EUROPEAN
COMMISSION

Brussels, XXX
[…](2026) XXX draft

ANNEX

ANNEX

to the

COMMUNICATION FROM THE COMMISSION

Draft Commission guidelines on the classification of high-risk AI systems under Article 6 of Regulation (EU) 2024/1689 (AI Act) for stakeholder consultation

Draft Commission guidelines on the classification of high-risk AI systems under Article 6 of Regulation (EU) 2024/1689 (AI Act) for stakeholder consultation

Contents

I. Introduction **3**

II. General principles for classification of high-risk AI systems **4**

III. High-risk classification according to Article 6(1) and Annex I AI Act **4**

IV. High-risk classification according to Article 6(2) and Annex III AI Act **4**

1. Rationale, approach 4

2. Horizontal issues for Annex III use cases 5

2.1. The role of human involvement and high-risk classification 5

2.2. Limitations in some use cases to natural persons 5

2.3. AI systems as part of complex systems/products and services 6

2.4. 'Intended to be used' 7

2.5. 'On behalf of' 7

2.6. 'In so far as their use is permitted under relevant Union or national law' 7

2.7. 'Filter' to exempt AI systems from being high-risk according to Article 6(3) 8

2.7.1. Conditions for the 'filter' to apply 8

2.7.2. Exception for profiling 13

2.7.3. Self-assessment by the provider, registration and monitoring of systems benefitting from the filter mechanism 14

2.7.4. Protection against circumvention 15

3. High-risk AI systems in the areas listed in Annex III 15

3.1. Biometrics 15

3.1.1. Overview of use cases and horizontal issues 15

3.1.2. Point 1(a): Remote biometric identification systems 18

3.1.3. Point 1(b): Biometric categorisation 33

3.1.4. Point 1(c): Emotion recognition 36

3.2. Critical infrastructure 38

3.2.1. Overview of use cases and horizontal issues 38

3.2.2. The critical digital infrastructure use case 41

3.2.3. The road traffic use case in critical infrastructure 42

3.2.4. The supply of water use case in critical infrastructure 44
3.2.5. The supply of gas use case in critical infrastructure 45
3.2.6. The supply of heating use case in critical infrastructure 46
3.2.7. The supply of electricity use case in critical infrastructure 46
3.3. Education and vocational training 48
3.3.1. Overview of use cases and horizontal issues 49
3.3.2. Point 3(a): AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels 50
3.3.3. Point 3(b): AI systems intended to be used to evaluate learning outcomes 53
3.3.4. Point 3(c): AI systems intended to be used for the purpose of assessing the appropriate level of education 55
3.3.5. Point 3(d): AI systems intended to be used for monitoring and detecting prohibited behaviour of students 58
3.4. Employment 60
3.4.1. Horizontal issues 60
3.4.2. Point 4(a): AI systems intended to be used for the recruitment or selection of natural persons 62
3.4.3. Point 4(b): AI systems intended to be used to manage work-related relationships 71
3.5. Access to and enjoyment of essential private services and essential public services and benefits 78
3.5.1. Horizontal issues and overview of use cases 79
3.5.2. Point 5(a): Evaluation of the eligibility of a natural person for essential public assistance benefits and services, and the granting or denying such benefits and services 79
3.5.3. Point 5(b): AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score 85
3.5.4. Point 5(c): AI systems intended to be used for risk assessment and pricing in the case of life and health insurance 89
3.5.5. Interplay with other Union legislation: Article 144 of Regulation (EU) No 575/2013 (Capital Requirements Regulation) and Article 120 of Directive /2009/13/8 EC (Solvency II Directive) 92
3.5.6. Point 5(d): Evaluation and classification of emergency calls or the dispatching or establishing prioritisation of emergency first response services 94
3.6. Law enforcement 99
3.6.1. Overview of use cases and horizontal issues 99
3.6.2. Point 6(a): Assessing the risk of a natural person becoming the victim of a criminal offence 104

3.6.3. Point 6(b): Polygraphs and or similar tools 106
3.6.4. Point 6(c): AI systems intended to be used to evaluate the reliability of evidence 108
3.6.5. Point 6(d): AI systems assessing offending or reoffending of concrete person(s) 111
3.6.6. Point 6(e): AI systems intended to be used for the profiling of natural persons in the course of the detection, investigation or prosecution of criminal offences 113
3.6.7. Other AI systems falling outside the use cases of point 6 of Annex III 115
3.7. Migration, asylum and border control management 116
3.7.1. Overview of use cases and horizontal issues 117
3.7.2. Point 7(a): AI systems intended to be used as polygraphs or similar tools 121
3.7.3. Point 7(b): AI systems intended to be used for risk assessment of persons seeking to enter or stay 122
3.7.4. Point 7(c): AI systems intended to be used for assistance in examining asylum/visa/residence applications and associated complaints 125
3.7.5. Point 7(d): AI systems intended to be used for detecting, recognising or identifying natural persons in migration, asylum or border control management contexts (excluding travel-document verification) 129
3.8. Administration of justice and democratic processes 131
3.8.1. Point 8(a): AI systems intended to be used to assist judicial authorities or in alternative dispute resolution 131
3.8.2. Point 8 (b): AI systems intended to be used for influencing the outcome of elections or referendum 142
V. Entry into application of the rules for high-risk AI systems 147
VI. Review and update of the high-risk use cases and the Commission guidelines 147

Disclaimer: These Guidelines are still a draft document. They provide clarifications for the classification of AI systems as high-risk pursuant to Article 6 AI Act and a list of practical examples to assist in such classification. The drafts are published for stakeholder feedback to provide input to the Commission before it adopts a finalised version. The Guidelines are presented in a user friendly manner on the AI Act Single Information Platform that allows users to look and search only the area(s) and use cases of interest to them.

I. Introduction

[see separated chapters]

II. General principles for classification of high-risk AI systems

[see separated chapters]

III. High-risk classification according to Article 6(1) and Annex I AI Act

[see separated chapters]

IV. High-risk classification according to Article 6(2) and Annex III AI Act

(63) Article 6(2) AI Act classifies as high-risk certain stand-alone AI systems that, in view of their intended purpose, are considered to pose a significant risk to health, safety or fundamental rights. This section explains how that classification is structured, including the Annex III areas and the approach for classification, provides clarifications for the certain horizontal concepts and detailed explanations for each of the areas and the exhaustive list of use cases covered with illustrative examples of systems that are high-risk or not.

1. Rationale, approach

(64) Annex III AI Act lists eight broad areas that are particularly susceptible to risks arising in relation to such systems. Those areas are the following:

1. Biometrics;
2. Critical infrastructure;
3. Education and vocational training;
4. Employment, workers' management and access to self-employment;
5. Access to and enjoyment of essential private services and essential public services and benefits;
6. Law enforcement;
7. Migration, asylum and border control management;
8. Administration of justice and democratic processes.

(65) In line with the risk-based approach of the AI Act, only a limited set of AI system use cases falling within those broad areas are classified as high-risk. Those use cases are explicitly listed for each area in Annex III. That list of use cases is exhaustive and can only be modified through the adoption of delegated acts, provided the conditions of Article 7(1) AI Act are fulfilled. This ensures that the rules and safeguards for the classification of AI systems as high-risk under Article 6(2) AI Act are targeted and proportionate, while avoiding unnecessary regulatory burdens for the majority of AI systems falling within the areas listed in Annex III.

(66) Article 6(3) AI Act provides a mechanism whereby AI systems that fall within one of the use cases listed in Annex III, but which do not pose significant risks of harm are exempted from high-risk classification ('the filter mechanism'). The filter mechanism is assessed in Section 2.7. below.

(67) Due to the direct and harmonised effects of the AI Act for the placement on the market, putting into service, and use of high-risk AI systems in the Union, the classification of an AI system as high-risk under Article 6(2) will have a uniform effect throughout all Member States. This is without prejudice to national prerogatives in certain areas (e.g., education under Article 165 TFEU).

(68) Classifying AI systems as high-risk under Article 6(2) AI Act does not mean that their use is prohibited. Rather, those systems are subject to appropriate requirements to ensure that they

perform accurately and as intended, and that risks to health, safety and fundamental rights are properly assessed and mitigated. This approach enables the creation of a single market for trustworthy AI systems in the Union and promotes trust and AI uptake in sensitive areas, where the identified high-risk use cases can lead to serious consequences.

2. Horizontal issues for Annex III use cases

(69) This section provides clarifications on certain horizontal aspects regarding the classification of AI systems as high-risk under Article 6(2) AI Act, which are relevant for all areas and use cases listed in Annex III AI Act.

2.1. The role of human involvement and high-risk classification

(70) To assess whether an AI system qualifies as high-risk under Article 6(2) AI Act, the only relevant determinant is whether the intended purpose of the system includes one of the use cases listed in Annex III AI Act. Since human involvement cannot change the purpose and area in which a system is intended to be used, it has no effect on the classification of the system as high-risk under Article 6(2) AI Act. Rather, human oversight is a prerequisite for compliance with the rules for high-risk AI systems pursuant to Article 14 AI Act and a necessary requirement for systems classified as high-risk.

(71) If the intended purpose of an AI system is covered by a use case listed in Annex III AI Act, the provider may exempt the system from high-risk classification pursuant to Article 6(3) AI Act, provided that it can demonstrate that at least one of the four conditions of that provision are met and provided the system does not perform profiling. To determine whether any of those conditions are met, the provider must consider which tasks the system is intended to perform, which again relates to the intended purpose of the system, including its context and the conditions of use (see Section II.2.). The type and degree of human involvement during the deployment of the system may therefore play a role in the classification of an AI system as high-risk, but only to demonstrate that the tasks the system is intended to perform are narrow procedural tasks or preparatory in nature, or that the system is only intended to improve a previously completed human activity. The provider cannot exempt and categorise an AI system as 'low risk' simply by adding to it a requirement for human involvement (see in more detail Section 2.7 below).

2.2. Limitations in some use cases to natural persons

(72) Several use cases listed in Annex III AI Act refer to the intended use of an AI system to directly or indirectly evaluate 'natural persons' in relation to the specific use case outside the cases prohibited by Article 5(1)(c) AI Act. To determine whether an AI system is intended to be used in such a manner, the provider must assess whether such use is within the intended uses of the system, irrespective of whether the application of the system to natural persons is the sole purpose of the system or only one among several purposes.

(73) A 'natural person' is distinct from a legal person. The notion of 'natural person' also includes, but is not restricted to, consumers. Sole traders, independent professions and other self-employed persons are also considered natural persons in relation to the commercial activity undertaken by

those persons. This includes, for example natural persons acting in a professional capacity (consultants, designers, journalists)[1].

Example: A provider develops an AI system which is intended to establish the credit score of an owner of a small business or a company, which is not a legal entity. Such a system is not intended to evaluate a 'natural person' when it uses only business or company data.

(74) The explicit mention of 'natural persons' in certain use cases listed in Annex III AI Act means that an AI system that is intended to be used to evaluate or assess natural persons is in scope, irrespective if it is (also) used to assess legal persons or companies. In contrast, such AI systems that are only intended to be used to assess legal persons or companies, without intending to evaluate natural persons, are outside the scope of those use cases and therefore do not constitute high-risk AI systems.

Example: A provider develops an AI system to assess the creditworthiness of companies by evaluating their data, balance sheets and financial statements. So long as the system is not intended to be used to evaluate the personal finances of natural persons, its intended use will not qualify as the evaluation of 'natural persons' and it will therefore not be considered high-risk. In addition, also when the owner of a legal entity is assessed for creditworthiness backing a company loan, the owner does not fall under Point 5b), even though they are acting as a natural person, as the primary beneficiary of the credit is the company, not the individual.

2.3. AI systems as part of complex systems/products and services

(75) Where several AI systems form part of a more complex AI system, so that their combined intended purpose or joint outputs materially influence an individual decision, the combined configuration is treated as a single AI system for the purpose of high-risk classification. To avoid circumvention of the high-risk classification rules by system design, split architectures are assessed as a whole. Where the components of an AI system are configured as intended to be used for a use case listed in Annex III AI Act, the combined system will be classified as high-risk pursuant to Article 6(2) AI Act. Even if certain modules on their own may be exempt under Article 6(3) AI Act, these exemptions do not apply if the overall system's configuration and functioning influence key aspects of the decisions made with the AI system's support in the context of the high-risk use case. This principle also extends to complex, interconnected setups like agentic AI systems that coordinate and interact through linked actions as long as these linked actions or components serve in conjunction an intended high-risk purpose.

(76) By contrast, strictly procedural or preparatory functions of an AI system that are linked to high-risk system remain eligible for exemption from high-risk classification under Article 6(3) AI Act where they are genuinely separable from the AI systemand when they do not structure or feed outputs that

[1] Para. 216 of the Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), Text with EEA relevance, (OJ L, 2024/1689, 12.7.2024).

materially influence the examination of an individual case (e.g. the examination of an application for essential public benefits). Furthermore, AI-enabled functions and components that are genuinely separable, put into service independently from that system and that do not contribute to a high-risk purpose are out of scope from the high-risk classification.

2.4. 'Intended to be used'

(77) The AI Act uses the terms 'intended to be used' as a requirement for the classification of an AI system as high-risk under the use cases listed in Annex III AI Act (with exceptions in point 1(a) and point 5(d) Annex III AI Act). Such intended use is identical to the intended purpose of the system as defined by the provider (see Section II.2. above). If the intended purpose does not encompass one of the use cases listed in Annex III AI Act, the system is not 'intended to be used' for such a use case and therefore cannot be classified as high-risk pursuant to Article 6(2) AI Act.

(78) Moreover, to be classified as high-risk pursuant to Article 6(2) AI Act, it is not necessary for the AI system to be actually in use. Instead, the provider must assess the intended use of the system before placing it on the EU market or putting it into service. It is at that moment that the AI system, if it is high-risk, must be in conformity with the requirements for high-risk systems and that the provider of the system must meet the obligations for such systems.

2.5. 'On behalf of'

(79) The use cases listed in Annex III that concern the use of an AI system by public authorities consistently use the terms 'on behalf of' or 'or on [their] behalf' to cover AI systems that are intended for use not only by the public authorities themselves, but also by third parties (i.e. private entities) where a public authority outsources activities to those entities falling within those use cases.

(80) The use of those terms is meant to avoid circumvention of the high-risk classification in cases where an AI system is marketed only to certain natural or legal persons, while the risk of the system for fundamental rights is the same as that where public authorities are involved, because the activity is performed on behalf of the public authority.

(81) A third-party/private entity will be considered to act 'on behalf of' a public authority if the public authority delegates the performance of certain activities (or parts of those activities) to that party/entity or that authority has requested the party/entity to support such activities in specific cases. A third-party/private entity will not be considered to act 'on behalf of' a public authority if the private entity acts on its own behalf, either on a voluntary basis or to comply with a legal obligation.

Example: An accounting firm that deploys an AI system that detects money laundering to comply with its obligations under EU anti-money laundering legislation will not be considered to act on behalf of law enforcement authorities, but on its own behalf, so that the system will not be classified as high-risk in the area of law enforcement listed in point 6 of Annex III AI Act.

2.6. 'In so far as their use is permitted under relevant Union or national law'

(82) As the terms 'in so far as their use is permitted under relevant Union or national law' used in points 1, 6 and 7 of Annex III AI Act suggest, the fact that an AI system falls within one of the use cases listed in those points does not necessarily mean that the system can be lawfully used in those cases. As stated in recital 63 AI Act, any such use may occur solely in accordance with the applicable requirements resulting from the Charter of Fundamental Right ('the Charter') and from the applicable acts of secondary Union law and national law.

(83) In addition to the prohibitions, the use of an AI system may also be restricted by other provisions of Union law or national law. This is also consistent with Article 2(9) AI Act, which states that the AI Act applies 'without prejudice' to the rules laid down by other Union legal acts related to consumer protection,product safety and data protection.

2.7. 'Filter' to exempt AI systems from being high-risk according to Article 6(3)

(84) Article 6(3) AI Act allows providers of AI systems listed in Annex III AI Act to exempt those systems from high-risk classification, even though the conditions for such classification have been met based on the intended purpose of the system. This 'filter mechanism' ensures case-specific proportionality in the classification of high-risk AI systems.

(85) The filter mechanism can be applied where an AI system meets one of the conditions set out in points (a) to (d) of Article 6(3) AI Act. The article and Recital 53 explain the reasoning behind the filter mechanism, notably that if one of the aforementioned conditions is fulfilled, the AI system typically does not materially influence the outcome of decision-making by the system and therefore does not lead to a significant risk of harm.

2.7.1. Conditions for the 'filter' to apply

(86) According to Article 6(3) AI Act, a provider of an AI system that would normally classify as high-risk pursuant to Article 6(2) AI Act may exempt that system from high-risk classification if any of the following conditions are met:

(a) The AI system is intended to perform a narrow procedural task;
(b) The AI system is intended to improve the result of a previously completed human activity;
(c) The AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or
(d) The AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III AI Act.

(87) First, it is important to clarify that the filter mechanism applies only to AI systems that would normally be classified as high-risk pursuant to Article 6(2) AI Act. It does not apply to AI systems that classify as high-risk pursuant to Article 6(1) AI Act.

(88) Second, the conditions listed in Article 6(3) AI Act are exhaustive, but alternative. Consequently, if the AI system falls within at least one of the conditions, it may be deemed not to pose significant risk of harm to the health, safety or fundamental rights of natural persons despite the fact that certain risks might remain. There is no separate or independent assessment to determine whether the AI system poses a significant or any risk of harm besides those conditions. Whether an AI system may benefit from the filter mechanisms in Article 6(3) AI Act depends on a self-assessment by the

provider. These conditions are explained in more detail in the subsections below. As Article 6(3) represents an exception from rules aimed at (among others) protecting fundamental rights, the conditions must be interpreted narrowly. The conditions for the filter must also be interpreted in the light of the first sub-paragraph of Article 6(3) AI Act that the system should not materially influence the outcome of the decision.

(89) Third, the third sub-paragraph of Article 6(3) AI Act provides that an AI system referred to in Annex III shall always be classified as high-risk where the system performs profiling within the meaning of Article 4(4) of Regulation (EU) 2016/679[2] or Article3(4) of Directive (EU) 2016/680[3] or Article 3(5) of Regulation (EU) 2018/1725[4] (see more on profiling in Section 2.7.3 below).

(90) Additionally, even if an AI system fulfils one of the conditions for the filter mechanism (for example, performs a narrow procedural task), such a system cannot benefit from that mechanism and will still be classified as high-risk if it forms part of a complex system where its combined intended purpose or joint outputs materially influence an individual decision within a high-risk use case or where the AI system is part of complex interconnected systems, such as agentic AI systems (see para. 72 above).

a) Narrow procedural task

(91) Point (a) of Article 6(3) AI Act lists as the first condition under which the filter mechanism may apply that an AI system is intended to perform a narrow procedural task. As clarified in Recital 53 AI Act, such a system is considered to pose only limited risks. That recital lists as examples of such systems '*an AI system that transforms unstructured data into structured data, an AI system that classifies incoming documents into categories or an AI system that is used to detect duplicates*'.

(92) This condition may therefore cover AI systems that are intended to categorise, change the format, structure or presentation of data, or change its metadata.

For example, an AI system performs a narrow procedural task when it sorts incoming applications for admission to school or university according to the grade or educational level applied for. Such systems may categorise applications into predefined categories (e.g. primary, secondary, high school or specific grades) based on information provided in the application, without evaluating applicants' suitability or making admission decisions.

(93) However, this condition does not apply to all categorisation systems. In particular, AI systems that perform a value judgement of data relevant for decision-making, for example categorisation of input

[2] 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, (OJ L119/1, 4.5.2016).
[3] 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, and repealing Council Framework Decision 2008/977/JHA. (OJ L119/89, 4.5.2016).
[4] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies, and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L295/39, 21.11.2018).

data as 'useful' or 'less useful' for the human assessment, or attributing a score or ranking to input data, are likely to have a broader impact on the assessment process and will therefore not be considered to perform only a 'narrow procedural task'.

For example, an AI system used in the context of migration, border control and management that performs narrow procedural tasks, such as scanning each submitted visa file, converting scanned documents into text for indexing, automatically filing items into fixed, predefined folders such as 'identity documents', 'travel itinerary', 'supporting evidence', and 'translations', and detecting exact duplicate attachments and marking them as duplicates, could benefit from the filter mechanism, provided it does not rank in a manner that evaluates, filter out or hide documents, does not label any material as 'useful' or 'less useful', and does not suggest next steps or credibility assessments.

In a similar scenario, an AI system that is used to detect and flag incomplete forms to initiate their return to the applicant to be completed correctly could be classified as a narrow procedural task and benefit from the filter mechanism.

b) Improves the result of a previously completed human activity

(94) Point (b) of Article 6(3) AI Act lists the second condition under which the filter mechanism may apply, which is that the AI system is intended to improve the result of a previously completed human activity. Several cumulative elements must be present for this condition to apply:

- a human activity has been completed (e.g., human assessments or decisions);
- the completion of the activity led to a result; and
- the result is improved by the AI system (e.g., adjusted to achieve more clarity without changing the outcome or conclusion, etc.).

(95) The fact that the human activity should be completed, and that the completion should lead to a result, means that the AI system should not replace, nor autonomously perform, the human activity. Recital 53 AI Act specifies that such an AI system '*provides only an additional layer to a human activity with consequently lowered risk*', referencing as an example an AI system that is applied ex post to improve a previously drafted text.

(96) The notion 'improve' in this context means that the application of the AI system may lead to changes, but these changes should not revert or lead to a full revision or replacement of the previously completed human activity. The EU legislature deliberately chose the formulation 'improve', rather than 'review', to make this distinction and to highlight that the AI system must not be intended to provide a materially different result to the one previously performed by a human activity, but to verify or refine that activity. Any improvement introduced by the AI system should not change the rights, protection, legal or economic position of the persons who may be impacted by the system's output or by decisions taken on the basis of that output.

For example, if an AI system checks a decision, plan, or construction made by a human and provides a substantially different solution, this would not be considered 'improving' a previously completed

human activity within the meaning of Article 6(3)(b) AI Act, since it is not limited to refining or enhancing the outcome of that activity.

By contrast, examples of AI systems that serve auxiliary improvement functions include systems that flag errors or contradictions in finalized human work that perform a quality-assurance function; systems that map conclusions to evidentiary records to strengthen the traceability of a decision without substituting the human judgment; systems that convert human-validated content for interoperability or accessibility purposes that transform but do not replace human output.

c) Detect decision-making patterns or deviations

(97) Point (c) of Article 6(3) AI Act lists the third condition under which the filter mechanism may apply, which is that the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment. Recital 53 lists as an example of such an AI system a system that is applied to detect inconsistencies or anomalies in the grading pattern of a teacher.

(98) The notion 'decision-making pattern' should be interpreted narrowly. Decision-making patterns are patterns or trends derived from past data that predict or analyse how decisions are taken over time on a specific subject matter.

