcement authorities or on their behalf or by Union institutions, bodies,

offices or agencies in support of law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups'. In addition, point 6(e) of Annex 3 also considers 'high-risk AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices and agencies in support of law enforcement authorities to profile natural persons as referred to in point (4) of Article 3 of Directive (EU) 2016/680, during the detection, investigation or prosecution of criminal offences.'

18. **Finally, the AI Act is without prejudice to the GDPR and Directive (EU) 2016/680.** Obligations of providers and deployers of AI systems in their role as controllers or processors stemming from Union or national law also apply in the design, development or use of AI systems.

IV. Criteria and questions regarding the prohibition

19. **In order to structure this call for input, separate criteria of the prohibitions have been highlighted in the following sections.** These criteria have been highlighted because they are important conditions for determining whether or not AI systems are covered by Prohibition D. For each criterion, a short explanation is provided, based on the explanation provided by the legislator in the explanatory recitals to the AI Act and the Guidelines published on 4 February 2025. In some cases, explanations are based on the AP's own interpretation; where this is the case, this is clearly indicated. This is followed by some accompanying questions that you can use when giving your input.

Criterion 1: Risk assessments

20. **This prohibition covers certain AI systems intended for making risk assessments in order to assess or predict the risk of a natural person committing a criminal offence.** Recital 42 to the Regulation explains that, in line with the presumption of innocence, natural persons in the Union should always be assessed on the basis of their actual behaviour: 'Natural persons should never be assessed on the basis of behaviour predicted by AI based solely on their profiling, personality traits or characteristics, such as nationality, place of birth, place of residence, number of children, level of guilt or type of car, without reasonable suspicion that that person is involved in a criminal activity based on objective, verifiable facts and without human assessment thereof. Therefore, risk assessments carried out in relation to natural persons, solely on the basis of profiling or assessment of their personality traits and characteristics, in order to assess the likelihood of them committing criminal offences, or to predict that an actual or potential criminal offence will take place, should be prohibited.' It follows from the prohibition that the 'risk assessments' include both the *assessment* and *prediction* of the risk of a natural person committing a criminal offence.

21. **The Guidelines state that the concept of risk assessments is also referred to as 'crime predictions'**. While there is no generally agreed definition of crime predictions, they generally refer to a variety of advanced AI technologies and analytical methods applied to a large amount of - often historical - data (including socioeconomic data, but also police records, etc.) which, combined with theories from criminology, are used to forecast crime as a basis to inform police and law enforcement strategies and actions to combat, control, and prevent crime.[2] According to the Guidelines, these risk assessments can be made at any stage in the law enforcement activities. For example: during prevention and detection of crimes, during investigation, prosecution and execution of criminal penalties (including assessing the risk of re-offending in the context of making decisions on the imposition of pre-trail detention) and individual's plan for reintegration into society after serving a criminal sentence.[3]

22. **Moreover, the prohibition applies regardless of whether there is profiling or assessment of personality characteristics of only one natural person or of a group of natural persons simultaneously**.[4]

[2] Guidelines, paragraph 189.
[3] Guidelines, paragraph 191.
[4] Guidelines, paragraph 194.

Questions on Criterion 1

1. Can you give a concrete example of (imaginary) AI systems used for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence?
2. Can you give an example of an (imaginary) AI system where it is unclear to you whether it is an AI system that is used for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence?
3. Is the distinction between *prediction* and *assessment* clear to you? If not, can you explain why in more detail?
4. The outcome of the AI system is a risk assessment to assess or predict the risk of a natural person committing a criminal offence. Can you give an (imaginary) example of what such a risk assessment could include?

Criterion 2: Criminal Offence

23. **The risk assessment shall also cover the risk of a natural person committing a *criminal offence*.** This could include, for example, AI systems deployed by the police for the purpose of detecting criminal offences committed by natural persons.