(99) Unlike the other conditions, which exclude AI systems from high-risk classification only if the system is restricted to procedural or preparatory tasks or improvements, the scenario listed in point (c) of Article 6(3) AI Act allows for a more substantive role for the system in the assessment process. In particular, it allows the AI system to compare the said human assessment with previous decisions and to potentially use this comparison to inform a human review that influences or replaces the previously completed human assessment. However, this impact is limited in three ways.

(100) First, the human assessment must have been completed, meaning that all necessary steps in the evaluation process must have been taken.

(101) Second, the AI system can only perform an ex-post comparative assessment, which involves determining whether a current decision aligns with previous patterns or decisions. It must not infer relevant criteria from previous decisions and propose a new assessment based on those criteria.

(102) Third, the AI system must not be intended to be used to replace or influence the previously completed human assessment without proper human review. 'Proper' means that the human review applied after the AI system's assessment should be meaningful and comprehensive, and it should consider, together with the result provided by the AI system, the various elements taken into account during the previously completed human assessment. Therefore, the output of the system can highlight discrepancies with previously made decisions, but cannot modify the input or alter the underlying reasoning. In order to allow proper human review, the system should not only flag, but also provide information on the discrepancies. It should however merely inform (e.g. through analytical tools used for quality assurance and statistics) and not replace the human assessment.

Example: An AI system intended to analyse past eligibility checks completed by public administrators in the public administration in order to detect decision-making patterns or deviations for quality-assurance and reporting, without proposing outcomes on live cases or evaluating the performance of staff members, e.g., in the context of the annual appraisal.

Assessment: If the system is intended to be used after the officials in the public administration have made their assessments, the system could be relevant for exemption pursuant to point (c) of Article 6(3) AI Act and does not constitute profiling. The comparison done by the system would allow the public administrator to detect divergences identified by the system from past decision-making patterns in similar cases, as well as all the elements and the evidence taken into consideration when the first assessment was made. The assessor or a quality assistance control will have the role to decide after proper human review whether the identified discrepancies are relevant or not for the completed assessment.

d) Preparatory task

(103) Point (d) of Article 6(3) AI Act lists the fourth condition under which the filter mechanism applies, which is that the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.

(104) The notion 'preparatory' in point (d) of Article 6(3) AI Act refers to tasks that occur prior to the actual assessment process. This specification is important, since it differentiates the preparatory task exemption in point (d) from the narrow procedural task exemption in point (a) of Article 6(3) AI Act, which can occur during the assessment process so long as it is clearly defined and limited in scope. At the same time, if the narrow procedural task occurs prior to the assessment and is preparatory in nature, both points in letters a) and d) may apply.

(105) As specified in Recital 53 AI Act, the preparatory nature of the task should be such that the '*possible impact of the output of the system [is] very low in terms of representing a risk for the assessment to follow*'. This aligns to the objectives of Article 6(3) AI Act, which sets out the conditions under which AI systems should not be considered to lead to a significant risk of harm, in particular because they do not materially influence the decision-making. Recital 53 AI Act specifies that an AI system that does not materially influence the outcome of decision-making should be understood as an AI system that does not have an impact on the substance, and thereby the outcome, of decision-making, whether human or automated.

(106) Recital 53 AI Act provides as examples AI systems performing preparatory tasks such as indexing, searching, processing, and linking. Such tasks add structure to the inputs that will be used in the later assessment producing an outcome, but they do not provide themselves an assessment leading to an outcome.

(107) The decisive factor in determining whether a task is 'preparatory' is the task's role in the decision-making process and proximity to the final human decision. If a task is deemed preparatory, the filter mechanism in point (d) of Article 6(3) AI Act may be applicable, regardless of the specific field in which the system will be used.

(108) If an AI system's output is intended to inform a human operator's assessment, it may be considered to perform a preparatory task only if the system's output is a general input or factor, for example supplementary information that supports an operator's decision-making process. Where the AI system is intended to produce a specific recommendation or evaluation of the case, it plays a decisive role in the assessment or the decision and can therefore not be considered to perform a preparatory task within the meaning of point (d) of Article 6(3) AI Act.

Example: An AI system is intended to be used for assessing data relevant to a decision (e.g. in relation to public benefits) and provides a human operator with references to the relevant legal provisions, information on jurisdiction, and possibly existing internal guidelines relevant to the decision-making process.

Assessment: The tasks performed by the system could be considered as preparatory within the meaning of point (d) of Article 6(3) AI Act, since they neither analyse nor evaluate the concrete cases at hand and do not produce an output that materially influences the decision. Rather, the system references general information as a supplementary information for the human assessor to consider in his or her decision.

2.7.2. Exception for profiling

(109) Article 6(3) AI Act provides that the filter mechanism may not be applied where an AI system performs profiling of natural persons. Article 3(52) AI Act defines the notion of profiling by cross-referring to Article 4(4) GDPR.

(110) Pursuant to that provision, profiling is to be understood as any automated form of processing, which is carried out on personal data with the objective to 'evaluate certain personal aspects' relating to a natural person[5]. That definition consists of three cumulative elements:

(i) there must be an automated form of processing;

(ii) which is carried out on personal data; and

(iii) the objective of which must be to evaluate personal aspects relating to a natural person.

(111) It is only if all three conditions are fulfilled that an AI system classified as high-risk pursuant to Article 6(2) AI Act does not benefit from the exemptions listed in Article 6(3) AI Act. While the element of automated processing will always be fulfilled with regard to AI systems, providers must determine whether the data input of the system includes personal data and whether the system is intended to be used to evaluate personal aspects relating to a natural person. Such an evaluation is normally conducted with the purpose of analysing or predicting personal aspects, for instance concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. In other words, profiling means the use of information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in

[5] See also Article 29, Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251 rev.01, 6.2.2018, p. 6 and 7, endorsed by the European Data Protection Board (EDPB).

particular to analyse, infer or make predictions about, for example, their ability to perform a task, interests, or likely behaviour[6].

For example, AI system used by customs authorities to assess the risk of goods entering the EU for not complying with legislation applicable at the border on the basis of information about the economic operators related to goods (e.g. container number, description of goods, routing, transport, payment method). The processing is not evaluating personal aspects of a natural person, but assesses the risk of non-compliant consignments, hence such evaluation would not amount to profiling.

(112) Where the personal data are not used to perform an evaluation of personal characteristics (which must always include a form of prediction, assessment or judgement) that evaluation will not constitute profiling[7]. For instance, a simple classification of individuals based on personal characteristics such as their age, sex, and height does not necessarily lead to profiling. Whether an evaluation includes predictions or the drawing of conclusions will depend on the purpose of the classification[8].

Example: An AI system is intended to be used in the context offor th recruitment of employees. The system is used to identify deviations from previous recruitment decision-making patterns before recruitment is completed (to detect potential inconsistencies and deviations from corporate recruitment policies), while evaluating the personal characteristics of the recruiters conducting the job interviews.

Assessment: The evaluation of the recruiter's decisions and their personal characteristics to analyse possible deviations from previous decision-making patterns constitutes profiling. While the use of the system could fall under point (c) of Article 6(3) AI Act, the fact that the system also involves the processing of personal data to profile recruiters means that the filter mechanism listed in that provision is not applicable.

2.7.3. Self-assessment by the provider, registration and monitoring of systems benefitting from the filter mechanism

(113) Whether an AI system may benefit from the filter mechanisms in Article 6(3) AI Act depends on a self-assessment by the provider.

(114) The consequence of applying the filter mechanism is that the AI system should not be classified as high-risk and therefore that neither the obligations for providers nor for deployers set out in Chapter III of the AI Act apply in relation to that system. However, Article 6(4) AI Act sets out specific obligations for providers of such AI systems, which are:

[6] Para. 154 of the Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), Text with EEA relevance (OJ L, 2024/1689).

[7] See also Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 6-7, endorsed by the EDPB.

[8] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 6-7, endorsed by the EDPB.

(i) to document the assessment before the AI system is placed on the market or put into service, and
(ii) to register the AI system in the EU database established pursuant to Article 71 AI Act, which is intended to ensure the traceability of exempted AI systems.

(115) The assessment should contain:

(i) a description of the intended purpose of the AI system;
(ii) a description why the system qualifies as high-risk pursuant to Article 6(2) AI Act;
(iii) a description which condition or conditions listed under Article 6(3) AI Act are considered to apply and why;
(iv) a description why the system does not perform profiling, in which case the filter mechanism of Article 6(3) AI Act should not be applied.

(116) The assessment should be recorded in a way that it can be made available at any time upon the request of a market surveillance authority. Deployers procuring AI systems are encouraged to verify the use of the exception in the EU database under Article 71 for their due diligence purposes.

2.7.4. Protection against circumvention

(117) The AI Act sets out several safeguards against the misapplication of the filter mechanism in Article 6(3) AI Act. According to Article 80 AI Act, market surveillance authorities may carry out evaluations of AI systems in respect of their classification as high-risk, request the provider of the system to bring that system into compliance with the high-risk requirements of the AI Act, and request the provider of the system to take corrective actions. Where the market surveillance authority finds that an AI system was misclassified as non-high risk to circumvent the application of the high-risk requirements and obligations in the AI Act, it is also empowered to impose penalties on the provider pursuant to Article 99 AI Act.

3. High-risk AI systems in the areas listed in Annex III

(118) This Section examines all high-risk use cases under each of the eight areas listed in Annex III AI Act and provides examples of AI systems that fall within or outside the scope of those use cases or that may be exempted under the filter mechanism of Article 6(3) AI Act, even if they fall within one of those use cases.

3.1. Biometrics

(119) Point 1 of Annex III AI Act lists three high-risk use cases covering AI systems intended to be used in the field of biometrics, in so far as such use is permitted under relevant Union or national law.

3.1.1. Overview of use cases and horizontal issues

(120) Point 1 of Annex III AI Act includes the following use cases:

(a) Remote biometric identification (RBI) systems;

(b) AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics; and

(c) AI systems intended to be used for emotion recognition.

(121) The aforementioned use cases are classified as high-risk given their potential intrusiveness on the rights and freedoms of the persons concerned by the systems, including because of the systems' reliance on biometric data and their sensitive nature. As explained in Section 2.6 above, the fact that an AI system is classified as a high-risk AI system under these use cases should not be understood to mean that the use of the system is lawful under other acts of Union law or under national law compatible with Union law.

i. Biometric data

(122) RBI systems involve the processing of 'biometric data'. Article 3(34) AI Act defines 'biometric data' as '*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data*'.

(123) Personal characteristics from which biometric data may be extracted are physical, physiological or behavioural attributes of a natural person. Physiological and physical biometrics employ bodily, structural, and relatively static attributes of a person, such as their fingerprints, the pattern of their iris, contours of their face, or the geometry of veins in their hands. Some attributes are microscopic in nature, but still exhibit biological and chemical structures that can be acquired and identified e.g., DNA and odour[9]. Behavioural biometrics monitor the distinctive characteristics of movements, gestures, and motor-skills of natural persons as they perform a task or series of tasks. This means that human movements, such as walking (gait analysis) or finger contact with a keyboard (keystrokes), are captured and analysed. Behavioural biometrics encompass a variety of attributes that exhibit both voluntary and involuntary repeated motions and associated rhythmic timings or pressures of body features ranging from signatures, gait, voice, click patterns, and keystrokes, through to eye tracking and heartbeats[10], electroencephalography (EEG)[11], or electrocardiograms (ECG)[12]. The biometric input may relate to one attribute (e.g., facial images) or multiple attributes (e.g., facial information combined with electroencephalogram (EEG)). Biometric data referring to characteristics of natural persons cannot, as such, concern deceased individuals, dead bodies, human remains of deceased people or traces thereof.

For example, the following AI systems do not fall within the use case of point 1 of Annex III:

- an AI system comparing DNA samples from a corpse;
- an AI system comparing facial image from human remains;

[9] Physiological and Behavioural Biometrics – Biometrics Institute, available online: https://www.biometricsinstitute.org/physiological-and-behavioural-biometrics/.
[10] Physiological and Behavioural Biometrics – Biometrics Institute; available online: https://www.biometricsinstitute.org/physiological-and-behavioural-biometrics/.
[11] See EDPS, TechDispatch 1/2024 – Neurodata, 3.6.2024, in which the use of brain data and related technology is discussed, as well as the legal implication, including the proposition of new 'neurorights', including mental privacy and integrity, In S. O'Sullivan, H. Chneiweiss, A. Pierucci and K. Rommelfanger, *Neurotechnologies and Human Rights Framework: Do we need new Human Rights?*, available online: https://rm.coe.int/rapporteur-report-neurotechnology-final-e-2758-7638-0166-1/1680a90ae0 Report, OECD and CoE, 9.11.2021, p.33 , a state of the art and legal aspects of neurotech is discussed.
[12] See Hasnul et al., 2021, Electrocardiogram-Based Emotion Recognition Systems and Their Applications in Healthcare, available online: https://www.mdpi.com/1424-8220/21/15/5015.

– an AI system comparing facial images, DNA, or fingerprints from a known deceased individual, coming from official register, including police records.

(124) AI systems intended to be used to search for objects that do not make use of biometric data to track the movement of a suspect, e.g. searches based on number plates, specific clothes, weapons, background, etc., will not be classified as high-risk pursuant to point 1(a) of Annex III AI Act.

Examples with regard to the element of biometric data:

– An AI system inferring emotions of an individual from key stroke (way of typing), facial expressions, body postures or movements is based on biometric data.

– An AI system following a person with a red scarf or a blue jacket is not based on biometric data.

– An AI system used in supermarkets to detect whether a product is being put into a basket, cart or into a bag is not based on biometric data when it only performs object recognition. The same is true for a system used at train stations or airports that detects suspicious objects.

– An AI system inferring emotions from typed text (content, sentiment analyses or stylometry) to define the style or the tone of a certain article is not based on biometric data.

(125) The AI Act's definition of biometric data is broad and includes any biometric data used for biometric identification, biometric categorisation, emotion recognition or other purposes. Contrary to the definition of biometric data in the EU data protection law, including Regulation (EU) 2016/679 ('GDPR'), Directive (EU) 2016/680 ('LED') and Regulation (EU) 2018/1725 ('EUDPR'), the definition of biometric data in the AI Act does not include the wording 'which allow or confirm the unique identification' (the functional use of biometric data), since it aims to cover AI systems that use biometric data not only in cases where the AI system identifies an individual or confirms its identity as specified in Recital 14 AI Act.

ii. Interplay with prohibited practices

(126) The use cases listed in point 1 of Annex III should be considered in the light of the AI practices prohibited by Article 5(1)(f), (g), (h) and (2) to (5) AI Act. That is because, in specific instances where all the conditions for one or more prohibited practices under Article 5 AI Act are met, the placing on the market, putting into service and use of the AI system is prohibited. It will then be unnecessary to consider whether those systems should be classified as high-risk. Most AI systems that fall under an exception from the prohibitions provided in Article 5 AI Act will qualify as high-risk.

For example, emotion recognition systems, where they do not fulfil the conditions for the prohibition of Article 5(1)(f) AI Act, will fall within the use case of point 1(c) of Annex III AI Act and be classified as high-risk pursuant to Article 6(2), insofar as the conditions under Article 6(3) AI Act do not apply. In particular, emotion recognition systems outside the areas of workplace and education institutions, as well as such systems used in the areas of workplace and education institutions, when used for medical or safety reasons, are not prohibited, but qualify as high-risk.

Similarly, biometric categorisation systems that do not fulfil the conditions for the prohibition of Article 5(1)(g) AI Act will fall within the use case of point 1(b) of Annex III and be classified as high-risk pursuant to Article 6(2) AI Act, where they are intended to be used for biometric categorisation according to sensitive attributes or characteristics protected under Article 9(1) GDPR (insofar as the conditions of Article 6(3) AI Act do not apply).

In contrast, RBI systems that fall within the use case of point 1(a) of Annex III AI Act may in some cases be prohibited if they fulfil the conditions for the prohibition under Article 5(1)(h) AI Act, i.e. they are being used in real-time, at publicly accessible places, for law enforcement purposes, and without one of the exceptions applying. Conversely, RBI systems that fall under one of the exceptions of Article 5(1)(h) AI Act[13] will be classified as high-risk under Article 6(2) AI Act, as will RBI systems that are not used for law enforcement purposes or not in real time.

3.1.2. Point 1(a): Remote biometric identification systems

(127) Point 1(a) of Annex III classifies RBI systems as high-risk. Such systems are deemed worthy of high-risk classification, since technical inaccuracies in the system may lead to biased results and entail discriminatory effects (especially on the grounds of age, ethnicity, race, religion or belief, gender, sexual orientation or disabilities) and RBI may lead to the feeling of surveillance and have a chilling effect on the exercise of fundamental rights, such as the freedom of expression and the freedom of assembly and association.

(128) The two subsections below describe (i) the scope of the high-risk use case point 1(a) of Annex III and (ii) the requirements for authorisation of certain law enforcement uses of post RBI systems under Article 26(10) AI Act.

3.1.2.1. Remote biometric identification system

(129) Article 3(41) AI Act defines an RBI system as '*an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database*'. An AI system must therefore fulfil three conditions to be classified as an RBI system: (i) its purpose must be biometric identification; (ii) that identification must occur without the active involvement of the person concerned, typically at a distance; and (iii) the system must perform a comparison between that person's biometric data and biometric data contained in a reference database. Each of these conditions is described in more detail in subsections below.

i. Biometric identification system

(130) Biometric recognition systems can be used for verification (authentication) and identification purposes[14]. Such systems always rely on biometric data to perform such verification and identification. They detect, capture, and transform measurable physiological and physical

[13] The exceptions set out in Article 5(1)(h)(i)-(iii) AI Act aim to allow the use of certain AI and investigative tools for law enforcement purposes: (i) the targeted search of victims of three specific serious crimes and missing persons [protection]; (ii) the prevention of imminent threats to life or physical safety or a genuine threat of terrorist attacks [prevention]; and (iii) the localisation or identification of suspects and offenders of certain serious crimes as listed in Annex II AI Act [prosecution/investigation].

[14] As defined in Article 3(36) AI Act, and agreed by the biometrics community in ISO/IEC Standard 2382-37:2022 Information Technology - Vocabulary, Biometric recognition, Term 37.01.03.

characteristics (such as eye distance and size, nose length, etc.) or behavioural characteristics (such as gait or voice) into machine-readable biometric data (see Section 3.1.1.i) above). Those data are available in different forms (images or templates), which are a mathematical representation of the salient features of an individual, used for verification and identification purposes.

(131) Article 3(35) AI Act defines 'biometric identification' as '*the automated recognition of physical, physiological and behavioural or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database.*' Such identification can be done for a variety of private or public sector purposes. Regarding law enforcement, such identification is typically done in view of an action or decision to be taken by either administrative, law enforcement or judicial authorities.

(132) This definition excludes systems whose intended purpose is not to establish the identity of a natural person and systems which do not compare the biometric data of a natural person to biometric data stored in a database. Processing of biometric data that is not done for the purpose of identifying persons do not constitute biometric identification (e.g. collecting additional information or establishing links between criminal cases based on biometric samples).

(133) AI systems may be used for biometric identification in all stages of activities. For example, biometric identification includes 'initial identification' as used in Article 26(10) AI Act (see Section 3.1.2.2. below). Biometric identification can also cover establishing the identity (including, but not limited to, the civil identity) of a natural person whose identity is already known or previously verified by a human.

(134) An AI system that locates an individual does not necessarily constitute an RBI system. Where the system does not rely on biometric features to locate a person (or there is no comparison of the biometric data of that person with biometric data stored in a reference database), that system will not be classified as high-risk pursuant to point 1(a) of Annex III AI Act.

For example, the following AI systems are not considered biometric identification systems:

- AI systems automatically searching for non-biometric identifiers (including logos on clothing, specific items).
- Automated number plate recognition (ANPR) systems when used for locating a motorised vehicle by the means of the car number plate, by the shape, the make or the colour of the vehicle, related to a person of interest (e.g. missing persons, persons suspected of having committed a crime, subject to a European arrest warrant).
- AI systems automatically searching occurrences of the validation of the individual's transport tickets (e.g., to establish the movements of the suspect). The 'tracking' is done based on the individual's validations of a ticket/subscription and not based on biometric data.
- AI systems used to geolocate a picture involving criminal activities (such as CSAM) based on background or unique identifiers in the picture excluding biometric data.

(135) By contrast, AI systems intended to be used to track natural persons (e.g., to determine the direction in which a suspect is moving or escaping in the view of taking a possible coercive action) are covered by the definition of biometric identification, provided the ability to track a person relies on a biometric data and a comparison is made of the biometric data of that person with biometric data stored in a reference database. This conclusion can be deduced from the meaning of Article 5(1)(h)(iii) AI Act and Article 26(10) AI Act. Article 5(1)(h)(iii) AI Act allows the use of real-time RBI for the tracking of suspects of crimes. Article 26(10) AI Act refers to the targeted search of a person suspected or convicted of having committed a criminal offence (see also Section 3.1.2.2. below), provided all other conditions for such use are met (see also Section 3.1.2.2. below).

For example, the following AI systems are considered biometric identification systems:

- Automated comparison of biometric identifiers (combination of face, height, frame, hair / eye colour, gait allowing the unique identification of a person) of one or several persons suspected of committing a crime with a live CCTV stream (when exempted from prohibitions in Article 5(1)(h) AI Act under one of the limited exceptions) or with CCTV recordings analysed after the crime and matched against a reference database of biometric templates of known convicted criminals.

- An AI system that uses gait recognition to compare the known fugitive's stored biometric gait profile of an individual against CCTV footage feeds collected from main transport hubs close by to track the individual after a first detection on the reference material.

- An AI system is deployed during a major event (e.g., sport event, political gathering) to detect the presence of specific known individuals linked to terrorist groups in specific sites using biometric data stored in law enforcement systems (when exempted from prohibitions in Article 5(1)(h) AI Act under one of the limited exceptions).

(136) AI systems that are intended to be used for biometric verification fall outside the scope of the high-risk classification[15]. Biometric verification (including authentication) consists of comparing biometric data presented at a sensor with another set of previously provided biometric data stored on a device, such as a smartphone, a passport, or an ID card or stored in a database in an encrypted form while the decryption key is solely stored at the individual's end, e.g., on a smartphone (one-to-one verification). The sole purpose of biometric verification is to confirm that a specific person is who they claim to be.

For example:

- An AI system that compares an image of a traveller's face (facial image) captured at an automated border control gate with the facial image stored in their passport's chip to confirm that the holder is the legitimate document owner would not be considered RBI system. If, however, within the same scenario the biometric data of the traveller captured

[15] Annex III, point 1(a) AI Act.

at the border is in addition to the verification purpose simultaneously compared against a criminal database, for example by Interpol, this would be RBI.

- An AI system comprising a mobile fingerprint scanner used to compare a live fingerprint against fingerprint templates stored on the persons' electronic ID card or driver's license for the purposes of checking their identity (e.g., a municipal employee or law enforcement officer requests individuals to place their finger on a mobile fingerprint scanner to verify their identity). Such system would not be considered an RBI system.

ii. Remoteness

(137) According to Article 3(41) AI Act, remoteness implies the ability of an AI system to identify an individual without their active involvement, typically at a distance.

(138) Point 1(a) of Annex III explicitly excludes from high-risk classification AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be. As clarified in Recital 15 AI Act, this may include a biometric system that confirms the identity of a natural person for the purpose of allowing them to have access to a service, unlock a device, or have security access to premises[16].

For example, the following would not be considered an RBI system

- An AI system using face scanning technology to admit entry to a restricted area (e.g. power plant premises): such a system compares the face of the individual presented at the entrance camera with a reference image contained in a reference database of persons allowed to enter the building (one-to-many).

- An AI system using smartphone facial authentication linked to a person's digital ID wallet to access an online police reporting portal: such a system compares the biometric sample stored in the digital ID wallet with the biometric data captured by another device to confirm the user's claimed identity before allowing the submission of the report.

(139) Recital 17 AI Act clarifies that the exclusion of biometric verification and authentication systems from the definition of RBI systems is justified by the fact that such systems are likely to have a minor impact on the fundamental rights of natural persons, as compared to RBI systems, which may be used for the processing of the biometric data of a large number of persons without their active involvement. That recital further clarifies that RBI systems are typically used to perceive multiple persons or their behaviour simultaneously to facilitate the identification of natural persons without their active involvement.

(140) For active involvement to be present, it is insufficient that persons on whom a biometric identification system is used are informed of such use. Rather, they need to actively participate in its use, for example, by actively and consciously presenting themselves in front of a sensor that is installed in a way to foster active participation.

[16] E.g. Ross A, Jain AK (2015) 'Biometrics, Overview' in Li S.Z. and Jain A.K. (eds) Encyclopedia of Biometrics, (1st ed. Springer Science, New York), pp. 289-294.

For example,

- An AI system used to give access to a metro station, such as biometric metro tickets, whereby persons are actively involved and consciously approach the biometric sensor to obtain access, does not fulfil the condition of remoteness.

- In contrast, an AI system used in cameras installed on the walls or ceilings of metro stations for surveillance purposes fulfils the condition of remoteness, since the persons on whom the system is used are not actively involved in their identification process.

- An AI system used for law enforcement purposes using the biometric data of a person included in evidence taken from a crime scene (e.g., finger latent) without the presence of that person (or with their presence, but where the person is unconscious) does not constitute active involvement.

- Following an arrest, a suspect is taken into police custody. In accordance with applicable national criminal procedural law, officers capture the suspect's facial photograph as part of the standard custody processing procedure, uses an AI system to compare a 'mugshot' taken during this formal identification procedure against a database of biometric templates. The system does not qualify as an RBI system as it is not remote (there is active involvement of the suspect).

- An AI system used by law enforcement whereby a witness offers to verify their identity by capturing their fingerprint and comparing it solely against the biometric template stored on the person's electronic ID card constitutes active involvement.

- An AI system used by a public authority to check the identity of individuals through facial recognition, against a predefined watchlist of persons suspected of involvement in terrorism. The AI system is used for the purposes of granting them entry to a restricted and fenced security perimeter within an otherwise publicly accessible space (e.g. a city square) during a major public event. Individuals wishing to enter the secured perimeter are informed in advance, through visible notices and public communication, that entry is subject to biometric checks and the facial recognition scanner is positioned to require conscious participation (e.g. standing within a marked capture zone and facing the sensor) to gain entry to the secured area. Such involvement would be considered active involvement.

(141) Biometric identification systems that process (also contactless, i.e., without physical contact) fingerprints, gait, voice, DNA, keystrokes and other (biometric) behavioural signals may also constitute RBI systems, provided they fulfil the condition of remoteness described above[17]. Palm scanning systems will mostly constitute biometric verification or authentication systems. However, in certain cases, palm scanning systems may also be used for identifying a suspect, for example when comparing child sexual abuse material to see whether the same offender is involved.

For example, the following biometric identification can be considered remote:

[17] EDPB-EDPS, Joint Opinion 5/2021, p. 11; Council of the European Union, 'Opinion of the Legal Service', 12302/22, 12 September 2022, paragraph 33, and Recital 15 AI Act.

- A biometric identification technology system that captures voice samples may be deployed on a person who is speaking by using a microphone to collect a biometric sample.
- A gait recognition system may be used via closed-circuit television (CCTV) and the videos automatically checked for matches with previously captured templates.
- Keystroke biometric technology may be used for finding a person typing a fraudulent message by matching the person's distinctive typing rhythm with previously captured keystroke templates.

(142) Body-cams used by individual law enforcement authorities for the purposes of, for example, the untargeted filming of a demonstration with hundreds of participants, will be considered to fulfil the condition of remoteness. RBI systems used in the virtual space may also be considered to fulfil that condition where the system typically functions at a distance without active involvement.

iii. Reference database

(143) Biometric identification is not possible without a reference database containing biometric data for comparison purposes for identifying natural persons. Thus, the existence of a reference database is indispensable to perform remote biometric identification of a person. A reference database may consist of biometric data of one or many individuals.

(144) Biometric identification against a reference database requires that the comparison is carried out against all data records containing biometric references[18].

For example,

- The Automated Fingerprint Identification System of SIS (SIS-AFIS)[19] database could be used as a reference database to carry out dactyloscopy searches.
- A national missing persons database could be used as a reference database for facial recognition in case of missing persons.
- A private company's voice database could be used as a reference database.

a) Practical examples of AI systems falling within the high-risk use case of point 1(a)

- **Facial/voice recognition for media archives:** AI-enabled facial and voice recognition technology intended to be used to identify selected individuals (e.g., public figures) from

[18] In line with ISO/IEC 2382-37.

[19] Article 42, 43 of the Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU and Article 32, 33 of the Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006.

audiovisual content by comparing that content against a reference database, such as media archives maintained by public broadcasters and national audiovisual repositories, without the individuals' active involvement.

- **(Voice)print matching in databases:** AI-enabled solutions intended to be used to analyse recordings or voiceprints to identify individual speakers, by comparing their biometric data against an established database of known individuals and voiceprints without their active involvement.

- CCTV **cameras installed in the walls and/or ceilings of a stadium (post remote):** If an incident happens during a match, the captured biometric data (i.e. facial images) is compared to a biometric database to identify offenders, without the active involvement of visitors to the stadium.

- An **AI system intended to be used to identify, from an image taken from a CCTV camera installed on private property, an individual suspected of carrying out a burglary and operating without their active involvement**. Unlike the prohibition in Article 5(1)(h) AI Act, the high-risk use case listed in point 1(a) of Annex III is not limited to RBI in publicly accessible spaces.

- **AI systems intended to be used to compare child sexual abuse material (CSAM) found on the Internet** to an established national or international database of suspects containing facial images and tattoos to identify an offender without their active involvement.

- **An investigation requiring the identification** on the internet, via backwards search (reverse image searches), **of a terrorist living undercover**, without his or her active involvement: A reference database can be a transformation of biometric template(s) taken from information available on the website or the Internet in general.

- **An AI system intended to be used to compare attributes in a picture, e.g., taken from the Internet or CCTV, with pictures taken from the Internet and indexed in a database** (a reference database can be a transformation of biometric template(s) taken from information available on the website or generally the Internet) to identify the person in the picture without their active involvement.

b) Practical examples of AI systems falling outside the high-risk use case of point 1(a)

- **A CCTV facial recognition system at the entry to a stadium to detect blacklisted individuals forbidden to enter the stadium via direct access control**: such a system would not fulfil the condition of remoteness, because natural persons need to actively participate, i.e., actively step in front of the AI system to get access to the stadium.

- **AI systems intended to be used for biometric verification (authentication) or for identification that is not remote, such as:**

    - AI based solutions to unlock a smartphone.

- AI-based solutions to streamline the onboarding experience for the purposes of identifying traders.
- AI-based solutions for the authentication of online exam proctoring (so-called remote proctoring).
- AI-based solutions to streamline access to a service (e.g., logging in to a bank account online (login authentication) or calling customer service of a bank to receive information about specific transactions).
- AI-based solution to carry out verification of identity during a roadside check by law enforcement. Officer uses a mobile device to compare the person's live fingerprint solely against the fingerprint stored on the ID card to verify the person's identity.

– **AI systems for smart homes/residential areas:** An AI system intended to be used to authenticate or verify the identity of an individual to give access to a home or residential area by scanning facial images, irises, voice (voiceprint identification), or fingerprints at the entrance and which grants access after a successful check against a reference database made up of biometric data which the relevant individual agreed to register, would be considered to be for biometric verification purposes and would not be considered to fulfil the condition of remoteness (the individual agreed to register and consciously presents themselves at the entrance).

– **Smart corridor AI biometrics system:** an AI system that captures the facial images of individuals from several angles in a short corridor or passage and compares those images against a biometric database of persons that have registered with the system through which those persons can enter a concert, stadium, major public event at a city square, etc., without stopping, whereas unregistered persons are approached and ejected by security staff or by automatic door systems, depending on the application. Such systems are used solely to gain access to a service/premises and persons that registered would be considered to actively participate in the identification.

– **AI systems intended to be used to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having secure access to premises**: e.g., an AI-enabled facial recognition system to contol access to hazardous areas (e.g., used in industrial settings to grant or deny access to machinery or areas with elevated safety risks); an AI-based solution to control physical access to secure areas within a corporation's office buildings; an AI biometric system for secure facility access used in critical electricity infrastructure or seaport/river port facilities (employees/authorized personnel only).

– **AI systems that make use of biometric data, but which are not intended to be used for biometric identification**: e.g. an AI system that uses a voice sample collected with the individual's active involvement to carry out language/dialect analysis in order to identify the country and region from where a person originates in the context of migration and asylum processes. The aim of such a tool is not to identify the person. Rather, a voice sample is matched against a pool of accredited voice samples to substantiate country of origin. However, see Section 3.1.3 on Point 1(b) and Section 3.7 on Point 7 of Annex III below.

- **AI systems filtering seized material to structure its content:** e.g. the AI system filters the seized footage, e.g., 100 000 files, in preparation for the evaluation of the seized evidence, e.g., whether there is a child present in a photo or not.

- **AI systems used by law enforcement authorities to analyse crime scenes**: All kinds of material are collected from a crime scene including CCTV, witnesses' material, etc. The objective is to gain investigative insights in what has exactly happened by analysing occurrences of persons and objects (e.g. via clustering, tracking or localisation based on objects such as cars, number plates, clothes, bags, weapons, drugs, and possibly as well for faces, tattoos and birthmarks). Persons are not matched against external databases, i.e. their identity is not established; and only material that has a direct link to the crime place is being used. This is the work-step prior to initial identification, and even if there might be a comparison of faces involved, in view of the closed dataset this would not yet be subject to the high-risk classification under Article 6(2) and Annex III, point (1)(a) AI Act.

- **AI systems that use multispectral imaging** to capture information from the surface and sub-surface (dermis) of the skin (collecting of biometric data) to capture fingerprints without carrying out biometric matching against a reference database.

- **AI systems used solely for cybersecurity and personal data protection purposes**: e.g. AI systems with the sole purpose of anonymising personal data, such as biometric systems which are intended to be used solely for the purpose of enabling cybersecurity and personal data protection measures as indicated in Recital 54 AI Act.

- **AI systems that use cameras (e.g., satellite, infrared/thermal) to detect the presence of humans, such as:**

    - AI systems that provide information on seat occupancy in trains or counting people: the AI system uses infrared thermal cameras installed on the ceiling in the train compartment; captures the temperature for each of the seats; and analyses the data and provides updates to the passenger via website/mobile application.

    - AI systems that are used to detect people on tracks (trespassers) to prevent accidents and damages to the infrastructure: the AI system uses infrared thermal cameras installed around rail tracks, in front of the train, etc.; alerts driver/security team that there are trespassers.

    - AI systems using images or recordings of specific spaces captured by cameras carried by drones/satellites to verify whether there are any humans present in those spaces based on non-biometric data (e.g., unusual motions, radio frequency signals emitted by the electronic device carried by humans) in the search for missing people (e.g., people lost in vast uninhabited spaces, for instance large forests). Although such AI systems can be used to identify individuals, they do not involve biometric data.

    - AI systems that use infrared thermal cameras to detect the presence of humans are not classified as high-risk AI systems because their purpose is not to identify

individuals, but instead to detect the mere presence of humans[20]. In addition, such systems do not rely on biometric data.

- **AI systems that do not track an individual on the basis of biometric data**: e.g., law enforcement uses AI video analytics tools to track a fleeing suspect across cameras based on clothing colour and body outline, without extracting or matching biometric features.

- AI-based large data processing systems used by law enforcement to cross-check and identify links between various criminal cases on the basis of facial imagery without using biometric data to identify the common suspects.

3.1.2.2. Authorisation requirement for certain law enforcement uses of post RBI under Article 26(10) AI Act

(145) Article 26(10) AI Act consists of seven subparagraphs that concern three specific situations[21]. Subparagraphs 1 and 2 contain a specific authorisation requirement for deployers of post-remote biometric identification (post-RBI) systems used for the targeted search of a person suspected or convicted of a crime in the framework of an investigation. Subparagraphs 3 to 6 contain general rules and procedural requirements directed at deployers of any high-risk post-RBI system used for any law enforcement purpose, including for the remote identification and localisation of offenders, the search for missing persons, and the prevention of crimes. Subparagraph 7 authorises Member States to introduce more restrictive laws on the use of post-RBI.

a) Subparagraphs 1 and 2 of Article 26(10) AI Act

(146) The use of a high-risk AI system for post-RBI for the purpose of law enforcement, **in the framework of an investigation for the targeted search** of a person suspected or convicted of having committed a criminal offence, requires the deployer (generally, a law enforcement authority) to ask for an **authorisation by a judicial authority or by an administrative authority** whose decision is binding and subject to judicial review. The authorisation requirement does not apply to all RBI systems classified under Point 1(a) of Annex III AI Act. As mentioned above, the scope of its application is narrowed down to specific situations in the framework of an investigation for the targeted search for law enforcement purposes.

(147) The term 'targeted' in 'targeted search' relates to the question whether the law enforcement authority has reasonable cause to suspect a connection between a suspect and a crime and is therefore searching for that suspect. Once this has been established, the law enforcement authority may use the most efficient RBI search method in view of the concrete situation. It may run, for example, probe or gallery searches, depending on the concrete circumstances. The term 'search' in

[20] However, in the context of migration, asylum and border control management, an AI system that uses infrared thermal or satellite imaging to detect people crossing a border in an unauthorised place would fall under the use case of point 7(d) of Annex III AI Act (Section 3.7.5 below).

[21] Beyond the specific deployer obligations under Article 26(10) AI Act, any high-risk post-RBI system also needs to comply with the requirements for high-risk AI systems and all obligations applicable to providers who place them on the market or put them into service, other obligations on the deployer, such as human oversight and monitoring etc. (Article 26), the obligation to conduct Fundamental Rights Impact Assessment (Article 27) or to provide for a right to an explanation of decisions (Article 86) also apply. These other obligations and requirements will be clarified in other set of guidelines that the Commission is preparing in 2026.

'targeted search' relates to the objective of identifying the location in time and place of the targeted individual.

(148) A search for a person may be targeted whether the identity of the person is known or unknown. A search can be considered targeted where there is a reason to search for a specific person. The suspect must be directly linked to a criminal offence as a suspect or convict.

Example of targeted searches:

- Following an armed robbery, investigators obtain CCTV images and identify a known individual, already present in police records, as the prime suspect. Authorities run a post-RBI query using the suspect's facial template to determine whether the person appears in footage from nearby transport hubs at that moment. The search is targeted as the search is narrowly focused on the one individual, and there is a direct link to a concrete criminal offence.

- A witness to a kidnapping provides investigators with video showing the suspect's face. Police extract a biometric template from the footage and run a post-RBI search to determine whether that same individual appears in footage captured by other cameras along the suspected escape route.

On untargeted search see paras. 159-160 below.

(149) The initial identification of a potential suspect, based on objective and verifiable facts directly linked to an offence, is excluded from the authorisation requirement under Article 26(10) AI Act. The AI Act does not define when a person is considered a suspect, but in the context of Article 26(10) AI Act this should be understood to mean persons who are reasonably believed by law enforcement authorities to have committed a criminal offence. The suspicion of the law enforcement authorities must be based on objective and verifiable facts. Initial identification relates to the identification of one or several potential suspects against a reference database to find out their identity or to establish the existence of a matching biometric profile in a reference database, without necessarily establishing the suspect's identity. The question is: *Who is the person (that is a potential suspect*?). Examples are the comparison of a suspect's biometric data against biometric templates of known persons, for instance from police files or EU information systems. The objective can be to find out the likely identity of the suspect (e.g. score 8/10 that this is Person A) or to find out whether the suspect has already previously committed crimes or was a suspect (this is a person whose biometric traces were already found previously at a crime scene; this is a person whose biometric profile is already on a reference database). In other words, initial identification is not necessarily aimed at establishing the civil identity of a person. In the case of initial identification, the system needs to comply with the requirements for high-risk AI systems, provided that the AI system constitutes a remote biometric identification system and therefore classifies as high-risk (see Section 3.1.2.1. above). No specific authorisation is needed for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence.

Examples of initial identification:

- After a stabbing, investigators obtain clear CCTV footage showing the perpetrator's face. Police generate a biometric template and compare it against national police and EU

databases to determine whether a matching biometric profile exists and to identify the likely person.

- Following a burglary, police extract a facial image of the perpetrators from CCTV and compare it against biometric traces previously collected from other crime scenes to determine whether the same individual may be involved in multiple offences.

- After a terrorist incident, investigators obtain video showing one perpetrator but cannot yet confirm his or her identity. Post-RBI is used against police databases to produce ranked candidate matches (e.g. 'likely person A') to which other pieces of evidence must be corroborated to identify the person.

- Searches carried out within reference databases, including police records, and public or private video surveillance camera systems, by comparing a given biometric sample of an individual, such as (a) pictures of the face, of tattoos, or any other identifiable body part, (b) gait, (c) voice, collected from the following sources and in the following situations (i) from video surveillance cameras, (ii) from human remains, whereabouts or traces notably from unknown persons, (iii) from unconscious persons, (iv) from social media, (v) from seized material, (vi) when taken in custody with coercion, (vii) from legal interception for the first identification in the context of an active search of a person. Examples of initial identification include:

- Airport authorities searching their video-surveillance camera system for the presence (the location) of a given person on the basis of pictures collected from social media, upon the request of national law enforcement authorities searching for that individual. However, upon a match in the system, further searches in the system for the individual and for the same purpose of searching this suspect are not considered to be initial identification.

- Member State B law enforcement authorities consulted by Member State A law enforcement authorities as part of a police cooperation information exchange for the first time in the context of an active search of a person suspected of having committed a crime and searching for the identity of a person in the criminal database is initial identification.

- A search carried out in another Member State's national criminal database through the Prüm II framework with latent fingerprints or latent palm prints, or with facial images collected on a crime scene, with the aim of identifying the suspect subject of an active search.

- Europol searches in Member States' database under the Prüm II framework with fingerprints or facial images received from third-country authorities for establishing the identity of the individual actively tracked until a match occurs .

- Europol, while supporting Member States active search for a given individual suspect of having committed a crime under Europol's mandate investigation comprising several ATM attacks, carries out comparisons in its own data on the basis of footage from the local surveillance camera. Such processing for identification purposes are considered initial so long as the person is not identified. Further identifications with the same sample

into Europol data and with the same purpose of searching that suspect, and potentially revealing the presence of the person in a new setting, cannot be considered initial.

(150) The authorisation for a targeted search is required when the investigation has been narrowed down from a broader number of persons of interest to a limited number of suspects and this is reflected in some formal status of an open investigation for a crime. This will normally be the case when there is a formal investigation under national law and a certain (official) procedure (of search) for the specific suspected person (who is known) is being initiated. The question is: *Where is the suspect*? Location of the person in time and place is an essential component of targeted searches carried out in the framework of investigations. The targeted search for a person in the context of Article 26(10) AI Act refers to the use of RBI systems to track an individual. For example, in the course of an investigation the law enforcement authority has considered that *Person B* is the likely offender of a crime that has taken place. A post-RBI system is being used to analyse CCTV footage and video material that was collected around the crime scene (i.e. link to the location and time of the offence) to find out where the suspect came from or went to in the view of taking possible law enforcement actions against that person with possible consequences on the rights and freedoms of the person concerned. A template with the biometric data containing a single picture or audio recording of the suspect could be considered a 'reference database' in this context and would be compared to the collected CCTV and video material.

For example, the prior authorisation by a competent judicial authority or an administrative authority pursuant to Article 26(10) AI Act would be required for:

- Repeated post-RBI queries to map movements of an identified suspect. Authorities repeatedly run post-RBI across multiple reference databases to reconstruct the movement of a suspect whose identity is already known in view of arresting that person; location in time and space of the person, even in the past, will help authorities to establish roadblocks at kilometric distance compatible with the time elapsed from the moment when the person appeared on the footage.

- Evidentiary confirmation for prosecution. Post-RBI is used specifically to produce confirmation that a known suspect appears on the crime-scene at a certain moment in a footage for evidentiary use.

(151) Targeted search includes finding out the location of concrete suspects. 'Localisation' is not a defined term under the AI Act. Localisation that is not based on biometric data is outside the scope of the AI Act's rules on biometrics, for example when following a person with a red scarf.

(152) Law enforcement authorities frequently use AI systems for the analysis of a crime scene. In such cases, the AI system is used as a screening tool for analysing large amounts of footage material for the purpose, for example, to investigate the course of events. All kinds of material are collected from a crime scene including CCTV material, etc. The objective is to gain investigative insights into what has exactly happened by analysing appearances of persons and objects. Persons are not matched against external biometric databases, and only material that has a direct link to the crime scene is being used. The use of the system is focused on understanding the movements of the persons present around the crime scene. This is a work-step prior to initial identification, and even if there might be comparison of faces or other biometric features involved, in view of the closed

dataset, this would not be considered RBI and high-risk. The same logic can be applied for AI systems used for screening child sexual abuse material (CSAM) that do not screen biometric data of individuals for identification purposes.

(153) Localisation that is based on biometric data is considered falling under the definition of biometric categorisation when persons are not being searched on the basis of biometric templates that allow their identification, but for example based on their eye or hair colour or their height (e.g. a search for a suspect described by witnesses as a skinny woman, mid-thirties, 160-165 cm, light skin, dark hair, brown eyes, leaving the surrounding of the crime scene). The AI system is sorting and filtering footage to flag persons that fall within this category. Pure searching for occurrences based on biometric characteristics – without establishing biometric templates that allows the identification is not considered RBI.

Examples of AI systems that are not considered RBIs:

- Filtering persons by hair and eye colour after a crime was committed. Witnesses describe the suspect as having dark hair and brown eyes. Investigators use AI to sort crime-scene footage to categorise persons matching these physical traits. This is not necessarily biometric identification, but may amount to biometric categorisation if the sorting is based on biometric data.