24. **The Guidelines state that the prohibition applies to law enforcement agencies, other public organisations and private organisations.**[5] As regards the latter, the Guidelines state that in some cases private organisations may also be covered by the prohibition. This stems from the wording of the prohibition, which does not mention that the prohibition exclusively applies to law enforcement authorities. [6]
In this context, the Guidelines state that it can be assumed that the prohibition applies to private actors, who are entrusted by law with the exercise of public authority and have public powers for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. [7]

25. **The Guidelines further state that private actors may also be explicitly requested to act on behalf of law enforcement authorities and carry out individual crime risk predictions on a case-by-case basis.** In those cases, the activities of those private actors could also fall within the scope of the prohibition.[8]

26. **In addition, the Guidelines mention that the prohibition may apply to private entities making risk assessments that are objectively necessary in order to comply with a legal obligation, to which those private entities are subject.** Consider, for example, the screening of customers that banks have to carry out in the context of anti-money laundering legislation of the Union.[9]

27. **In other words, the Guidelines state that if private parties are not entrusted by law with certain specific law enforcement tasks, act on behalf of law enforcement authorities or are subject to specific legal obligations as described above**, the use of AI systems for making risk assessments in the context of the

[5] Guidelines, parapraph 219.
[6] Guidelines, paragraph 207.
[7] Guidelines, paragraph 208.
[8] Guidelines, paragraph 208.
[9] Guidelines, paragraph 209.

normal course of business and with the aim of protecting their own private interests is not considered to be covered by the prohibition.[10]

28. **The Guidelines state that the prohibition applies to criminal offences only. Administrative offences do not fall within the scope of prohibition D.**[11] Whether an offence is administrative or criminal in nature may depend on Union or national law, however. For offences not directly regulated by Union law, the national qualification of the offence is subject to scrutiny of the Court of Justice, as 'criminal offence' has an autonomous meaning within Union law and must be interpreted consistently by the Member States.[12]

Questions on Criterion 2

5. Can you give an (imaginary) example of an AI system where it is not sufficiently clear to you whether it qualifies as a system used to assess or predict a risk of a criminal offence?
6. Can you give examples of offences where, despite the explanations above, it is still unclear to you whether they classify as criminal offences?

Criterion 3: Solely on the basis of profiling of a natural person or an assessment of their personality traits and characteristics

29. **A third criterion for the applicability of the prohibition is that, as stated in the Guidelines, risk assessments must be based *solely* on profiling of a natural person or *solely* on the assessment of his or her personality traits and characteristics.** The Guidelines state that the element 'solely' applies to both profiling and assessment of personality traits or characteristics. In any event, as described in the recitals, the prohibition does not cover risk analyses that are not based on profiling of natural persons or on the personality traits and characteristics of natural persons. Those analyses must therefore be based solely on them in order to be covered by that prohibition.

30. **According to the Guidelines, solely implies, on the one hand, the possibility that other elements may be involved, as a result of which this criterion may no longer be met**. On the other hand, such elements must be sufficiently substantial and significant for the risk assessment to fall outside the scope of the prohibition.[13]

31. **Risk assessments can first be based on profiling. For the definition of profiling, the AI Act refers to the definition in the General Data Protection Regulation (GDPR).** Profiling is defined as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

[10] Guidelines, paragraph 211.
[11] Guidelines, paragraph 217.
[12] Guidelines, paragraph 218.
[13] Guidelines, paragraph 202.

32. **In the 'Guidelines on automated individual decision-making and profiling for the purposes of Regulation (EU) 2016/679', the European data protection authorities provide further explanations on the concept of profiling in the GDPR and Directive (EU) 2016/680.**[14] The Guidelines explain that profiling consists of three elements, namely, a) it must be an automated form of processing, b) it must relate to personal data, and c) the objective of the profiling must be to evaluate personal aspects about a natural person. Attention should be paid to the fact that 'any form of automated processing' is intended to have a broad effect. However, a form of automated processing is not always the same as a decision 'based solely on automated processing' (within the meaning of Article 22 GDPR). Even if there is no automated decision-making within the meaning of Article 22 GDPR (because, for example, there is meaningful human intervention), there may still be profiling.

33. **The Guidelines further explain that the use of the word "evaluate" suggests that profiling involves some assessment of a person.** A simple categorisation of individuals based on characteristics such as age, gender and height does not necessarily lead to profiling.

34. **In addition to a risk assessment based on profiling, the risk assessment may also be based on an assessment of personality traits and characteristics of a natural person.** The recitals to the Regulation list a number of examples of what can be understood by personality traits and characteristics, namely, nationality, place of birth, place of residence, number of children, level of guilt or type of car. These examples are mainly about characteristics of natural persons and not so much about personality traits. The Guidelines explain that personality traits and characteristics are often also part of profiling. However, the assessment can also be based on personality traits and characteristics without profiling.[15]

35. **The recitals to the AI Act provide two further examples of AI systems that in any case do not fall under the scope of the prohibition.** In any event, the prohibition does not cover risk analyses that are not based on the profiling of natural persons or on the personality traits and characteristics of natural persons, such as AI systems that use risk analyses to assess the likelihood of financial fraud by companies based on suspicious transactions, or risk analysis tools to predict the likelihood of localisation of narcotic drugs or illicit goods by customs authorities, for example based on known trafficking routes.