- Age-range estimation for investigative triage. An AI system groups individuals appearing in crime-scene footage into approximate age brackets to support manual review.

(154) The objective of requiring authorisation for the use of a post-RBI system for the targeted search of a person suspected or convicted of having committed a criminal offence is the need for an assessment and a decision as to whether the envisaged use of the AI system for the purpose is **strictly necessary** for finding the person in the context of the investigation of a specific criminal offence. This necessity assessment must take account of the personal, temporal and geographic scope of the targeted search and assess whether there are not less intrusive means for finding the person in question. The condition of strict necessity is assessed for each concrete case by the law enforcement authority intending to deploy the system. The authorisation request can be linked to the opening of an investigation or the request for other surveillance measures according to national law to streamline procedures.

(155) According to Article 26(10), subparagraph 1, AI Act, the request must be made ex ante or without undue delay and no later than 48 hours after starting the use of the post-RBI system.

(156) The authorisation must be requested from a judicial authority or an administrative authority whose decision is binding and subject to judicial review. The obligation to request an authorisation solely applies to the targeted search of a person suspected or convicted of having committed a criminal offence in the framework of an investigation. This excludes, for example, the targeted search for missing persons or victims (no authorisation is needed) or searches outside the framework of an investigation of a crime (e.g., law enforcement use a biometric template of a known child sexual abuse victim to identify whether images/videos featuring the same child come up in other unrelated reports of child sexual abuse or to search for the appearances of a picture of a witness of a crime scene in an indexed version of social media, e.g. scraped material, on the basis of the witness driver's license mugshot). Depending on national law, the authoritsation granted by the judicial

authority or administrative authority may concern a particular person or a specific group of persons suspected of having committed or convicted of concrete criminal offence(s) in the context of a specific investigation. It may not be necessary to know the civil identity of the person(s).

(157) The authorisation procedure required by Article 26(10) AI Act can be designed with sufficient flexibility to also cover unforeseeable operational scenarios and the screening of large data volumes, for example CSAM. In case of CSAM the search for victims would not be subject to an authorisation requirement. Neither would the sorting and filtering of data be relevant. The authorisation requirement would apply only in the case of a specifically targeted search against a concrete suspect (unless it is an initial identification). Without prejudice to the independence of the judiciary and to national procedural law and practices, and to facilitate the implementation of this requirement and make it operational, Member States could consider relying on the judicial authorisation procedures that are currently established for compliance with other Union or national laws, e.g., concerning an authorisation for the interception of communications.

(158) If the requested authorisation is rejected, the use of the post-RBI system shall be stopped with immediate effect and the personal data linked to the use of the high-risk AI system for which the authorisation was requested must be deleted. This does not imply that a standard reference database is to be deleted, but only personal data that is specific to the investigation. This requirement applies to the results of the processing of CCTV or video material, such as biometric profiles and identifications or links made through comparison of the material with reference data. It does not apply, for example, to the CCTV material itself, where this material has been lawfully obtained.

(159) In no case shall post-RBI be used for law enforcement purposes in an untargeted way, without any link of a specific person to a criminal offence, a criminal proceeding, a genuine and present or genuine and foreseeable threat of a criminal offence, or the search for a specific missing person (Subparagraph 3). That applies universally, also to cases of post RBI use of systems for law enforcement purposes when there is no requirement for an authorisation for the targeted search of persons in the framework of an investigation as set out under Article 26(10), subparagraph 1, AI Act.

(160) Recital 95 AI Act further specifies that '[p]*ost-RBI systems should always be used in a way that is proportionate, legitimate and strictly necessary, and thus targeted, in terms of the individuals to be identified, the location, temporal scope and based on a closed data set of legally acquired video footage. In any case, post-RBI systems should not be used in the framework of law enforcement to lead to indiscriminate surveillance. The conditions for post-RBI should in any case not provide a basis to circumvent the conditions of the prohibition and strict exceptions for real time remote biometric identification.*' Use cases are different and depend on the concrete situation. Compliance with the condition of strict necessity for the investigation of a specific criminal offence must be assessed and demonstrated by the law enforcement authority intending to deploy the system. This can also apply to intelligence operations, if they are carried out for the purpose of law enforcement and are not exclusively for national security purposes.

Examples of untargeted searches include:

- Police run facial recognition across all persons appearing in city-center CCTV over a weekend, without searching for a specific person in mind, to detect possible offenders.

- Police deploy a post-RBI system after a public demonstration happened to scan all persons appearing in footage from a public square where the demonstration took place, without having previously identified a specific suspect or concrete individual linked to an offence.

- Authorities regularly check public space (e.g. transport hubs) video feeds using facial recognition to detect any persons of potential interest, without a time-bound or crime-linked investigative purpose.

b) Subparagraph 3 of Article 26(10) AI Act

(161) Article 26(10), subparagraph 3, AI Act provides that no decision that produces an adverse legal effect on a person may be taken by the law enforcement authorities based solely on the output of a post-RBI system. This restriction comes on top of the requirement under Article 14 AI Act for human oversight. Further analysis to inform a decision can, for example, relate to the question whether a given person has been at a different place or also whether there are other reasons why the person cannot be the subject of a search[22].

c) Subparagraph 4 of Article 26(10) AI Act

(162) Article 26(10), subparagraph 4, AI Act confirms that the requirements in Article 26(10) AI Act are without prejudice to Article 9 of Regulation (EU) 2016/679 and Article 10 of Directive (EU) 2016/680 for the processing of biometric data.

d) Subparagraphs 5 and 6 of Article 26(10) AI Act

(163) According to Article 26(10), subparagraphs 5 and 6, AI Act, deployers of post-RBI systems must document each use of such systems in the relevant police file and make the documentation available upon request. Furthermore, they must proactively submit annual reports (that may be aggregated to cover more than one deployment) to the relevant market surveillance authority and the national data protection authority, excluding the disclosure of sensitive operational data related to law enforcement.

e) Subparagraph 7 of Article 26(10) AI Act

(164) Pursuant to Article 26(10), subparagraph 7, AI Act, Member States may introduce, in accordance with Union law, more restrictive laws on the use of post-RBI systems.

3.1.3. Point 1(b): Biometric categorisation

(165) Point 1(b) of Annex III classifies as high-risk AI systems intended to be used for biometric categorisation according to sensitive or protected characteristics based on the inference of those attributes or characteristics. Such systems are deemed worthy of high-risk classification since they

[22] More details on human oversight in the context of RBI under point 10.2.2.5. of the Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) (OJ L, 2024/1689).

involve the processing of additional sensitive personal data and pose significant risks to other fundamental rights of natural persons, such as the right for private and family life, non-discrimination, and human dignity.

(166) Article 3(40) AI Act defines a biometric categorisation system as '*an AI system for the purpose of assigning natural persons to specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons*'. The biometric categorisation of an individual by an AI system is thus typically the process of establishing whether the biometric data of an individual belongs to a group with some pre-defined characteristic. It is not about identifying a specific individual or verifying their identity, but about assigning an individual to a certain category. The notion of 'biometric data' is explained Section 3.1.1. above.

(167) Biometric categorisation may rely on categories of physical characteristics (e.g. facial features and form, skin colour) based on which persons are assigned to specific categories. Biometric categorisation may also be based on DNA or on behavioural aspects, such as keystroke analysis or a person's gait[23]. Biometric categorisation excludes categorisation according to clothes or accessories, such as scarfs, hats, gloves, watches or crosses, as well as social media activity.

(168) If a system is '*ancillary to another commercial service and strictly necessary for objective technical reasons*' it will fall outside the scope of the definition of biometric categorisation systems. Recital 16 AI Act explains that a purely ancillary feature is a feature that is intrinsically linked to another commercial service, meaning that the feature cannot, for objective technical reasons, be used without the principal service, and the integration of that feature or functionality is not a means to circumvent the applicability of the rules of the AI Act.

i. According to sensitive or protected attributes or characteristics

(169) According to point 1(b) of Annex III AI Act, only AI systems intended to be used for biometric categorisation according to sensitive attributes or characteristics will be classified as high-risk, in so far as those systems are not prohibited under the AI Act. Recital 54 AI Act clarifies that sensitive attributes or characteristics are those protected under Article 9(1) GDPR. They include attributes and characteristics on '*racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*' The placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems 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 are prohibited by Article 5(1)(g) AI Act. Therefore, the attributes and characteristics of ethnic origin, genetic data, and data concerning health are here of key relevance.

ii. Biometric categorisation must be based on the inference of those attributes or characteristics

(170) To be classified as high-risk, the AI system must use biometric data to infer a sensitive or protected attribute or characteristic and then classify the individuals according to that attribute or that

[23] See e.g., the Article 29 Working Party, *Opinion 3/2012 on developments in biometric technologies*, WP193, 27.4.2012, pp.16-17. The Group refers here to 'soft recognition' (p. 17), i.e. 'detection of behaviour or specific needs of people'.

characteristic. This means that biometric data must be used as an input, while a sensitive or protected attribute or characteristic is the output of the AI system inferred from the biometric data.

a) Practical examples of AI systems falling within the high-risk use case of point 1(b)

- **An AI system to categorise patients**. The AI system is used to detect early symptoms of diseases that manifest themselves in mobility issues. The AI system captures patients' gait, infers their health data based on captured gait data, and assigns those individuals to pre-defined categories (e.g., early stages, advanced stages of diseases).

- **AI system to categorise passengers**. The AI system is used in cameras installed at the airport to analyse passengers' movement between terminals. The AI system captures travellers' biometric data (e.g., gait, facial templates), infers biometric identifiers based on these captured data, and uses them to assign travellers into a category. Initial categorisation is based on inferred biometrics, e.g., ethnic origin. These categories are used, for example, to generate aggregated passenger profiles (e.g., solo passenger, passengers travelling as a family) or to support targeted operational measures.

b) Practical examples of AI systems falling outside the high-risk use case of point 1(b)

- **AI system to categorise foreign persons crossing the EU border**. The AI system is used in cameras installed at border crossing points and captures facial images to infer foreigners' age and gender. The system is not high-risk because attributes such as age and gender are not considered as sensitive or protected under Article 9(1) GDPR. If age and gender are collected for the purposes of assessing the risk posed by foreigners entering into the EU territory, the AI system could be qualified as a high-risk system under point 7 (b) of Annex III, AI Act.

- **AI system to categorise customers based on their gender to offer/improve personalised experience for customers**. The AI system captures keystrokes, analyses them to assign a gender to the customer to offer/improve personalized experience (e.g., personalised advertising). The AI system deploys biometric categorisation (assigns a customer to a certain category based on their biometric data). However, the AI system infers gender, which is not a sensitive or protected attribute or characteristic under Article 9(1) GDPR.

- **AI systems intended to be used for age estimation**. The AI system prevents minors from, e.g., (i) accessing online harmful content, (ii) accessing age-restricted services (such as online betting, personal loans, credit cards, investment platforms, mobile payment wallets), (iii) accessing physical premises not appropriate for children, or (iv) using vending machines that provide products intended exclusively for persons over a legally defined age threshold (e.g., tobacco). The AI system captures keystrokes or/and facial features through a camera and assigns individuals to a specific age group on the basis of a comparison of the captured images/keystrokes patterns with characteristics of people in certain age groups and a probability prediction. The AI system infers age, which is not sensitive or protected attribute or characteristic under Article 9(1) GDPR.

- **AI system intended to be used as a content moderation tool.** The AI system scans text/pictures to identify illegal or inappropriate content. Although the system categorises content based on specific indications (e.g., extreme content that may reveal political opinions and be considered

as a sensitive or protected attribute or characteristic), that categorisation is not made on the basis of biometric data.

3.1.4. Point 1(c): Emotion recognition

(171) Point 1(c) of Annex III classifies emotion recognition systems as high-risk. Article 3(39) AI Act defines 'emotion recognition systems' as AI systems '*for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data*'.

(172) Serious concerns exist about the scientific basis of AI systems aiming to identify or infer emotions or intentions, particularly since the expression of emotions vary considerably across cultures and situations and even within a single individual. Emotion recognition systems are intrusive and present key shortcomings that may affect individuals' fundamental rights. Among the key shortcomings of such systems are their limited reliability, their lack of specificity, and their limited generalisability.

(173) While language-based AI social companions are not specifically classified as high-risk under the AI Act, it cannot be excluded that, in certain cases, they might be intended to be used for emotion recognition (identifying and inferring emotions or intentions based on biometric data from, e.g., voice or video calls) and therefore fall to be classified as high-risk pursuant to point 1(b) of Annex III AI Act.

i. Identification and inference of emotions or intentions

(174) The identification of emotions or intentions occurs where the processing of the biometric data (for example, the voice or a facial expression) of a natural person allows to directly compare and identify an emotion or intention with one that has been previously programmed in an emotion recognition system. Inferring occurs by deducing information generated by analytical and other processes by the system itself. In such a case, the information about the emotion is not solely based on data collected on the natural person, but is inferred from other data, including machine learning approaches that learn from data how to detect emotions or intentions[24]. Inferring generally encompasses identifying (of emotions or intentions) as a prerequisite, so an AI system intended to be used for inferring emotions or intentions should be understood as also identifying emotions or intentions[25].

ii. Emotions or intentions

(175) The concept of emotions or intentions should be understood in a wide sense and not interpreted restrictively. Recital 18 AI Act provides some clarifications on this concept, listing emotions '*such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement*'. These examples are not exhaustive.

[24] See Recital 12 AI Act. Inferred data is hence also often the result of probability-based analytical (big data) processes aimed at finding correlations and finding patterns in data sets.
[25] Recital 18 AI Act.

(176) The AI Act should not be circumvented by referring to attitudes and therefore the high-risk use case in point 1(c) of Annex III includes cases where an AI system is intended to be used to find, based on biometric data, that a person is showing, for example, an angry attitude.

(177) Recital 18 AI Act clarifies that emotions or intentions do not include '*physical states, such as pain or fatigue, including, for example, systems used in detecting the state of fatigue of professional pilots or drivers for the purpose of preventing accidents*' (for example, identifying whether a person is sick is not emotion recognition). It further clarifies that emotion recognition systems do not include '*the mere detection of readily apparent expressions, gestures or movements, unless they are used for identifying or inferring emotions*'. Those expressions can be basic facial expressions, such as a frown or a smile, or gestures such as the movement of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whispering. However, when these readily apparent expressions or gestures are used for identifying or inferring emotions or intentions, they are covered by the concept of 'emotions or intentions'.

a) Practical examples of AI systems falling within the high-risk use case of point 1(c)

- **The integration of AI with body-worn cameras or remote surveillance systems (so-called police bodycams)**: e.g. AI-enhanced body-worn cameras used across patrol units that enables automated behavioural pattern detection, flagging 'aggressive posture' through gait, body posture, movement and facial analysis to assess whether an individual is likely to engage in fight during police encounters. This qualifies as an emotion recognition system because it interprets physical cues to infer an individual's emotional or mental state - in this case, anger.

- **An AI system for the gaming industry that is intended to measure a gaming experience to further improve the product (real-life gaming experience)**. The AI system tracks body posture, facial expressions, eye closures and gazes to measure the reaction of the player, including their excitement, anger, frustration, amusement; analyses the above-mentioned recorded data to identify relevant elements of the gaming experience that needs improvement. Such a system involves processing of biometric data (e.g., facial expressions which are a source of biometric data). It also identifies or infers gamers' emotions based on their biometric data. Excitement, anger, frustrations are examples of emotions.

- **An AI-based solution to maintain order during concert events.** The AI system is installed in cameras at walls or ceilings; screens the mood of the audience, e.g., voices, faces and movements; when the system finds that the mood is getting aggressive in a certain area of the stadium, more security personnel is sent to that area. The AI system is intended for emotion recognition: it screens emotions of individual participants to assess the mood of the audience.

- **An AI system used in call centres to infer emotions of customers.** The AI system analyses customers' voices and evaluates vocal tone, pitch and volume to gauge customer satisfaction level for statistical reasons, to identify the moment to route them to a human agent (e.g., anger), for troubleshooting purposes, or to enhance customer care business unit. These AI systems deduce from the customer's voice their emotions, e.g., if they are happy or angry. It does not matter whether the biometric system is intended to identify the customer.

- **Smart watch mood monitor/wearable device**. The AI system is integrated into a smart watch to measure biometric data (e.g., voice, heart rate) and monitor user emotions (e.g., sad, curious,

happy, bored) to assist users in recognising their emotional state and provide emotional improvement suggestions. Such AI systems infer user emotions, which is intrusive. It is not relevant whether the emotion recognition results are disclosed solely to the specific user.

b) Practical examples of AI systems falling outside the high-risk use case of point 1(c)

- **An AI system intended to be used by the automotive industry to help prevent accidents by detecting when a driver loses focus** (i.e., drowsiness, falling asleep, experiencing sudden health issues). The AI system tracks body posture, facial expressions, eye closures and gazes via installed cameras and motion detectors in a vehicle; analyses the collected data to alert the driver or assume control of the vehicle, and safely bring it to a stop. Such AI systems are not considered high-risk AI systems because emotions or intentions do not include pain or fatigue, which are physical states.

- **The observation of readily apparent expressions.** The mere observation that a person is smiling is not emotional recognition. A TV broadcaster using a device that allows to track how many times its news presenters smile at the camera is not emotion recognition.

3.2. Critical infrastructure

(178) Point 2 of Annex III AI Act lists as high-risk six use cases of AI systems intended to be used as a safety component in the management and operation of certain specific cases of critical infrastructure, notably critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity. Recital 55 AI Act clarifies that this classification aims to address the risk that a failure or malfunctioning of such a system could endanger the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities.

(179) However, even if certain AI systems may fall outside the scope of the critical infrastructure use case listed in point 2 of Annex III AI Act, they could still be classified as high-risk pursuant to Article 6(1) AI Act where they are regulated by Union harmonisation legislation listed in Annex I (see Section III). This may be the case, for example, for AI systems embedded in products covered by the Union harmonisation legislation listed in Annex I AI Act, such as radio equipment, cableway installations, civil aviation, or rail systems.

3.2.1. Overview of use cases and horizontal issues

Two conditions must be fulfilled for an AI system to fall within the high-risk use case listed in point (2) of Annex III AI Act. First, the AI system must be intended to be used as a safety component within the meaning of Article 3(14) AI Act. Second, that intended use must concern the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity.

i. A safety component in critical infrastructure

(180) As explained in Section III.2.2. above, the AI Act is based on a product safety-oriented legal framework. Accordingly, the classification of an AI system as a safety component in critical

infrastructure must be assessed primarily in the light of the protective function performed by the AI system itself. In the context of critical infrastructure, that assessment must focus on whether the AI system directly protects the physical integrity of the infrastructure by reducing, preventing, controlling, or mitigating risks that, if materialised, would lead to physical harm to people or physical damage to property. In critical infrastructure, the functionality of the safety component is intrinsically linked to the preservation of the physical integrity of that infrastructure.

(181) The requirement that a safety component performs a safety function excludes from high-risk classification AI systems which are merely supportive, informational, organisational or optimisation-oriented (i.e. optimise critical infrastructure's performance and operation e.g. efficiency, cost) and which do not themselves perform such a direct protective function.

(182) For example, an AI system intended to be used as a "mere conduit" function—referring to the passive conveyance of traffic or data without any control or decision-making over its content or destination—will not be classified as high-risk.

(183) **An AI-enabled traffic flow optimisation system based on real-time data collection**. Such a system is a traffic data analytics platform enabling intelligent analysis for flow optimisation functions, but does not directly trigger changes in the traffic management that may impact the safety; it does not directly protect safety or physical integrity. These systems provide insights but do not directly protect physical integrity. Traffic systems can function without it. Such a function does not have a direct and immediate impact on the physical integrity of critical infrastructure. While it may affect the availability of services, it is not inherently responsible for triggering harmful outcomes.

(184) More specifically, an AI system should be classified as a safety component in critical infrastructure only if it performs one of the following safety functions[26]:

a. the AI system is intended to be used as a component in critical infrastructure to **monitor and detect situations** which may directly lead to physical harm to natural persons or physical damage to property by directly protecting the physical integrity of the critical infrastructure (e.g. an AI system detecting abnormal behaviour in the critical infrastructure operation);

b. the AI system is intended to be used as a component in the critical infrastructure to **monitor and detect the need to schedule maintenance and inspections**, which, **if not conducted**, may directly lead to a risk to the physical integrity of the critical infrastructure and to physical harm to natural persons or physical damage to property (e.g. an AI system detecting whether physical parts of the critical infrastructure are worn and may need replacement or maintenance);

c. the AI system is intended to be used as a component in the critical infrastructure to **prevent** physical harm to natural persons or physical damage to property by directly protecting the physical integrity of the critical infrastructure (e.g. an AI system preventing critical infrastructure operations to start if abnormal behaviour is detected);

d. the AI system is intended to be used as a component in the critical infrastructure which is intended to **control or limit possible** physical harm to people or physical damage to property by directly protecting the physical integrity of the critical infrastructure (e.g. AI system

[26] For definition see Section Chapter III, 2.2.2. above.

controlling specific behaviour or function of a critical infrastructure and adjusting its function accordingly);

e. AI system is intended to be used as a component in the critical infrastructure to **mitigate consequences** of possible physical harm to natural persons or physical damage to property by directly protecting the physical integrity of the critical infrastructure (e.g. an AI system that triggers action, such as safe stop, if dangerous condition occurs);

f. the AI system is intended to be used as a component in the critical infrastructure to **control or supervise another system** that performs a safety function (e.g. an AI system that supervises an operation of another system through sensors in real time and acts as a safety component that directly performs the safety function).

(185) Components designed solely to prevent the following types of harm or damage should not be regarded as 'safety components': a) non-physical harm or non-physical and immaterial damages (such as moral harm, rights infringement); b) any damages caused by third parties, including those arising through the use of intermediation services.

(186) In practice, when assessing whether an AI system qualifies as a safety component in critical infrastructure, one should take into consideration the availability of a redundant or backup system that directly protects the physical integrity of critical infrastructure and could prevent the harm or damage from materialising.

(187) Recital 55 AI Act makes a clear distinction between a 'safety component' and a 'cybersecurity component'. To fall within the use case listed in point 2 of Annex III, an AI system must not be used solely for cybersecurity purposes. Without a direct safety role, an AI system cannot be considered a safety component in a critical infrastructure and therefore cannot be classified as high-risk under Article 6(2) AI Act.

Examples of AI systems used solely for cybersecurity purposes, thus falling outside the use case of point 2 of Annex III AI Act:

- An AI honeypot system intended to proactively identify and neutralise cyber threats on a real-time basis.
- An AI-enabled technology intended to actively engage with potential attackers to learn about new attack patterns.
- An AI system intended to support the detection of unauthorized access (i.e. affected customers are informed before their password is misused).
- An AI system intended to detect suspicious email addresses and identify stolen data.

ii. The AI system must be used by an entity identified as critical under the Critical Entities Resilience Directive

(188) For an AI system to be classified as high-risk pursuant to point (2) of Annex III AI Act, it must be intended to be used in one of the sectors of critical infrastructure listed in that provision. Point (2)

of Annex III lists as high-risk AI systems intended to be used as safety components in the management and operation of one of the following critical infrastructure areas: a) digital infrastructure, b) road traffic, or c) in the supply of water, gas, heating or electricity.

(189) To delineate the exact scope of this use case, the AI Act refers in Article 3(62) AI Act to the definition of critical infrastructure in Directive (EU) 2022/2557 on the resilience of critical entities (the 'Critical Entities Resilience' or 'CER' Directive')[27]. Article 5(1) CER Directive empowers the Commission to establish a list of essential services in the sectors and subsectors covered by the Directive. On that basis, the Commission adopted Delegated Regulation (EU) 2023/2450 (the 'CER Delegated Regulation'), which provides a list of essential services and links each of those services to the corresponding categories of entities in the Annex to the CER Directive that may be identified as a critical entity under the CER Directive.

(190) The reference in Article 3 (62) AI Act to the CER Directive should be understood in a way that an AI system is classified as a safety component in critical infrastructure (hence as high-risk) only if used by an entity identified as a critical entity by a Member State under the CER Directive.

(191) It should also be noted that this interpretation does not require the disclosure of the status of an identified critical entity to third-party AI system provider. First, third-party providers may choose to develop and place on the market AI systems that comply with requirements for the high-risk AI systems under the AI Act and are intended to be used for high-risk purposes, irrespective of the status of the prospective deployer. Second, an identified critical entity acting as a deployer may require compliance of the purchased AI system with the AI Act in procurement procedures, contractual documentation or technical specifications without disclosing that it has been identified as a critical entity under the CER Directive. In practice, entities may choose to procure AI systems meeting high-risk requirements for a variety of operational, cybersecurity, corporate governance or liability related reasons, irrespective of whether they have formally been identified as critical entities.

(192) Additionally, in reality, procurement and supply arrangements concerning the European critical infrastructure operators already frequently involve confidentiality and security safeguards that limit the disclosure of sensitive operational information to third-parties.

3.2.2. The critical digital infrastructure use case

(193) According to the approach presented in section 3.2.1.ii above, '*an AI system intended to be used in the management and operation of critical digital infrastructure*' refers to an AI system intended to be used in an asset, a facility, equipment, a network, or a system or a part of an asset, a facility, equipment, a network or a system which is necessary for the provision of the essential services established in Article 2(8) CER Delegated Regulation. This includes:

- the provision and operation of internet exchange point services *(providers of internet Exchange Points);*

- the provision of domain name system (DNS) services, excluding services related to root name servers *(DNS service providers);*

[27] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, (OJ L 333, 27.12.2022, pp. 164).

- the operation and administration of top-level domain (TLD) name registries *(TLD name registries);*

- the provision of cloud computing services *(providers of cloud computing services);*

- the provision of data centre services *(providers of data centre services);*

- the provision of content delivery networks *(providers of content delivery networks);*

- the provision of trust services *(trust service providers);*

- the provision of publicly available electronic communications services *(providers of electronic communications services);*

- the provision of public electronic communications networks *(providers of public electronic communications networks)*.

(194) An AI system intended to be used in the management and operation of critical digital infrastructure should therefore be considered as high-risk only if it is intended to be used by an entity that has been identified as a critical entity by a Member State under the CER Directive.

a) Practical example of an AI system falling within the high-risk use case of critical digital infrastructure

- An AI system used as a fire alarm controlling system in cloud computing centres , due to its direct safety function (Recital 55 AI Act). None of the exceptions listed in Article 6(3) AI Act apply to such a system due to its role in preventing direct damage to the physical infrastructure of the centre, as well as harm to natural persons.

b) Practical examples of AI systems falling outside the high-risk use case of critical digital infrastructure

- AI systems intended to be used to improve the service quality and operations of critical digital infrastructure , e.g.: AI systems used for trouble tickets management; AI systems intended to be used to optimise the network and adapt to tailored customer needs; AI-based interactions with technical user guide for network maintenance; AI systems intended to be used to predict a network load. Such AI systems should not be considered to have a direct safety function.

3.2.3. The road traffic use case in critical infrastructure

(195) Road traffic should be understood as surface roads[41] excluding waterways. According to the approach presented in Section 3.2.1.ii above, '*an AI system intended to be used in the management and operation of road traffic*' refers to an AI system intended to be used in an asset, a facility, equipment, a network, or a system or a part of an asset, a facility, equipment, a network or a system which is necessary for the provision of the essential services established in Article 2(2) point (d) of the CER Delegated Regulation. This includes:

- Traffic management control, including aspects related to road network planning, control and management services, excluding traffic management or the operation of intelligent transport systems where they are not an essential part of the general activity of public entities *(road authorities)*;

- Intelligent Transport Systems services *(operators of Intelligent Transport Systems)*;

(196) An AI system intended to be used in the management and operation of road traffic should therefore be considered high-risk only if it is intended to be used by a road traffic entity (i.e. a road authority or an operator of Intelligent Transport Systems) that has been identified as a critical entity by a Member State under the CER Directive.

a) Practical examples of AI systems falling within the high-risk use case of road traffic

- **An AI system intended to be used as a real-time translation tool**. Such a system is necessary for transport service employees to overcome language barriers between the control centre and drivers or between passengers and drivers, which ensures linguistic communication and contributes to the safety of public transport operations.
- **An AI system intended to be used to monitor road traffic and to adjust traffic lights accordingly**. Such a system controls or limits possible physical harm to people or physical damage to vehicles, road users and surroundings by directly protecting the physical integrity of road traffic management system. It should therefore be considered to have a direct impact on road traffic safety.

- **An AI system intended to be used in the recognition of heavy objects on vulnerable bridges and quaysides**. Such a system helps prevent the collapse of bridges and quay walls. It prevents physical harm to natural persons and physical damage to objects under a bridge or a quayside by directly protecting the physical integrity of road infrastructure dependent on the road traffic management system. The failure of the AI system could result in potential collapse not being detected on time and natural persons on the bridges and quay walls being at risk when they collapse. The AI system is not needed for managing bridges and quays and is an additional safety component, comparable to an emergency button.
- **An AI system intended to be used to link real-time water level data to lock management for road traffic** (e.g. in flood-risk scenarios). Such a system monitors and detects situations that may directly lead to physical harm to natural persons or physical damage to property by directly protecting the physical integrity of the road infrastructure dependent on the road traffic management system.

- **An AI system intended to be used as a control system capable of communicating with road users via telecommunication networks** (Intelligent Traffic Control System - iTCS). Such a system can recognize traffic, perform analyses on received data, and make decisions based on these analyses. This enables the prioritisation of certain road users over others; a key advantage being improved traffic flow on busy roads. Through data exchange with iTCS, road users can also be informed about how long a traffic light will remain red or green. Such an AI system prevents accidents (e.g., head-on collisions if two traffic flows cross paths, chain-reaction accidents in congestion), its malfunction could cause gridlock, the obstruction of emergency services, (e.g., ambulances) or an increased likelihood of accidents at busy junctions, and such

failures create direct and immediate risks to both infrastructure integrity (damage to signals, road surfaces, vehicles, etc.) and health and safety of natural persons (fatalities and injuries).

b) Practical examples of AI systems falling outside the high-risk use case of the road traffic

- **An AI-enabled traffic flow optimisation system based on real-time data collection**. Such a system is a traffic data analytics platform enabling intelligent analysis for flow optimisation functions, but does not directly trigger changes in the traffic management that may impact the safety; it does not directly protect safety or physical integrity. These systems provide insights but do not directly protect physical integrity. Traffic systems can function without it.
- **An AI system used for predictive maintenance which allows for more accurate predictions regarding infrastructure maintenance** as part of a range of safety measures. Such an AI system merely helps prevent failures; it is not a safety component and malfunctioning of the system would not endanger the safety as the system can function without it as it is only one measure that is precautionary in nature among other safety safeguards and not essential for the safe operation of the system.

3.2.4. The supply of water use case in critical infrastructure

(197) According to the approach presented in section 3.2.1.ii above, '*an AI system intended to be used in the management and operation of supply of water*' refers to an AI system intended to be used in an asset, a facility, equipment, a network, or an system or a part of an asset, a facility, equipment, a network or a system which is necessary for the provision of the essential services established in Article 2(6) and (7) CER Delegated Regulation. This includes:

- Drinking water supply and drinking water distribution, excluding distribution of water for human consumption, where that service is a non-essential part of the general activity of distributors distributing other commodities and goods *(suppliers and distributors of water intended for human consumption).*
- Waste water collection, treatment and disposal, excluding collecting, disposing of or treating urban wastewater, domestic wastewater, or industrial wastewater where they are not an essential part of the general activities of undertakings (*undertakings collecting, disposing of or treating urban waste water, domestic waste water and industrial waste water*).

(198) AI systems intended to be used in the management and operation of the supply of water should therefore be classified as high risk only if they are intended to be used by a water entity that has been identified as a critical entity by a Member State under the CER Directive.

a) Practical examples of AI systems falling within the high-risk use case of water supply

- **An AI system intended to be used as a pressure sensor in water pressure monitoring systems**. Such an AI system fulfils the definition of a 'safety component' and it is intended to be

used in the distribution of drinking water, which is covered by the supply of water use case (Recital 55 AI Act).

- **An AI system intended to be used to predict sewage system overflow that impacts drinking water**. Such an AI system fulfils the definition of a 'safety component' and it is intended to be used in the distribution of drinking water, which is covered by the supply of water use case.

3.2.5. The supply of gas use case in critical infrastructure

(199) According to the approach presented in section 3.2.1.ii above, '*an AI system intended to be used in the management and operation of supply of gas*' refers to an AI system intended to be used in an asset, a facility, equipment, a network, or an system or a part of an asset, a facility, equipment, a network or a system which is necessary for the provision of the essential services established in in Article 2(1)(d) CER Delegated Regulation. This includes[28]:

- the supply of gas (supply undertaking);
- the distribution of gas (distribution system operators);
- the transmission of gas (transmission system operators);
- the storage of gas (storage system operators);
- the operation of a liquified natural gas (LNG) system (LNG system operators);
- the production of natural gas (natural gas undertakings);
- the purchase of natural gas (natural gas undertakings);
- the refinement and treatment of natural gas (operators of natural gas refining and treatment facilities).

(200) An AI system used in the management and operation of supply of gas should be considered high risk if it is intended to be used by a gas entity (i.e.: gas supply undertaking, distribution, transmission or storage system operator, LNG system operator, natural gas undertaking, operator of natural gas refining and treatment facility) that has been identified by a Member State as a critical entity under the CER Directive.

a) Practical example of an AI system falling outside of the high-risk use case of the supply of gas

AI system used as a predictive maintenance tool for gas pipeline monitoring by analysing operational data to predict maintenance needs. Such AI system does not directly control safety functions and existing safety systems remain independently operational.

[28] The supply of gas use case does not include an oil subsector as defined in Annex III point 1c of the CER Directive (operators of oil transmission pipelines; operators of oil production, refining and treatment facilities, storage and transmission; central stockholding entities as defined in Article 2, point (f), of Council Directive 2009/119/EC).

3.2.6. The supply of heating use case in critical infrastructure

(201) According to the approach presented in section 3.2.1.ii above, '*an AI system intended to be used in the management and operation of supply of heating*' refers to an AI system intended to be used in an asset, a facility, equipment, a network, or a system or a part of an asset, a facility, equipment, a network or a system which is necessary for the provision of the essential services established in point (b) of Article 2(1) CER Delegated Regulation. This includes the provision of district heating or district cooling (*operators of district heating or district cooling*).

(202) An AI system used in the management and operation of supply of heating should be considered high risk if it is intended to be used by an entity providing district heating or district cooling that has been identified by a Member State as a critical entity under the CER Directive.

a) Practical examples of AI systems outside the high-risk use case of the supply of heating

AI used in autonomously moving robots that perform regular, predefined patrols and checkpoints in heating (power) plants. Such an AI system can only be used for detection purposes. It is not capable of taking preventive measures, actively intervening in operations, rectifying malfunctions, or averting dangers. It therefore lacks a safety function.

3.2.7. The supply of electricity use case in critical infrastructure

(203) According to the approach presented in section 3.2.1.ii above, '*an AI system intended to be used in the management and operation of supply of electricity*' refers to an AI system intended to be used in an asset, a facility, equipment, a network, or an system or a part of an asset, a facility, equipment, a network or a system which is necessary for the provision of the essential services established in point (a) of Article 2(1) CER Delegated Regulation. This includes[29]:

- the supply of electricity (electricity undertakings);
- the operation, maintenance and development of an electricity distribution system (distribution system operators);
- the operation, maintenance and development of an electricity transmission system (transmission system operators);
- the generation of electricity (producers);
- the nominated electricity market operator service (nominated electricity market operators);
- the demand response (electricity market participants);
- the aggregation of electricity (electricity market participants);

[29] The supply of electricity use case does not include the hydrogen sector as defined in Annex III point 1c of the CER Directive (operators of hydrogen production, storage and transmission).

- the energy storage (electricity market participants).

(204) An AI system used in the management and operation of supply of electricity should be considered high risk if intended to be used by an electricity entity (i.e.: electricity supply undertaking, distribution or transmission operator, electricity producer, nominated electricity market operator or electricity market participant) that has been identified by a Member State as a critical entity under the CER Directive.

(205) A specific consideration is needed in relation to AI systems used as safety components in nuclear energy production. Recital 5 CER Directive delineates the scope within the energy sector, acknowledging that electricity generation may include electricity transmission parts of nuclear power plants, but excludes nuclear-specific elements covered by treaties and Union law, including relevant Union legal acts concerning nuclear power.

(206) For this reason, AI systems used as safety components in nuclear energy production do not fall within the high use case listed in point (2) of Annex III. AI systems deployed within nuclear power plants are not covered by the critical infrastructure use case, while AI systems used as safety components in electricity components of nuclear power plants could be included.

a) Practical examples of an AI system falling within the high-risk use case of the supply of electricity

An AI system used in a surveillance and protection for physical perimeter protection such as camera systems, radar systems and drone control systems used to directly protect the physical integrity of the infrastructure.

An AI system used for the detection of anomalies in data patterns when operating electricity grids for the purpose of monitoring and supporting decision-making in relation to critical functions, such as power load distribution, grid stability, or shutdown procedures.

b) Practical examples of AI systems falling outside the high-risk use case of the supply of electricity

- **An AI system used for electricity grid optimization by forecasting the energy demand**. The core safety functions are handled separately, so that the system cannot be considered to have a direct safety function.

- **An AI system used in a cybersecurity monitoring for energy grid networks.** Such a system is intended to be used solely for cybersecurity purposes. It continuously monitors network traffic, detects anomalous patterns, and identifies potential cyber threats across electricity grid communication networks. It analyses data flows, identifies suspicious activities, and alerts security personnel to potential intrusions or malware. It operates independently from operational technology systems that directly control physical grid operations.

- **An AI system used as a quality assurance of meter installation**. Such an AI system analyses the images of installed electricity meters. The output of the system is provided to the human

worker with recommendations regarding errors and improvements. It does not have a direct safety function.

- **An AI system used as an incident detection for e.g. precautionary outage prevention**. The output is the detection of anomalies and the prediction of impending outages or incidents. In order to prevent them from happening the AI system is sending the grid control centre a warning of the detected or foreseen incident as part of a range of safety measures. The grid control centre operator can then take precautionary measures like switching loads to prevent an outage. Such AI system is not considered as a high risk due to lack of a direct safety function as it is only one measure that is precautionary in nature and not essential for the safe operation of the system. It does not act on itself but rather only enriches the decision-making options in the grid control centre. Even if the system wrongly indicates impending outages or incidents, no outage is created.

- **An AI system used for detection and analysing anomalies in data provided from operating the power grid, where the output e.g. is the basis for future improvements in operating the power grid**. An AI system that is used for detection of anomalies in data patterns when operating electricity grids so that they are checked by the human operator exists to enrich the decision-making process. It lacks a direct safety function.

- **An AI system used for providing recommendations as an assistant, predicting energy consumption at transmission, regional or local level**. Such an AI system lacks a direct safety function.

- **An AI-system, supervised by a human worker, makes forecasts for grid imbalances, e.g. 15-minutes interval**. That forecasts support operational planning, but also directly influence market players. A malfunctioning in the AI-system could mislead both external and internal actors, potentially causing suboptimal dispatch or hedging strategies. This can affect grid stability, which can lead to malfunctioning in electricity supply. This will not be classified as a high-risk system due to lack of a direct link between the system and potential harm.

3.3. Education and vocational training

(207) The AI Act acknowledges the potentially high-risk nature of AI systems intended to be used in the area of education and vocational training. While AI systems used in this area may promote high-quality education and training, certain AI systems may have a negative impact on the health, safety or fundamental rights of the persons affected by them, such as students or apprentices, insofar as they may affect the educational and professional course of a person's life and therefore that person's ability to secure a livelihood[30]. When improperly designed and used, such systems may be particularly intrusive and may violate the right to education and training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation.

(208) The AI Act, which is based on Article 114 TFEU, establishes a harmonised framework for the placement on the market, putting into service, and use of high-risk AI systems, ensuring a consistent

[30] Recital 56 AI Act.

approach to such systems across the Union. Consequently, the prerogatives of the Member States in the realm of education under Article 165 TFEU do not affect the classification of an AI system intended to be used in the area of education and vocational training as high-risk pursuant to point 3 of Annex III and the application of the obligations for high-risk AI systems laid down in the AI Act to that system.

3.3.1. Overview of use cases and horizontal issues

(209) Point 3 of Annex III lists as high-risk four AI system use cases intended to be used in the area of education and vocational training, namely:

(a) AI systems intended to be used to determine access or admission to or to assign natural persons to educational and vocational training institutions or programmes at all levels;

(b) AI systems intended to be used to evaluate learning outcomes of natural persons;

(c) AI systems intended to be used to assess the appropriate level of education that an individual will receive or will be able to access, in the context of or within educational and vocational training institutions at all levels; and

(d) AI systems intended to be used to monitor and detect prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels.

i. The concept of 'educational and vocational training institution'

(210) An AI system will only be classified as high-risk under point 3 of Annex III if it is intended to be used in the context of or within educational and vocational training institutions at any level. The reference to 'educational and vocational training institutions' in conjunction with the reference to 'at all levels' should be understood in a broad manner so as to encompass all levels of formal and non-formal education, including early childhood, primary, secondary, tertiary and vocational education and training, as well as adult education.

(211) As explained in the Guidelines on prohibited artificial intelligence practices[31], the reference to 'educational institutions' in the AI Act is broad, encompassing both public and private institutions, with no limitation on the types or ages of pupils or students, or the specific environment (online, in person, in a blended mode, etc.). Educational institutions are normally accredited or sanctioned by the relevant national education authorities or equivalent authorities, and may provide a certificate (with participation as a precondition for obtaining a certificate).

(212) This includes not only formal educational and vocational training institutions, but also non-formal institutions, such as adult education and continuing educational institutions, which may offer personalised learning and skill development opportunities, and which may provide a certificate upon completion of the training or course.

(213) In particular, formal education refers to the structured education system that runs from primary to tertiary education and may also include specialised programmes for technical and professional training. Non-formal education refers to any deliberate, voluntary and planned programme of

[31] Paragraph 255, Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act).

personal and social education that aims to convey and practice values, and develop a wide range of skills and competences, outside the formal education curriculum. Vocational training is an integral part of formal education in several EU education systems.

(214) AI systems falling within one of the use cases listed in point 3 of Annex III are those that are intended to be used in the context of or within educational and vocational training institutions at all levels. Such systems primarily impact individuals engaged in learning, such as students or apprentices. Where an AI system is used in the context of an educational or vocational training institution, but it is mainly directed to the training of educators and training staff, including teachers and academic staff, that system will fall outside the use cases listed in point 3 of Annex III, although it may fall within one of the employment use cases listed in point 4 of Annex III.

(215) AI systems falling within the use cases listed in point 3 of Annex III will often involve the automated processing of personal data to evaluate the personal aspects of a natural person, in particular to analyse or predict aspects related to that person's academic or vocational training path. Such systems will often perform profiling of natural persons and may lead to automated decision-making within the meaning of Article 22 GDPR. They should always be classified as high-risk, even if the system fulfils the conditions of the filter mechanism listed in Article 6(3) AI Act.

ii. Interplay with the prohibited practices and the use case in point 1(c) of Annex III

(216) Article 5(1)(f) AI Act prohibits the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the area of education institutions, except where the use of the system is intended to be placed on the market or put into service for medical or safety reasons. Where an AI system to infer emotions of natural persons in the area of education falls outside the scope of this prohibition, it may nevertheless be classified as high-risk, either because it falls within one of the use cases listed in point 3 of Annex III or the use case listed in point 1(c) of Annex III.

3.3.2. Point 3(a): AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels

(217) Point 3 (a) of Annex III classifies as high-risk AI systems intended to be used to determine access or admission, or to assign natural persons, to educational and vocational training institutions at all levels. In this context, 'access, admission or assignment' refers to the process by which it is determined whether a person may enrol, gain entry, or be placed into a specific course, programme or learning pathway. The output of these systems could affect one's learning and educational pathway and right to education.

(218) AI systems typically falling within this use case are those intended to be used to assess applications to determine the access of specific natural persons to specific educational institutions at various levels, to process the evaluation of their applications, or to assist in such admission decisions, such as student placement and assignment. Similarly, vocational training assignment systems, which match job seekers or employees with suitable vocational training programs, should also be considered to determine access or admission to vocational training institutions, including access or admission to various programs within those institutions at all levels, and therefore be classified as high-risk pursuant to point 3(a) of Annex III. Considering that the evaluation of a learner's performance or progress can occur independently of the admission and assignment processes, AI

systems intended to be used for such evaluations should be considered to fall outside this use case, although they may fall within the use case listed in point 3(b) of Annex III.