---

[14] See also Guidelines on automated individual decision-making and profiling for the purposes of Regulation (EU) 2016/679', footnote 1: "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. "Profiling and automated individual decision-making also fall within the scope of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. These guidelines focus on profiling and automated individual decision-making under the GDPR, but also cover these two topics under Directive (EU) 2016/680 with regard to their similar provisions. These guidelines do not include an analysis of specific features of profiling and automated individual decision-making under Directive (EU) 2016/680, as they are included in Opinion WP258 on some key issues of the Law Enforcement Directive (EU 2016/680) adopted by the Article 29 Working Party on 29.11.2017. Pages 11 to 14 of that opinion deal with automated individual decision-making and profiling in the context of data processing for law enforcement purposes. The opinion is available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178.'

[15] Guidelines, paragraph 197.

Questions on Criterion 3

7. Can you give an (imaginary) example of an AI system making risk assessments or predictions of natural persons in order to assess or predict the risk of a natural person committing a criminal offence solely *on the basis of automated profiling of natural persons?*
8. Could you give an (imaginary) example of an AI system making risk assessments or predictions of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, where this is made possible *solely on the basis of the assessment of their personality traits and characteristics*?
9. Could you give an example of an (imaginary) AI system making risk assessments or predictions of natural persons in order to assess or predict the risk of a natural person committing a criminal offence , but where these risk assessments are not solely based on profiling or assessing personality traits or characteristics of natural persons?
10. Is the difference between profiling on the one hand and assessing a person's personality traits or characteristics on the other, clear?
11. Is the distinction between personality traits and characteristics sufficiently clear to you?

Scope of the prohibition: 'this prohibition shall not apply to AI systems used to support the human assessment of a person's involvement in a criminal activity, which is already based on objective and verifiable facts directly linked to the criminal activity'

36. **Prohibition D does not apply to AI systems used to support the human assessment of a person's involvement in a criminal activity, which is already based on objective and verifiable facts directly linked to the criminal activity.** The legal text clarifies that this is an AI system used to *support* a human assessment of a person's involvement in a criminal activity. In addition, the human-assisted assessment should cover *objective and verifiable facts directly linked to* the criminal activity.

Questions about the scope of prohibition

12. Can you give an example of an (imaginary) AI system *to support* the human assessment of a person's involvement in a criminal activity?
13. Can you give an example of objective or verifiable facts directly linked to the criminal activity?
14. What further questions or need for clarification do you have in relation to the scope of the prohibition?

37. **In conclusion, it is stressed that this document does not cover all aspects of the prohibition.** Therefore, interested parties are expressly invited to provide relevant input, also outside the questions asked, for the further explanation of prohibition D.

Concluding questions

15. Apart from the questions asked, is there any other relevant input that you would like to provide for the further explanation of Prohibition D?
16. Do you think it is desirable that we explicitly mention your organisation or group in our public response and appreciation to this call for input, for example so that we can discuss examples and considerations that you provide?

Annex: overview of prohibitions from Article 5(1) of the AI Act 2024/1689

Prohibition A: Certain manipulative AI systems

AI systems that deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm.

Prohibition B: Certain exploitative AI systems

AI systems that exploit any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm.

Prohibition C: Certain AI systems that work with a social score

systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:

- detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;
- detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity.

Prohibition D: AI systems for risk assessments or predictions that a natural person commits a criminal offence

AI systems for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity.

Prohibition E: Untargeted scraping of facial images

AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.

Prohibition F: Certain AI systems for emotion recognition in the workplace or in education

AI systems that infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons.

Prohibition G: Certain AI systems for biometric categorisation of persons

AI systems for biometric categorisation that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorising of biometric data in the area of law enforcement.

Prohibition H: Certain AI systems for real-time remote biometric identification in publicly accessible spaces for the purpose of law enforcement

AI-systems used for of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

- the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;
- the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack
- the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 for the processing of biometric data for purposes other than law enforcement.