(219) The use case listed in point 3(a) of Annex III should also be understood to include AI systems intended to be used to assign students or apprentices to specific programs or courses within an educational or vocational training institution (or to a subunit of it) at all levels, since their output directly affects a person's effective exercise of their right to study, train, or enrol in that institution.

a) Practical examples of AI systems falling within the high-risk use case of point 3(a)

- **Automated admissions systems** intended to be used to review and evaluate student applications, transcripts, and test scores to determine eligibility for admission to an educational institution. This includes systems that evaluate applications from prospective students and determine their eligibility for admission, since the system's output will directly affect the applicant's right to study, train, or enrol at the institution. That will be the case, for instance, where the system's evaluation and recommendation have the potential to influence the decision-making process, in that it determines the outcome of an admissions decision. In cases where the system does not perform profiling, the filter mechanism in Article 6(3) AI Act could apply, for example, if the system is instead intended only to perform a preparatory task to the assessment of eligibility done by the educational institution (Article 6(3), letter (d)).
- **School assignment systems which take their decisions based on location, availability and other personal characteristics of the applicant** that is intended to be used by municipalities or regional authorities to assign students - often in primary or secondary education - to public schools in an automated manner. Such systems function by collecting structured data, such as the student's home address, the geographical boundaries of school catchment areas, and the available capacity at each school. They also factor in sibling attendance and parental status to keep families together or to optimise for logistical efficiency, such as minimising commuting distance. Such systems process such data to assign students to schools, ensuring compliance with zoning rules and balancing enrolment across institutions. Since the system's assessment of data constitutes profiling, the filter mechanism in Article 6(3) AI Act cannot be applied to it.
- **Vocational training assignment AI tools** intended to be used by a regional employment agency to process applicants' prior education records, completed certifications, and standardized aptitude test results to match individuals to available apprenticeship programs should be classified as high-risk. Such systems apply predefined eligibility criteria, such as minimum qualifications required for each program and capacity limits, to assign candidates to appropriate training slots. Since the system's assessment of data constitutes profiling, the filter mechanism in Article 6(3) AI Act cannot be applied to it.
- **Automated scholarship eligibility assessment** system intended to be used to automate the process of determining an individual's eligibility for a scholarship programme based on data about the individual's financial situation, including their income, expenses, and family size. Such systems assess the eligibility of an individual's eligibility for financial assistance, thus determining their access to an educational institutional.

b) Practical examples of AI systems falling outside the high-risk use case of point 3(a)

- **Educational programme matching platform** using AI to provide secondary school students with recommendations on tertiary education programmes and the most suitable institutions based on their indicated preferences and previously selected topics of interest The output of such systems does not determine access or admission to educational programs, but rather serves as a tool to inform prospective students to support their own decision-making process on whether to apply to a specific institution or programme.

- **Chatbot for admission information** provided by a university to answer prospective students' questions and to provide them with information about its admission requirements, application process, and available programs. While such chatbots are linked to the admission process, they do not make decisions about student admissions or provide personalised recommendations that could influence an admissions decision. Such a chatbot's output is limited to providing general information and guidance, and it does not have the potential to materially influence the decision-making process.

c) Practical examples of AI systems falling within the use case but exempted by the filter mechanism in Article 6(3)

- **AI systems supporting the processing of applications** to be used by an education institution for file handling, such as indexing, searching, text and speech processing, as well as for the translation of documents provided along with applications, and for extracting, transforming, and organising the data collected into a meaningful and usable format. Although such systems support the assessment process, they do not have a relevant impact on the decision-making process, since they are only intended to facilitate the organisation and review of applicant files. Such systems therefore fall under the exception for AI systems intended to perform a preparatory task listed in Article 6(3)(d) AI Act.

- **AI-enabled admissions decision review tools** intended to be used by an educational institution to review and analyse ex post admissions decisions made by an admissions committee. Such systems are not intended to be used to replace or influence human assessment, but to provide a quality control check to ensure that the admissions process is functioning as intended and to support and improve future decision-making processes, rather than to make decisions. Since such systems are intended to detect decision-making patterns and deviations, and are not meant to replace or influence the previously completed human assessment, they can be considered to fall under the exception for AI systems intended to detect decision-making patterns listed in Article 6(3)(c) AI Act.

- **AI-enabled admissions data organisers** intended to be used by an educational institution to automatically categorise and organise incoming applications prior to the admissions process. Such systems are intended to be used to extract relevant information from unstructured application documents, such as resumes, cover letters, transcripts, and convert it into a structured format, to classify each application into one of several predefined categories, such as undergraduate, graduate, international student, and to identify and flag duplicate applications to prevent unnecessary processing. Provided the system does not take any decision on admission or access to the educational institution, it can be considered to fall within the exception for systems

intended to perform a narrow procedural task of data processing and organisation listed in Article 6(3)(a) AI Act.

3.3.3. Point 3(b): AI systems intended to be used to evaluate learning outcomes

(220) Point 3(b) of Annex III classifies as high-risk AI systems intended to be used to evaluate learning outcomes in educational and vocational training institutions at all levels. The evaluation of learning outcomes refers to the process of appraising knowledge, know-how, information, values, skills and competences - acquired in formal and non-formal, educational and vocational training settings - against relevant standards (learning outcomes, validation).

(221) The outcome of this evaluation process typically involves a quantified or qualitative assessment of the learner's achievement against predefined learning objectives, standards, curriculum goals, or competency frameworks. The resulting evaluation may be used for a range of purposes, such as issuing grades or certificates, awarding a qualification identifying gaps in mastery, informing accreditation or qualification decisions, and automatically steering or personalising subsequent instructional pathways (e.g., recommending remedial modules, adaptive learning resources, or progression to more advanced content).

(222) A distinction should be made between 'summative' evaluation and 'formative' evaluation, in view of their different objective and impact on a person's learning prospectus. Summative evaluation refers to the assessment of student learning, which leads to a grade, evaluation, or qualification, or at the end of an formal instructional unit (a course, programme, or educational pathway, such as a term, semester, or a school year), and can thus have a significant impact on the learner's educational trajectory, including by steering his or her learning process. Formative evaluation, by contrast, is an ongoing process of assessing student learning and progress, and has the objective of improving performance, rather than leading to a final grade, evaluation, or qualification. Formative evaluation is, in most cases, conducted continuously throughout the implementation phase of the academic project or programme and does not lead to a summative evaluation. Its primary purpose is to support learning through activities such as exercises, providing feedback and guidance to help students progress.

(223) Considering the impact on the student's educational trajectory, only AI systems that make an evaluation towards a final decision affecting educational and professional pathways based on a summative assessment fall under point 3(b) of Annex III. This means that AI systems that have a significant influence on a student's educational path, such as AI-powered grading systems that determine a student's final grade or intermediate grades that are considered in the final evaluation or academic standing, should be classified as high-risk. This follows from the use of the terms 'evaluate learning outcomes' used in that provision.

(224) By contrast, AI systems that provide feedback and learning support as part of the ongoing educational process should not be classified as high-risk. This category includes adaptive learning systems that adjust the difficulty level of course materials based on a student's performance, intelligent tutoring systems that provide personalised feedback and guidance to students, and learning analytics platforms that track student engagement and progress and provide insights to teachers and educators. Such systems generally do not make final decisions affecting the educational pathways of a person, but rather support the learning process and provide feedback to students in a continuous manner.

(225) In addition, AI systems used by students on their own volition to support non-formal and informal learning, without specifically being required to do so by the educational or vocational training institution at which they are enrolled, should not be classified as high-risk. Such systems should only be classified as high-risk if they lead to the attainment of a credential, certification, or a form of validation recognised by the relevant public authorities, since they would then have an impact on student's educational and professional trajectory, unless one of the exceptions in Article 6(3) AI Act applies.

a) Practical examples of AI systems falling within the high-risk use case of point 3(b)

- **AI-enabled grading and feedback systems** intended to be used to evaluate students' assignments, such as tests, quizzes, and exams which count towards a final evaluation. Such AI systems have an impact on the summative evaluation of students by analysing the results of assignments and proposing grades.
- **AI-enabled personalised learning assistant** intended to be used to provide recommendations and feedback to students on their progress by generating reports at the end of each unit, which include grades, areas of strength and weakness, and recommendations for improvement. Although such AI systems support formative evaluation by providing ongoing feedback and guidance to students to help them improve their understanding of course material, their output is also used by the teacher to inform decisions about student's grades at the end of the academic period and therefore have an impact on summative evaluation.

b) Practical examples of AI systems falling outside the high-risk use case of point 3(b)

- **AI-enabled language learning software applications** intended to be used by students to support non-formal and informal learning by providing instant feedback and corrections on identified errors, but which does not lead to the attainment of a credential, certification, or form of accredited validation. Such AI systems are used by students on their own volition, without being required to do so by an educational institution.
- **AI-enabled neurodiverse learning companions** intended to be used to support students with neurodivergence, such as autism, dyslexia, and ADHD, which uses machine learning algorithms to create personalised learning pathways that cater to the individual needs and learning styles of each student by providing real-time feedback and adjustments to the learning materials, pace, and format to help such students stay engaged and motivated. For example, such an AI system may provide a student with dyslexia text-to-speech functionality, font size and colour adjustments, and multisensory learning materials to help that student better understand and retain information. Such a system may also provide accommodations such as extra time to complete assignments, breaks, and stress-reducing exercises to help students with anxiety or sensory processing issues. Such a system's output is used to inform the teacher's instruction and provide additional support to students with neurodivergence, but it is not intended to be used to determine grades or to assess student learning.
- **AI-enabled pronunciation feedback tool** intended to be used to provide feedback to students on their language pronunciation or fluency by analysing the student's speech and providing suggestions for improvement, such as correcting intonation, rhythm, and accent. The feedback

provided by the system is used by the students to improve their pronunciation skills; it is not used by educators to determine grades counting towards a final evaluation or assess language proficiency. Same example can be applied for an AI tool on reading skills providing feedback intended to be used by learners or students only.

c) Practical examples of AI systems falling within the use case but exempted by the filter mechanism in Article 6(3)

- **AI-enabled exam quality checker** intended to be used to check an exam prepared by a teacher for errors, such as grammatical issues, ambiguous wording, or inconsistencies with the rubric, and to suggests revisions for the teacher's consideration. However, since the AI system does not alter the core content of the exam, nor does it change the level of difficulty or the educational intent behind the questions, and the teacher remains responsible for any final decisions on the exam's content, the AI system's role should be considered strictly to enhance the clarity and accuracy of the exam, ensuring that it is error-free and aligns with the intended learning outcomes. Such a system would therefore fall under the exception for systems intended to improve the result of a previously completed human activity listed in in Article 6(3)(b) AI Act, namely, the preparation of the exam, by refining its quality without altering the substance or impact of the teacher's original educational decisions.

- **AI-enabled grade calculator** intended to be used by an educational institution to process data related to assessment and test grades obtained by students during the academic period which determines the final grade of the students' learning outcomes for the year. Such an AI system is designed to perform a simple calculation of the average grade, taking into account the grades and weights of each assessment, and test the output of the system as a numerical value representing the average grade, which is then used by the teacher to inform their final evaluation of the student's performance. Such a system would therefore fall under the exception for systems intended to perform a narrow procedural task listed in Article 6(3)(a) AI Act.

- **AI-enabled assessment review tool** intended to be used to detect decision-making patterns or deviations from prior decision-making patterns, with the goal of identifying potential inconsistencies or anomalies in the assessment decisions made by instructors. Such an AI system analyses the grading patterns of instructors over time, and flags any deviations from the expected pattern. For example, if an instructor has consistently given high grades to students who complete a certain assignment, but suddenly gives low grades to a group of students who complete the same assignment in the same manner, the AI system will flag this deviation as a potential anomaly. The output of the AI system is then reviewed by a human assessor, who investigates the flagged deviations and determines whether they are justified or not. The human assessor may decide to adjust the grades or take other corrective action, but the AI system's output is not used to automatically change the assessment decisions. Such a system would therefore fall under the exception for systems intended to detect decision-making patterns or deviations from prior decision-making patterns listed in Article 6(3)(c) AI Act, since it is not meant to replace or influence a previously completed human assessment.

3.3.4. Point 3(c): AI systems intended to be used for the purpose of assessing the appropriate level of education

(226) Point 3(c) of Annex III classifies as high risk AI systems intended to be used to assess the appropriate level of education that an individual will receive or will be able to access in the context of or within educational and vocational training institutions at all levels. Such systems may serve two main purposes. The first is determining the level of education an individual will receive in terms of progression within an ongoing learning path, such as advancing to the next grade or moving to a higher-level course. The second is assessing the level of education an individual will be able to access by evaluating their readiness and qualifications before they enter or begin a programme. The latter assessment often happens through placement tests or skill assessments used to determine the appropriate starting level or eligibility for specific educational or vocational pathways.

(227) AI systems intended to be used for the first purpose may use as a basis the student's current level of knowledge and skills in a particular subject area, such as mathematics or languages, and in this way determine the most suitable level of course, programme, or training module for them to follow next, thus supporting a personalised learning pathway. Such systems may also take into account any special educational needs or talents that a student may have, such as dyslexia or a prodigious ability in music, and provide personalised recommendations for their education. For example, an AI system may recommend a student with a special talent in mathematics to take advanced courses in calculus or number theory, while recommending a student with dyslexia to receive additional support in reading and writing.

(228) AI systems intended to be used for the second purpose may be used to evaluate an individual's skills, knowledge, and abilities to identify the most suitable educational or vocational training level for that person. By analysing the learner's current competencies - and, where relevant, their potential for progression - the system can recommend the appropriate placement within the education pathway and determine whether the student is ready to advance to the next stage of study.

(229) The ultimate decision-making responsibility rests with teachers and educational and vocational training institutions' responsible staff who may accept the AI system's recommendations or override them based on their professional judgment and knowledge of each student's needs and abilities. However, if not properly designed and deployed, such systems could misclassify students and negatively impact their learning opportunities and long-term outcomes, which is why they should be classified as high-risk.

a) Practical examples of AI systems falling within the high-risk use case of point 3(c)

- **AI-powered adaptive placement tools** intended to be used by an educational or vocational training institution to determine the optimal course level for incoming students. Such a system assesses a student's abilities to formulate recommendations addressed to educators whether the student should be in beginner, intermediate, or advanced classes, or decides if he or she should move to higher education or vocational training based on their skills.

- **Vocational training level assessment systems** intended to be used by a vocational training institution to assess the level of education that a learner will be able to access in a specific vocational program. Such a system may use a combination of placement tests and skill assessments to evaluate the learner's knowledge and skills in relevant areas, such as mathematics, physics, and engineering principles, and determine their eligibility for a particular level of study or course.

- **AI classifiers for special education** intended to be used to classify students with special educational needs into appropriate educational programs and recommend the most suitable educational placement for each student, including the level of support required. Such a system may use a machine learning algorithm to analyse a range of data, including student assessment data, such as results from standardized tests, including IQ tests, achievement tests, and behavioural assessments. It may also consider teacher's feedback on student's behaviour, social skills, and academic performance, as well as psychological evaluations, including reports from psychologists on student's cognitive abilities, emotional intelligence, and learning styles, and the student's medical history, including information on any diagnosed conditions or disabilities.

b) Practical examples of AI systems falling outside the high-risk use case of point 3(c)

- **Personalised education recommendations for students:** An AI system intended to be used to provide personalised educational recommendations to students for the appropriate level of education, such as courses, programs, or certifications, that they may be interested in applying for the following academic year on the basis of information provided by students themselves, such as interests and career goals. Since the system is not intended to be used by an educational institution, but is only intended to help students make informed decisions about their educational path, of the system does not fall within the use case listed in point 3(c) of Annex III.

- **Trend Analysis of Educational Attainment:** An AI system intended to be used by educational institutions, policymakers, and researchers to analyse from various sources, including educational institutions and government databases, trends in the levels of education accessed after completion of secondary education by students, and to identify patterns in the types of educational programs and levels of education that students are pursuing. Since the system's output is not used to make decisions about individual students' educational placement or opportunities, but rather to provide a broader understanding of the educational landscape, it does not fall within the use case listed in point 3(c) of Annex III.

c) Practical examples of AI systems falling within the use cases but exempted by the filter mechanism of Article 6(3)

- **AI-enabled pre-assessment tool** intended to be used to help educators prepare for the assessment of a student's readiness for a particular level of education or training, based on data about the student's prior education and work experience, and generating a set of questions and topics that the educator can use to assess the student's readiness should not be considered high-risk. Since the system's output is used by educators to inform their assessment methodology, but does not itself make any decisions about the appropriate level of education that an individual will receive or will be able to access, it should therefore be considered to fall under the exception for systems intended to perform a preparatory task listed in Article 6(3)(d) AI Act.

- **Improving recommendations for advanced course placement:** An AI system intended to be used by an educational or vocational training institution to analyse the results of tutors' recommendation to apprentices to pursue certain advanced courses, based on data from the apprentice's performance records and learning outcomes, and providing suggestions for improving the recommendation methodology, such as identifying additional factors that could

be considered, or suggesting alternative courses of action that could be taken. Since the system's output is used by the institution to refine its recommendations and to improve the decision-making process, but it does not take any decisions on the apprentice's educational placement or opportunities, it should be considered to fall under the exception for systems intended to improve the result of a previously completed human activity listed in Article 6(3)(b) AI Act.

3.3.5. Point 3(d): AI systems intended to be used for monitoring and detecting prohibited behaviour of students

(230) Point 3(d) of Annex III classifies as high-risk AI systems intended to be used to monitor and detect prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels.

(231) This use case encompasses AI systems intended to be used to monitor and identify prohibited behaviours of students during tests, both on-site and remote or online, synchronously and asynchronously.

(232) Prohibited behaviour of students should be understood, in this context, to refer to any action or activities by students that compromise the integrity of the testing process. This may include a broader range of behaviours, such as plagiarism, collusion, and tampering with exam materials. AI systems falling within this use case are typically used to prevent forms of compromising academic integrity in test settings (e.g. cheating). They may encompass a range of AI technologies, including facial recognition, keystroke analysis, screen monitoring, audio and video recording.

(233) The AI system must both monitor and detect the prohibited behaviour. Monitoring and detecting are interconnected processes, where monitoring is often a prerequisite for detection.

(234) The reference to tests in point 3(d) of Annex III means that the prohibited behaviour must occur during a process leading to an evaluation or a grade of a student, thus in the context of a summative assessment. Key elements to assess whether the monitoring and detection occurs during tests is the timing and the context in which the AI system is intended to be used. The system must be intended to be used during a controlled testing situation, such as written exams, oral exams, or other real-time assessments under supervision, by educational and vocational training institutions at all levels.

(235) Activities like checking homework, essays, or other assignments for plagiarism or improper collaboration fall outside the scope of this use case, since they typically take place in an unsupervised environment, after the work has been completed and submitted, and do not involve live monitoring or real-time behavioural analysis during the testing process itself.

a) Practical examples of AI systems falling within the high-risk use case of point 3(d)

- **AI-enabled proctoring system for exam certification** intended to be used by an educational or vocational training institution to monitor test-takers for prohibited behaviour during a certification exam, such as accessing unauthorized materials or communicating with someone else during the exam, by using a combination of facial recognition, keystroke analysis, and screen monitoring.

- **Real-time behaviour analysis system** using machine learning algorithms intended to be used by an educational institution to analyse student behaviour and detect patterns that may indicate cheating during online exams.

- **AI-enabled exam monitoring system** intended to be used by an educational institution to monitor and detect prohibited behaviour during in-person exams, such as the use of unauthorized materials or devices, by using facial recognition and object detection.

b) Practical examples of AI systems falling outside the high-risk use case of point 3(d)

- **AI system intended to be used by an educational institution to check homework or assignments for plagiarism** against a database of existing content. Such a system is not intended to be used to monitor and detect prohibited behaviour during tests, but to analyse submitted work which has been produced in a non-supervised environment and does not involve live monitoring or real-time behavioural analysis during the testing process.

- **AI system for non-academic student behaviour monitoring** intended to be used by an educational institution to monitor and detect student behaviour in the cafeteria, hallways, and other non-testing environments and to alert staff to potential incidents of bullying, harassment, or other undesirable behaviour. Such a system is not used to monitor and detect prohibited behaviour during tests, but for non-academic purposes, such as maintaining a safe and orderly school environment, and it does not involve the evaluation or assessment of student academic performance. However, this AI system could be classified as high-risk under point 1 of Annex III, if the system fulfils the definition of a remote biometric identification system.

c) Practical examples of AI systems falling within the use case but exempted by the filter mechanism in Article 6(3)

- **AI-enabled confirmation of suspicious behaviour:** During an online test, a human proctor observes a student exhibiting suspicious behaviour, such as consistently looking away from the screen or typing in a pattern that suggests they may be copying from a hidden source and uses an AI system to confirm or deny his suspicions. The AI system is trained on a dataset of known cheating behaviours and can identify patterns that are indicative of academic misconduct. The AI system analyses the student's data and provides a report to the human proctor, indicating that the student's behaviour is consistent with cheating. The report highlights specific patterns and anomalies that the AI system has identified, such as unusual keystroke patterns or excessive mouse movements. The human proctor reviews the report and may decide to investigate further and take appropriate action, such as alerting the student's instructor or initiating a formal investigation. Such a system would fall under the exception for systems intended to improve the result of a previously completed human activity listed in Article 6(3)(b) AI Act.

- **Identity verification:** An AI system intended to be used during a test to automatically processes students' identity verification documents, such as IDs or biometric data like facial recognition scans, to confirm that the person taking the test matches the registered candidate. Since the system helps streamline identity verification, but it does not directly decide if the student can proceed with the exam or if any sanctions should be applied in the case of misrepresentation, as

these decisions are made by the human proctor, it should fall under the exception for systems intended to perform a procedural task listed in Article 6(3)(a) AI Act.

3.4. Employment

(236) Point 4 of Annex III lists as high risk two use cases of AI systems intended to be used in employment, worker's management and access to self-employment. These include:

(a) AI systems intended to be used for the recruitment or selection of natural persons, [and] in particular:
- to place targeted job advertisements;
- to analyse and filter job applications; and
- to evaluate candidates.

(b) AI systems intended to be used:
- to make decisions affecting:
  - terms of work-related relationships;
  - the promotion; or
  - termination of work-related contractual relationships.
- to allocate tasks based on individual behaviour or personal traits or characteristics; or
- to monitor and evaluate the performance and behaviour of persons in work-related relationships.

(237) Recital 44 AI Act clarifies that, in the specific context of emotion recognition (particularly in the workplace), the use of AI systems may aggravate structural imbalances of power[32]. Such imbalances relate to the unequal bargaining position of workers and job candidates *vis-à-vis* employers. Recital 57 AI Act justifies classifying AI systems in the area of employment as high-risk on the ground that such systems may have '*an appreciable impact on future career prospects, livelihoods of those persons and workers' rights.*' That recital also makes explicit that work-related contractual relationships should, in a meaningful manner, include both employees and persons providing services through platforms. Moreover, the same recital indicates that '*such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation (...) and may also undermine their fundamental rights to data protection and privacy*'.

3.4.1. Horizontal issues

i. Personal scope

[32] The recital addresses, in specific, AI systems intended to be used to detect the emotional state of individuals in situations related to the workplace and education. However, its logic can be transposed to the wider set of high-risk AI systems falling within point 4 of Annex III AI Act.

(238) The personal scope of the use cases listed in point 4 of Annex III covers '*employment, workers' management and access to self-employment*'[33]. The AI Act does not itself define those notions, but requires a common understanding of them[34].

(239) CJEU case law has developed an autonomous notion of 'worker' in relation to Article 45 TFEU, from which inspiration may be drawn to define the notion of employment. According to that case law, the essential feature of being a worker is that, for a certain period of time, a person performs services for and under the direction of another in return for remuneration[35]. However, the notion of 'worker' must be considered as just one element of the broader expression '*employment, workers' management and access to self-employment*' and the reference in Recital 57 AI Act to '*work-related contractual relationships*' should not be read limited to a formal employment contracts but as capturing the broader spectrum of arrangements that constitute work, 'employment', and self-employed activity in general (e.g., natural persons who are self-employed due to regulatory requirements or choice, but are formally integrated within an organisation to whom they provide services).

(240) The notion 'worker's management' recognises AI-enabled management of workers as a feature increasingly present in the workplace. Including workers' management within the scope of the high-risk use cases listed in Annex III allows the AI Act to address the risk of harm to fundamental rights at the hiring and employment stage. The provisions of the AI Act for high-risk AI systems, in conjunction with the prohibition laid down in Article 5(1)(f) on emotion recognition in the workplace, establish a comprehensive legal framework for the regulation of the development of AI systems automating managerial tasks and a minimum standard for the protection of the rights of the workers in respect of the use of AI systems by employers[36]. Managerial functions such as, *inter alia,* recruitment processes, work allocation, monitoring and worker evaluation, as well as decisions on promotion, remuneration or termination are covered by the use cases listed in point 4 of Annex III.

(241) The inclusion of 'access to self-employment' in point 4 of Annex III aims to cover self-employed individuals such as persons working as independent contractors, service providers or performing independent professions rely on access to contracts or assignments to secure their livelihood. While Recital 57 AI Act recognises that work-related contractual also involve persons providing services through platforms[37] the notion of 'access to self-employment' is broader than platform work and covers other forms of self-employed activity such as solo self-employed persons who are in a

---

[33] In ascertaining, in specific, the use cases in scope, Recital 57 AI Act will be an important tool supporting interpretation.

[34] Not all AI system used in selection, recruitment or in the workplace are classified as high-risk. Only AI systems which are intended to be used within the use cases referred to in paragraphs a) and b) of point 4 of Annex III AI Act whose scope is further detailed below and that are not exempted under the filter.

[35] Case 66/85, Lawrie-Blum, EU:C:1986:284, Case C-256/01, Allonby, EU:C:2004:18, and Case C-229/14, Balkaya, EU:C:2015:455.

[36] In accordance with Article 2(11), the AI Act '*does not preclude the Union or Member States from maintaining or introducing laws, regulations or administrative provisions which are more favourable to workers in terms of protecting their rights in respect of the use of AI systems by employers, or from encouraging or allowing the application of collective agreements which are more favourable to workers'*.

[37] Article 2(1)(c) of Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving working conditions in platform work ('the Platform Work Directive'), OJ L 2024/2831, 11.11.2024, defines platform workers as 'any natural person who performs platform work, irrespective of the legal nature of their employment relationship.

situation comparable to workers[38]. In this regard, the EU acquis extends some protections to the self-employed, as regards the access to opportunities for professional activity[39]. As a consequence, freelancers, independent professionals, service providers, and platform workers regardless of contractual status fall within the personal scope of the use cases listed in point 4 of Annex III wherever AI systems mediate or condition their access to work opportunities. The Commission Guidelines on prohibited artificial intelligence practices[40] further clarify that the notion of 'workplace' must be interpreted broadly, encompassing '*any specific physical or virtual space where natural persons engage in tasks and responsibilities assigned by their employer or by the organisation they are affiliated to, for example in case of self-employment.*'

ii. Interplay with the prohibited practices

(242) Where an AI system intended to be used in the field of employment falls within one of the prohibitions laid down in Article 5 AI Act, its placing on the market, putting into service and use is per se unlawful, irrespective of any safeguards put in place by its provider or deployer. By contrast, AI systems falling within one of the use cases listed in point 4 of Annex III are classified as ''high-risk' and subject to heightened compliance obligations. If an AI system falls within the scope of both provisions, the prohibition will prevail and the system will remain unlawful. In this context, it is particularly relevant to consider the prohibition concerning AI systems inferring emotions in the workplace, which are prohibited pursuant to Article 5(1)(f) AI Act. For examples of AI systems captured by the prohibition in Article 5(1)(f) AI Act, reference is made to the Guidelines on prohibited artificial intelligence practices[41].

3.4.2. Point 4(a): AI systems intended to be used for the recruitment or selection of natural persons

[38] The Communication from the Commission (2022/C 374/02), Guidelines on the application of Union competition law to collective agreements regarding the working conditions of solo self-employed persons, OJ C 374, 30.9.2022, pp. 2–13, defines a solo self-employed person as someone who 'does not have an employment contract or who is not in an employment relationship, and who relies primarily on his or her own personal labour for the provision of the services concerned'. These Guidelines also refer to categories of solo self-employed persons who are in a situation comparable to workers.

[39] As can be seen in Directive 2010/41/EU on the application of the principle of equal treatment between men and women engaged in an activity in a self-employed capacity. Additionally, in this context, it is important to refer to Directives 2000/43/EC and 2000/78/EC here, which cover access to self-employment in protection from discrimination on the grounds of racial or ethnic origin, religion or belief, disability, age and sexual orientation. See Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010 on the application of the principle of equal treatment between men and women engaged in an activity in a self-employed capacity and repealing Council Directive 86/613/EEC, OJ L 180, 15.7.2010, pp. 1–6, Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180, 19.7.2000, pp. 22–26 and Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, OJ L 303, 2.12.2000, pp. 16–22.

[40] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) (OJ L, 2024/1689).

[41] With regards to emotion recognition AI systems that do not fall under the scope of the prohibition under Article 5(1)(f), please see the analysis of Annex III(1)(c) within these Guidelines.

(243) Point 4(a) of Annex III classifies as high-risk AI systems intended to be for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates.

(244) The classification of AI systems intended to be used in recruitment and selection as high-risk is justified by the fact that those processes constitute the principal entry point into the labour market. Decisions taken at this stage can condition an individual's career prospects and access to livelihoods. At the same time, the structural power asymmetry between internal and external recruiters and candidates, combined with the high degree of information held by employers on the candidate and contracting parties for self-employed, the job requirements, and the labour market creates a context in which ensuring the protection of job applicant's rights is essential.

(245) For an AI system to be classified as high-risk pursuant to point 4(a) of Annex III, the activity for which it is intended to be used should relate to or impact the substance of the recruitment process: covering preparatory steps (special advertising, prospecting, pre-application screening) and the selection process (shortlisting, grading, ranking, or testing of candidates). The notions of 'recruitment" and 'selection" require a functional interpretation, since they are partly overlapping but not identical.

i. The notion of 'recruitment'

(246) Recruitment constitutes the process of preparing the constitution of a new work-related relationship, commencing already with the identification and attraction of potential applicants, and continuing until the conclusion of a contract, if applicable. This encompasses early-stage prospection activities, including the placement of targeted job advertisements (see point *iii* below), the identification of potential candidates in databases, or other informal approaches undertaken prior to the launch of a formal procedure[42]. AI systems may also be intended to be used in recruitment, for instance, for the screening of CVs, candidate sourcing, or applicant ranking.

(247) AI systems may also analyse hiring data to predict which candidates are most likely to succeed based on skills and past performance or to help generate job descriptions. These may or may not fall within the scope of point 4 of Annex III depending on whether the system truly pertains to the domain of recruitment in a manner that impacts in substance career prospects or workers' rights. Where that is the case, the system may be exempted from high-risk classification if it fulfils any of the conditions in Article 6(3) AI Act. To assess this, it is key to examine the AI system's potential impact on prospective or actual candidates' employment and career opportunities, or the risk of discrimination[43].

[42] This understanding is consistent with the case law of the Court of Justice of the European Union which confirms that EU equality law applies already at the stage of access to employment. In Case C-54/07, Centrum voor gelijkheid van kansen en voor racismebestrijding v Firma Feryn NV, EU:C:2008:397 and subsequently in Case C- 507/18, Associazione Avvocatura per i diritti LGBTI, EU:C:2019:922 the Court held that discriminatory statements by an employer concerning prospective employees constituted discrimination, even in the absence of a formal recruitment procedure.

[43] For instance, job descriptions or advertisements may have a strong influence on who will be successful in the recruitment procedure, especially if they set out the qualifications required for the job and/or the selection criteria. Drafting them based on biased data, such as past recruitment patterns, can increase the risk of discrimination for disadvantages groups.

AI system generating job descriptions

An AI system exclusively generates job descriptions based on a list of tasks to be carried out and a set of necessary qualifications and skills previously defined by a human recruiter. AI tools of this type can fall within the high-risk use case of point 4 of Annex III, if it is within their intended purpose to play a role in the recruitment process in a manner that affects applicants' prospects. However, the specific AI system referred above should be considered as performing a narrow procedural task (Article 6(3)(a)) as this specific use case poses only limited risks and does not meaningfully influence the application process and, hence, should be exempt from the high-risk classification.

In contrast, an AI system of the same type, but where the AI system itself generates the necessary qualifications and skills based on a high-level description of the job position or that has an additional function allowing it to substantially affect the application process by evaluating the candidates' CVs against the job description that it created and to make recommendations of suitability on this basis cannot be considered as falling within the filter and should be classified as high-risk.

(248) The notion of recruitment includes onboarding processes where the outcome of an AI system performing such a process may affect access to work, in particular where onboarding constitutes a relevant aspect of the recruitment process and not the first step after its conclusion (e.g. when the employer performs checks on preliminarily hired workers). Recruitment is concluded when the worker is understood to be hired and dismissal procedures must follow through specific channels foreseen to that effect.

ii. The notion of 'selection'

(249) Selection has two distinct meanings. On the one hand, it reflects the fact the high-risk area of Annex III, point 4 also encompasses 'access to self-employment'. While such processes might not be 'recruitment' in the strict sense, natural persons who are self-employed may also undergo a selection process before they are contracted. Therefore, AI systems used in the selection of self-employed persons by their contracting parties should fall within the scope of Annex III, point 4(a). On the other hand, 'selection' also refers to the specific stage in recruitment where candidates are assessed, filtered, and chosen for advancement or hiring. It covers activities such as the analysis of applications, automated shortlisting, scoring, ranking, or assigning predictive scores of job suitability.

iii. Place targeted job advertisements

(250) Although point 4(a) of Annex III, lists examples of selection, such as 'analysing and filtering job applications' and 'evaluating candidates,' this list should not be seen as being exhaustive[44]. The explicit inclusion of targeted job advertisements in point 4(a) of Annex III follows from the fact that the placement of advertisements that are algorithmically tailored to reach certain groups of

[44] The application of point 4(a) is limited by the intended purpose of the AI system, as such AI systems intended to select or evaluate tender offers or responses to requests for proposals will not be classified as high-risk just because they are theoretically capable of selecting or evaluating an offer from a self-employed sole proprietor. However, to fall out of scope of the high-risk classification, the use of the AI system may not result in a *de facto* selection (or exclusion) of the self-employed person (instead of the proposal) nor an evaluation of the self-employed person (instead of the proposal).

individuals determine who becomes aware of, and who is encouraged to apply for, specific vacancies. Where an AI system placing targeted job advertisements relies on profiling, it should always be considered high-risk, given the exclusion in Article 6(3), last subparagraph, AI Act of AI systems based on profiling from benefiting from the filter mechanisms contained in that provision. Even where such an AI system does not involve profiling, the system should be considered high-risk, if it meaningfully conditions access to employment opportunities or can lead to a risk of discrimination.

(251) A job advertisement must be understood to represent an active indication that an employer is seeking candidates for a concrete vacancy. Employer branding or generic advertisements related to the firm, which do not in practice relate to a vacancy, fall outside the use case listed in point 4(a) of Annex III.

(252) Moreover, where the personalisation of the persons to whom an advertisement is shown results directly from non-discriminatory, objective and reasonable criteria[45] that are inherent requirements of the job description, it may be excluded from the scope of 'targeted job advertisements". Likewise, the placing of job advertisements by AI system that are based exclusively on contextual elements (contextual targeting), such as content of the location where the advertisement is placed (*e.g.,* website) and that are not directly related to specific natural persons or groups of natural persons, should also be considered to fall outside the use case listed in point 4(a) of Annex III. In such a case, the target audience of the location will be the same as the relevant audience that the advertiser is trying to reach to fill a vacancy. However, the job advertisement can still be shown to anyone who accesses the location (*i.e.,* there is no exclusion).

iv. Analyse and filter job applications

(253) The terms 'to analyse and filter job applications' used in point 4(a) of Annex III should be understood broadly and not as limiting the use case to AI systems that always perform both functions simultaneously. A functional interpretation is required: where an AI system merely analyses applications in a descriptive sense (such as converting file formats or classifying degrees into standard categories without applying evaluative weight), it may be considered to perform a preparatory task within the meaning of Article 6(3)(d) AI Act. In contrast, AI systems that analyse job applications with an effect that may result in a restriction of the applicant in accessing certain job opportunities, for example by producing suitability scores, assessing compatibility of a candidate's profile or experience with the selection criteria or job description, or producing competence profiles that condition shortlisting, fall within scope of the high-risk use case listed in point 4(a) of Annex III. In this case, 'analysis" and 'filtering" form part of a continuum: analysis

[45] This would be the case if the requirements stem from a genuine and determining occupational requirement whose absence may make it impossible for the candidate to perform the functions stated in the job description, and not when it is about a preferred characteristic, or a specific profile that while desirable does not have a direct and objective link to the required qualifications/skills. In assessing the mentioned non-discriminatory, objective and reasonable criteria, it is important to consider the EU non-discrimination acquis, including Article 4 of Directives 2000/78/EC and 2000/43/EC and Article 14(2) of Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast), OJ L 204, 26.7.2006, pp. 23–36.

that influences access to later stages operates de facto as filtering, and therefore falls within the scope of Annex III, point 4(a).

v. Evaluate candidates

(254) The terms 'to evaluate candidates' used in point 4(a) of Annex III must also be understood broadly. Evaluation refers to any assessment of a candidate's (including self-employed) suitability, merit or potential, whether through scoring, ranking, predictive modelling, or qualitative judgements derived from data inputs. The provision does not require that the evaluation carried out by the AI system directly determines the hiring outcome. It suffices that it appreciably influences the decision-making process, for example by laying out shortlists, prioritising certain applicants or scoring assessments within the context of the recruitment or selection process that may result in advantages for certain candidates. AI tools that merely present factual information without involving evaluative weight (such as software displaying unaltered employment history) may fall outside scope if they do not generate assessments of suitability.

a) Practical examples of AI systems falling within the high-risk use case of point 4(a)

- **AI systems intended to be used as an automated job matching and ranking tool** designed to assist internal and external recruiters in the recruitment and selection processes by analyzing and filtering candidates should be classified as high-risk. Such a system processes structured and unstructured data (e.g., CVs, skills, education, past placements, cognitive, social and emotional competencies) and compares it to job descriptions or historical hiring data to generate quantitative scores, rankings (e.g., 'top 5 candidates'), and/or qualitative fit categories (e.g., 'high fit,' 'low fit'). These outputs are used to shortlist candidates for internal and external recruiters, who retain discretion to review, override, or supplement algorithmic recommendations. However, the system's rankings and scores serve as a primary input for decision-making. For example, it could lead to low ranking or exclusion of candidates of a certain gender or of candidates with disabilities. It therefore falls to be classified as high-risk pursuant to point 4(a) of Annex III.

- **AI system intended to be used for candidate or contractor sourcing across online platforms** A recruitment agency deploys an AI-enabled tool to search social media, professional sites or job boards, and its own CV databases. Recruiters input pre-defined criteria such as years of experience, technical skills, or educational background. The system processes unstructured and structured data, identifies matching profiles, and generates a shortlist of potential candidates or contractors who are natural persons.

  This system falls within the use case of point 4(a) of Annex III, since it directly and meaningfully affects the recruitment and selection of natural persons by filtering and identifying candidates. None of the exceptions in Article 6(3) apply considering the tasks carried out by the AI system and its material influence on the outcome of decision-making.

- **AI system ranking self-employed service providers** An online platform designed to help consumers in finding a self-employed service provider to assist them with various tasks uses an AI-enabled job-matching tool that ranks service providers and determines which are presented to potential consumers.

This system falls within the use case of point 4(a) of Annex III since it directly and meaningfully affects selection of natural persons by filtering and ranking potential service providers. Because its output shapes access to future assignments and may have a decisive impact on the careers of self-employed persons, along with their livelihoods and rights, none of the exceptions in Article 6(3) apply.

- **AI-based vision monitoring system intended to be used for pilot recruitment**
  An AI-enabled system is intended to be used to assess the visual capacities of pilot candidates. Using cameras and sensors the system monitors relevant metrics (e.g., visual acuity and reaction speed) then evaluates whether candidates meet the thresholds required for passenger flights. These results directly determine candidates' eligibility for certain roles. This system falls within the use case of point 4(a) of Annex III, since it is used in recruitment and selection to evaluate candidates' suitability (i.e., in this case whether they are eligible to fly long-haul or short-haul flights). None of the derogations in Article 6(3) apply considering the nature of the tasks being carried out by the AI system and its material influence on the outcome of the decision-making.

- **AI system intended to be used for scoring applicant answers in a recruitment process**
  An AI system is intended to be used to evaluate written or oral responses[46] given by job applicants during an online assessment. The system assigns each applicant a numerical score based on linguistic and substantive criteria, then generates a ranking used to determine who is invited to the interview stage. This system falls within the use case of point 4(a) of Annex III, since it is used in recruitment and selection. The AI performs core evaluative functions and meaningfully impacts the substance of the recruitment and selection. None of the exceptions in Article 6(3) AI Act apply, in particular, considering the fact that the AI system will materially influence the decision-making.

- **AI system intended to be used to support apprenticeship recruitment at a commercial firm**
  A firm uses an AI system to support the recruitment of apprentices. The system is applied to manage and process applications for apprenticeship positions, potentially by screening CVs, matching applicants to roles, or generating shortlists based on pre-defined criteria such as qualifications or age. Although apprenticeships include training elements, the AI is used within the context of hiring for a formal employment relationship and therefore falls within the use case of point 4(a) of Annex III. None of the exceptions in Article 6(3) AI Act apply considering the nature of the tasks being carried out by the AI system.

- **AI system intended to be used to place targeted job advertisements to specific users on social media**
  The system collects and analyses a wide range of data navigation patterns and user characteristics. Advertisers provide targeting criteria, such as age, educational and professional background, or sector, and the system identifies and prioritises potential audiences. The system goes beyond merely matching requirements such as whether the candidate possesses certain professional accreditations or their geographical location. Since the system determines access to employment opportunities through targeted advertising, it falls within the use case of point 4(a) of Annex. Since the system's functioning can materially affect which candidates are able to learn

[46] Oral responses could be evaluated, for example, through an AI system capable of processing video- and audio and interacting with the applicant through an avatar.

about job vacancies, thereby influencing their ability to pursue employment, it cannot benefit from the exceptions in Article 6(3) AI Act.

- **AI system intended to be used by employment agencies to assign candidates to vacancies**
  The system processes candidate data such as information in CVs, including skills, education history, and prior work experience. On the employer side, the system incorporates job requirements, occupational classifications, and labour market data. The system then generates recommendations by ranking candidates for specific vacancies or by suggesting suitable job postings to jobseekers. These outputs are used by caseworkers in the agency, who may rely heavily on the system to manage large volumes of applications. Since the system evaluates candidates in the context of recruitment and access to employment opportunities, it falls within the use case of point 4(a) of Annex III. Since the system's recommendations have a direct bearing on which candidates are referred to employers and which vacancies are presented to jobseekers, it cannot benefit from the exceptions in Article 6(3) AI Act.

- **AI system intended to be used to perform background checks on job applicants during recruitment**
  The system aggregates and analyses multiple types of data. Standard inputs include official records, such as education and professional certifications, employment history, social network history, and credit or financial data, where legally permissible. The system also incorporates open-source and online information. Employers or recruiters receive outputs in the form of composite risk scores, categories such as 'low," 'medium," or 'high risk," or specific alerts highlighting potential issues (e.g., unexplained employment gaps, flagged financial liabilities, or controversial online activity).
  These outputs can be used as filters in high-volume hiring, where candidates flagged as 'high risk" may be deprioritized or excluded before a caseworker reviews their file. While human review is formally part of the process, in practice the system's output heavily influences which candidates advance in the recruitment process, hence materially influencing the outcome of the recruitment process. Since the system materially influences career prospects and is used in the scope of recruitment, it falls within the use case of point 4(a) of Annex III. Since the system performs profiling, it cannot benefit from the exceptions in Article 6(3) AI Act.

b) Practical examples of AI system falling outside the high-risk use case of point 4(a)

- **AI system intended to be used exclusively to identify non-inclusive or discriminatory wording in ad descriptions**
  The system's identification logic is based on patterns and terms defined and reviewed by human experts, and the system flags potentially problematic phrases. At first glance, the system operates within the broad employment domain, but the job ad screening tool is not intended to be used for the recruitment or selection of natural persons and therefore falls outside the use case of point 4(a) of Annex III.

- **AI system intended to be used for employer brand advertisements to present the company as an attractive place to work**
  The advertisements highlight aspects, such as workplace culture, employee benefits, or career development opportunities, but are not tied to any specific job opening and are non-discriminatory. The system may optimise the placement of ads to reach broader or more suitable

audiences, using metrics, such as website traffic, engagement rates, or general demographics. However, the system is limited to employer branding advertisements and does not concern specific job vacancies, and therefore falls outside the use case of point 4(a) of Annex III.

- **AI system intended to be used for employer reputation monitoring**
  A company uses an AI system to scan online platforms and social media for comments or reviews mentioning the employer, with the purpose of tracking the organisation's reputation as a workplace and identifying general trends in how the company is perceived by potential applicants. No analysis or tracking of specific comments or specific users (which are anonymized at collection) are undertaken.Although the AI system is linked to recruitment more broadly, since employer reputation may affect how attractive the company appears to jobseekers, it is not intended to be used for the direct recruitment or selection of natural persons and therefore falls outside the use case of point 4(a) of Annex III.

- **AI system intended to be used for employee onboarding support**
  The system provides personalized information about company policies, training schedules, and answers common questions during their onboarding process. Since the system supports internal HR operations after hiring and does not influence the recruitment or selection of natural persons or affect in any manner their access to work, the system does not fall within the use case of point 4(a) of Annex III. The system may fall within the use case of point 4(b) of Annex III, if it affects the terms of the work-related relationship or feeds into performance evaluations or monitors workers.

- **AI system intended to be used for assisting candidates in tailoring their CV to specific open positions**
  The AI system analyses the candidate's CV along with the description of the open position provided by the candidate. Based on these elements, the AI tool recommends changes to the CV of the candidate with the aim of increasing the likelihood of selection for an interview. These recommendations are exclusively shared with the candidate. While the AI system may indirectly impact the success of the candidate in obtaining the desired position, its use is initiated and managed by the candidate, outside of the potential employer's control and occurs outside of the recruitment and selection process. It therefore falls outside the use case of point 4(a) of Annex III.

- **AI system intended to be used for assisting candidates in finding the best available position**
  The system is used by candidates to analyse both job vacancies and information provided by the candidate covering their skills, experience, and professional expectations. Based on these elements, the system ranks job vacancies and recommends the most suitable positions for the candidate. These recommendations are exclusively shared with the candidate. While the AI system may indirectly impact the success of the candidate in obtaining the desired position, its use is initiated and managed by the candidate, outside of the potential employer's control and occurs outside of the recruitment and selection process. It therefore falls outside the use case of point 4(a) of Annex III.

c) Practical examples of AI systems falling within the use case but exempted under the filter mechanism of Article 6(3)

- **AI system intended to be used for verifying professional accreditations of applicants from official registries** (e.g. bar membership number provided by each candidate with official

registries maintained by national or regional bar associations). The outputs of the system are factual: either 'confirmed" or 'not confirmed," with any issues flagged for manual follow-up by HR or legal staff. While the system is applied during recruitment, it does not filter or assess candidates beyond confirming a credential. Because the system does not materially shape candidate selection beyond this binary factual confirmation and performs a clearly defined and limited function, it can be considered to perform a narrow procedural task. It therefore falls under the exception listed in Article 6(3)(a) AI Act.

- **AI system intended to be used for recognising and organising information in CVs** received for an open position and to organise it within an internal database that can be searched by recruiters. Such a system will be used for a clearly defined and limited function and does not have a material impact on the recruitment or selection of the applicant and. It therefore falls under the exception for AI systems intended to perform narrow procedural tasks listed in Article 6(3)(d) AI Act.

- **AI system intended to be used for scheduling interviews**
  The system is used to automate the coordination of interview appointments with job applicants. The system operates by integrating with the company's calendar tools and the availability preferences provided by each candidate. It proposes interview time slots based on mutual availability and logistical constraints, such as time zone differences or maximum daily meetings per recruiter. It also sends reminders to recruiters and candidates a few days before the interview reminding them of the date, time and location of the interview. The system includes a function allowing candidates to indicate specific accessibility needs, such as requests for sign language interpretation, extended interview duration, or alternative formats for communication. These preferences are then automatically incorporated into the scheduling process to ensure the appropriate arrangements are made. While the scheduling system operates in the recruitment context, it does not perform any function that contributes to the selection of candidates. Since the system's purpose is purely logistical and it does not initiate nor influence employment-related assessments, it falls within the exception for narrow procedural tasks listed in in Article 6(3)(a) AI Act.

- **AI system intended to be used to check human patterns in hiring**
  The AI system is used to audit past hiring decisions by analysing anonymized recruitment data, including CV scores, interview notes, and hiring outcomes. The system employs statistical modelling to detect potential biases or inconsistencies. It does not participate in ongoing recruitment or influence current candidate evaluations, nor does it assess or make decisions based on identified or identifiable recruiters' or applicants' personal characteristics. Its role is purely retrospective based on anonymized information and for already completed human assessments. Although it falls within the use case of point 4(a) of Annex III, the system benefits from the exception listed in Article 6(3)(c) AI Act for AI systems intended to detect decision-making patterns or deviations from prior decision-making patterns without replacing or influencing previously completed human assessments.

- **AI system intended to be used for sending personalized acknowledgement emails** acknowledging receipt of applications with the name and pronouns of the candidate who applied. Such a system does not influence in any way the likelihood of the candidate being selected for the position. It falls within the exception for AI systems intended to be used to perform narrow procedural tasks listed in Article 6(3)(a) AI Act.

3.4.3. Point 4(b): AI systems intended to be used to manage work-related relationships

(255) Point 4(b) of Annex III classifies as high-risk AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics, or to monitor and evaluate the performance and behaviour of persons in such relationships.

(256) These AI systems concern situations taking place after the recruitment and selection process, and encompass the exercise of certain managerial prerogatives and the organisation of work throughout the duration of the employment or contractual (for self-employed) relationship up until its termination.

(257) AI systems in workplace management, although capable of enhancing efficiency and consistency, can also exert decisive influence over workers' livelihoods, future career prospects and rights, and can lead to risk of discrimination. Using AI to manage or make decisions about the workforce is not unlawful per se under the AI Act, but its risks, in particular concerning transparency, responsibility and structural power imbalance justifies classifying certain AI systems as high-risk system under point 4(b) of Annex III and subjecting them to the requirements and obligations provided in Chapter III AI Act[47].

i. AI systems intended to be used to make decisions affecting terms of work-related relationships

(258) The term 'decisions' used in point 4(b) of Annex III should be understood in a functional, rather than a formalistic sense (focusing on substance over form). In the context of employment relations, a decision is any act or omission[48] attributable to the employer that produces material effects on the worker's contractual position or relationship or the modalities of its work. It is not limited to unilateral modifications of contract or relationship in the strict sense, but extends to operational determinations that materially affect the enjoyment by the worker of essential rights and obligations under the contract or relationship. The terms 'intended to be used to make decisions' should be understood as including both cases where the AI system takes the decision in an automated manner and cases where a human operator formally takes a decision, but significantly relies on the output of the AI system.

(259) As regards the words 'terms of work-related relationships' used in point 4(b) of Annex III, these are the fundamental elements to the work contract or relationship that, if they were not present or were different, might have resulted in one or the two parties not consenting to the contract or relationship. This encompasses those conditions that define the balance of reciprocal rights and duties of employer and employee, including working conditions, such as pay entitlements, working time arrangements, leave rights, and resting periods. The EU acquis (including the Directive on

[47] The AI Act rules on classification of high-risk AI systems and the relevant requirements and obligations are directly and horizontally applicable to operators. However, without prejudice to the full and uniform application of the rules under the AI Act, even in cases where their AI systems fall within the filter, operators should be aware that they may be subject to obligations arising from other EU legal instruments, such as the GDPR. For example, in the context of platform work, the Platform Work Directive is of particular importance.

[48] The functional reading of 'decision" in employment law encompasses not only formal acts but also omissions producing binding effects on the worker's position. A 'failure to promote" is a legally relevant determination: see Case C-409/95, Marschall, EU:C:1997:533, Case C-407/98, Abrahamsson and Anderson v Fogelqvist, EU:C:2000:367.

Transparent and Predictable Working Conditions)[49] and Member State labour law, and should be considered when ascertaining which elements fall within the scope of 'terms of work-related relationships'. Decisions on such terms are not limited to unilateral modifications of the contract or relationship in the strict sense, but extend to determinations that materially affect the enjoyment of the rights and obligations of the worker arising from the abovementioned fundamental elements (*e.g.,* denial of a leave request or a significant change to regular working hours).

(260) The term 'work-related relationships' includes employment relationships but also self-employment, including those contractual relationships of self-employed persons providing services through platforms (see Recital 57) and other solo self-employed persons who are in a situation comparable to workers.

(261) The training entitlement provided by the employer is an 'essential aspect of the employment relationship' under Article 4(2) of Directive Transparent and Predictable Working Conditions[50]. However, optional or ancillary training with no entitlement and no legal or collectively agreed obligation does not automatically fall within the use case of point 4(b) of Annex III. For the purpose of high-risk classification, training acquires decisive legal significance where completion or assessment is made a condition for advancement or promotion, or it is otherwise linked to remuneration, grade or continued employability and keeping the job. In such cases, its relevance becomes a determinant of career progression or continued employability. If an AI system evaluates performance in training modules, and such an evaluation feeds into performance appraisals, continued employability, or eligibility for higher-grade positions, it should be considered to fall within the use case of point 4(b) of Annex III.

(262) However, it is equally important to recognise that not every day-to-day managerial or operational organisational adjustment amounts to 'decisions affecting terms of the work-related relationship' within the meaning of point 4(b) of Annex III. To fall within that use case, the decision needs to reach a threshold of significance. A functional interpretation of point 4(b) of Annex III in light of Recital 57 AI Act cannot be stretched to include all day-to-day or operational decisions. While influencing the factual conditions under which work is carried out, decisions that do not materially alter the rights or obligations arising from the underlying contract or work relationship do not constitutes 'decisions affecting terms of the work-related relationship' within the meaning of point 4(b) of Annex III. This includes individual operational decisions taken by managers on a day-to-day basis within the limits of those 'terms of the work-related relationship', such as allocation of office space and break or lunch time within the context of an assigned shift (as long as no changes occur to the total break and lunch time enjoyed by the worker).

ii. Promotion and termination of work-related contractual relationships

(263) The terms 'promotion and 'termination of work-related contractual relationships" used in point 4(b) of Annex III should be understood as any act or omission attributable to the employer that produces effects on the worker's position by, respectively, elevating grade, responsibilities, remuneration or access to career development, or any element that would contextually lead to an

[49] Including the essential aspects of the employment relationship referred in Article 4(2). Directive (EU) 2019/1152 of the European Parliament and of the Council of 20 June 2019 on transparent and predictable working conditions in the European Union, OJ L 186, 11.7.2019, p. 105.

[50] Information on the training entitlement, if any, shall be provided by the employer individually to the worker in the form of a document within one month of the first working day.

effective form of promotion; and any act or omission attributable to the employer which ends the employment relationship or other work-related contractual relationship or deprives the worker of the essential rights and benefits attached to it[51].

(264) As regards 'promotion', EU employment law has recognised that decisions concerning career advancement constitute legally significant determinations[52]. Similar considerations could apply when interpreting that term as used in the context of point 4(b) of Annex III. As regards 'termination', it could be understood in a similar manner to that used in Union law, namely as the final, irrevocable endpoint of the work-related contractual relationship decided by the employer or contracting party. Other forms of removal from work, if not definitive, may qualify for material modifications of the terms of the work-related relationship, and thus may fall within that notion and within the notion of 'termination' as used in point 4(b) of Annex III. Termination includes dismissal, redundancy, and non-renewal of fixed-term contracts when the decision to not renew is AI driven, or any act producing equivalent effects. As previously stated, omissions also constitute elements on which termination can be claimed.

(265) Although non-standard work arrangements and particularly platform work might blur the distinction between 'suspension', 'deactivation' and 'termination', where an AI system definitively suspends a platform account, the effect is to deprive the individual of access to their professional activity, irrespective of contractual form. Lengthy or frequent suspensions of access to the platform may produce similar effects. More generally, the functional equivalence between dismissal of an employee and termination or suspension of a contract with a nominally self-employed person[53] confirms that determinations on contract termination, by act or omission, may amount to restrictions on access to self-employment covered by point 4(b) of in Annex III.

(266) While termination is the decision with the most far-reaching consequences in the employment setting, the filter mechanism under Article 6(3) AI Act may still apply to AI systems falling within the use case of point 4(b) of Annex III. For example, where an AI system merely keeps a record and flags to the appropriate manager the imminent lapsing of a fixed-term contract before its end point, free from discretionary consideration, evaluative judgment, and without suggesting a decision, the outcome follows directly from the contract itself and not from a decision of the AI system. In such instances, the system does not alter the rights of the worker in substance and therefore should not be considered as high-risk.

iii. AI systems intended to be *used to allocate tasks based on individual behaviour or personal traits or characteristics*

---

[51] Constructive dismissal is not an autonomous concept of Union law, but it is widely recognised in Member States' labour law. For example, in Spain, Article 50 of the Estatuto de los Trabajadores allows an employee to terminate the contract with entitlement to compensation where the employer's conduct entails a 'serious breach" of obligations, such as unilateral downgrading of conditions or harassment.

[52] Directive 2006/54/EC, identifies 'promotion" as a protected domain alongside*, inter alia*, access to employment, self-employment and training.. Also See Case C-409/95, Marschall, EU:C:1997:533, Case C-407/98, Abrahamsson and Anderson v Fogelqvist, EU:C:2000:367, both concerning the application of sex equality rules to promotion decisions. While centred on gender discrimination, these cases illustrate the Court's broader approach in treating promotion as a legally significant employment determination.

[52] In Case C-715/20, K.L, EU:C:2024:139 the Court held that fixed-term workers must be afforded reasons for termination equivalent to those required for permanent employees, thereby recognising the possibility of a functional equivalence of non-renewal and dismissal.

[53] Union equality law expressly protects not only 'access to employment" but also 'access to self-employment" and to occupation more broadly: see, as referred before, Directive 2000/78/EC and Directive 2000/43/EC.

(267) The terms 'intended to be used to allocate tasks based on individual behaviour or personal traits or characteristics' in point 4(b) of Annex III should be read in conjunction with Recital 57 AI Act, which clarifies that such systems may have a significant impact on future career prospects, livelihood and rights of the worker. An allocation of tasks is not just an operational arrangement, but may be a determinant of professional development. For instance, the distribution of more complex, visible or lucrative assignments may open pathways to advancement, while the allocation of repetitive or less valued tasks may in practice preclude promotion and potentially affecting current or future income.

(268) If an allocation of tasks is driven by taking into account individual behaviour or personal traits, the risk of structurally disadvantaging certain groups is increased, in addition to dignity, data protection, and privacy concerns. This is also reflected in Recital 57 AI Act, which clarifies that such systems '*may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation'*.

(269) The scope of point 4(b) of Annex III should be understood to cover any individual task allocation 'based on individual behaviour or personal traits or characteristics', which may include data based on personality testing, behavioural scoring, or inferred productivity traits.

(270) Behavioural indicators, such as punctuality, responsiveness to customer requests, reliability metrics, or performance ratings, fall within the scope of 'personal traits or characteristics'. AI systems that, for instance, withhold access to delivery slots from workers with lower acceptance rates or slower response times or that rank self-employed external lawyers from a pool based on response time and performance ratings provided by internal company counsel condition work opportunities on such behavioural profiling.

(271) The dividing line between individual behaviour or personal traits and characteristics, and those that are not, is whether the attribute in question pertains to the worker's personal traits or social identity, rather than to neutral, objective and external factors that preclude the execution of the required tasks, such as unavailability or inadequate location[54].

(272) Task allocation systems that rely only on objective, neutral, and external criteria tied directly to the requirements of a job fall outside the scope of the use case listed in point 4(b) of Annex III. Objective, neutral, and external criteria cannot be proxy for nationality or ethnicity. These include attributes that do not pertain to the worker's individual behaviour, personal traits or social identity, and that are also not covered by the EU non-discrimination acquis. For example, an AI system allocating tasks based on availability as indicated by workers in scheduling tools or distributing assignments according to possession of a required professional accreditation, such as a forklift permit or professional bar accreditation, would not constitute reliance on personal traits within the meaning of point 4(b) of Annex III. Similarly, AI systems assigning work based on geographical proximity to a delivery location should generally not be classified as high-risk.

iv. AI systems intended to be used to monitor and evaluate the performance and behaviour of persons in such relationships

[54] Characteristics such as those protected by the fundamental right of non-discrimination under Article 21 of the Charter (sex, age, disability, etc.) are clearly covered, among others.

(273) AI systems can considerably extend an employer's means to supervise, monitor and evaluate the performance and behaviour of workers or other persons in work-related relationships. The deployment of such systems is not per se unlawful: managerial oversight is inherent in the employment relationship and employers may legitimately seek to enhance productivity, protect property, or ensure workplace safety. However, such deployment can raise concerns of privacy and personal data protection, but also concerns related to health, safety, discrimination, and dignity in the workplace.

(274) The terms 'to monitor and evaluate the performance and behaviour of persons in such relationships' used in point 4(b) of Annex III must be understood as an autonomous high-risk category. The conditions of 'monitor' and 'evaluate' are alternative and they cover AI systems intended to monitor 'or" evaluate workers' performance or behaviour systematically, including during probationary periods[55], regardless of whether this affects a formal term contractually established, such as pay or working time.

(275) The notion of 'performance' includes quantitative productivity measures, such as the number of tasks completed or output speed. It also includes qualitative productivity measures such as the quality of work[56]. For example, AI systems that automatically rate workers on the number of deliveries per hour fall under that notion. So should qualitative indicators, such as feedback scores, performance assessments, appraisals or rankings generated by AI systems that feed directly into employee files.

(276) The notion of 'behaviour' may encompass punctuality, adherence or potential adherence to workplace rules (e.g., employee risk profiling), responsiveness to clients, patterns of interaction with colleagues, and engagement with trade unions[57]. An AI system that assesses (including potentially downgrading) workers for low acceptance rates of shifts or for declining tasks should be considered to evaluate behaviour.

(277) AI systems deployed by employers exclusively to meet external legal or regulatory obligations (for instance transaction logging to comply with financial market abuse rules) should not be considered to monitor or evaluate an individual's performance or behaviour for employment purposes, as long as they are also not used for this purpose. Likewise, out of scope of the notions monitoring or evaluating an individual's performance or behaviour for employment purposes are AI systems deployed purely and exclusively for medical and safety reasons or to protect property and company assets. These AI systems will be not covered by the use case listed in point 4(b) of Annex III.

(278) AI systems that monitor the behaviour or performance of workers in order to support them in the performance of their tasks without being designed to pressure workers to achieve additional productivity, such as by preventing information or products being sent to incorrect recipients though automated flagging, should not be classified as high-risk, provided the AI system only flags potential issues to the worker, not to the employer or any other person within the employer organisation. Similarly, AI systems that convey data on performance, such as systems that

[55] Recital 57 AI Act.

[56] AI systems designed to measure physiological indicators such muscle movement, fatigue, brain waves or heart rate may be considered as high-risk when the abovementioned physiological indicators are used to monitor or evaluate performance. The same will not be the case if the use of the AI system is related only to purely medical or safety reasons.

[57] Without prejudice to the lawfulness of or the monitoring or evaluation of the behaviour under applicable Union and national laws.

aggregate data from successful sales transactions and compare them across company average and only notify them to the worker, should not be classified as high-risk.

a) Practical examples of AI systems falling within the high-risk use case of point 4(b)

- **A retail/logistics company deploys an AI-enabled scheduler to assign shifts, rest periods and on-call windows**
  Inputs provided to the AI system include, among others, behavioural/performance signals (punctuality, non-show history, acceptance/decline rates for offered shifts, customer/manager ratings). The optimiser ranks workers for each slot and auto-allocates shifts, allocating the highest performing workers to the most important shifts. Workers ranked lower receive less important and possibly fewer shifts, lower variable pay, and less predictable patterns. The optimiser also downgrades priority if a worker declines 'priority offers".
  The AI system will evaluate the performance and behaviour of workers and assign tasks based on this evaluation and, as such, falls within the scope of point 4(b) of Annex III. Use of this AI system will affect workers' remuneration, their access to priority tasks and possibly progression. As such, the system cannot benefit from the exceptions in Article 6(3) AI Act.

- **An online tutoring platform deploys an AI system to manage self-employed teacher accounts**
  Inputs include student satisfaction ratings, lesson completion rates, and punctuality logs from the videoconferencing system. The system aggregates these into a 'tutor performance score." If the score falls below 4/5 for three consecutive weeks, the system automatically suspends the tutor's account for a month. If low ratings persist for another review period, the account is permanently deactivated. The practical effect is that tutors can no longer accept lessons, which ends their work relationship with the platform. The system's effect is the functional termination of the work relationship. The term 'termination' used in point 4(b) of Annex III is to be understood in substantive terms, covering any decision that deprives workers of continued engagement.

- **AI system for workload allocation among associates in a law firm**
  The system ingests data on billing hours, turnaround times on prior assignments, responsiveness to emails, and voluntary participation in firm activities (e.g. training, client development). These behavioural inputs are aggregated into a score, which serves as a basis for the allocation of client matters. Since the system allocates tasks based on the individual behaviour of associates, materially affecting both present work conditions and long-term career trajectories, it falls within the use case of point 4(b) of Annex III.

- **AI system for pricing and pay determination in platform work**
  A ride-hailing platform deploys an AI system to dynamically set driver compensation. Inputs include real-time demand, driver acceptance rates, passenger ratings, and average completion times. The system calculates per-ride fares and adjusts individual drivers' pay multipliers. For example, drivers with consistently lower passenger ratings or slower completion times receive a reduced pay coefficient, while highly rated drivers earn bonuses. These adjustments are made automatically and applied in real time, directly affecting income. Human oversight exists formally, but in practice pay levels are determined exclusively by the algorithm and appeals

rarely alter outcomes. Since remuneration decisions fall within the terms of a work-related relationship, the system falls within the use case of point 4(b) of Annex III[58].

- **AI system intended to be used for assignment of civil servants to posts**
  A public administration uses an AI system to allocate successful candidates (e.g. teachers or doctors) to specific posts after they have passed a competition exam. The system takes into account test scores, geographical preferences, availability of vacancies, and seniority. It generates final assignment lists that determine which candidate goes to which post. Appeals are possible, but in practice the AI system's allocation output is decisive, as administrative services rely on the system to finalise placements. Since the system is used for the allocation of roles in the public sector, directly and meaningfully determining working conditions and career paths of civil servants, it falls within the use case of point 4(b) of Annex III.

b) Practical examples of AI systems falling outside the high-risk use case of point 4(b)

- **AI system for tracking delivery operations**
  A courier and shipping company uses an AI system to track shipping data and detect potential mistakes in labelling or issues with distribution. The system assesses the content of labels, monitors parcels in transit and detects potential deviations between the expected and actual route taken by the parcel in transit to its destination. If the AI system detects deviations, it will inform only the employee in charge. The employee in charge will then adopt the necessary procedures for correction (if any are needed). As the system's purpose is ensuring smooth workflow operations and contractual compliance, supporting workers in their tasks rather than evaluating workers' performance, the monitoring activity is incidental and falls outside the use case of point 4(b) of Annex III[59].

- **AI system for training performance evaluation**
  A company uses an AI system to assess employees' progress in voluntary training modules by analyzing quiz results and course completion data. The system only provides feedback and learning recommendations to the employee to support individual development. Its function is limited to measuring learning outcomes within a training context, not to appraising job performance, determining promotions, or shaping managerial decisions.

- **AI system for office space optimization**
  A company uses an AI-enabled booking tool to optimise desk allocation in a hybrid workplace by matching employee reservations with available desks or meeting rooms. While the system organises physical workplace resources, it does not allocate tasks, determine promotions, evaluate workers, or affect employment rights.

- **AI system for corporate travel planning**
  A company uses an AI application to optimise business travel arrangements, suggesting cost-effective flights, hotels, and itineraries for employees required to attend meetings or conferences. The AI application's suggestions do not prevent the employee from making alternative choices or even fully manually booking as long as it does not breach objective rules of company policy

[58] An AI system may be used to dynamically set prices for end users without necessarily falling within the scope of Annex III, point 4(b) of the AI Act. However, for this to occur the AI system may not structure or influence employment conditions (such as pay).
[59] Provided that it is not intended to be used also for performance assessment.

(e.g., maximum prices). The system supports logistics and budgeting, but does not determine the distribution of work, performance evaluations, career progression or termination decisions.

- **AI system suggesting delivery areas to platform couriers**
  A food delivery platform deploys an AI system that recommends geographic areas where demand is expected to be higher, based on factors such as weather, past orders, and real-time traffic data. Couriers receive notifications such as 'high demand expected in Area X between 1-2 pm' but they are free to ignore the suggestions. There are no penalties for declining recommendations, no specific registry of couriers that accepted or rejected the recommendation, and the system does not reduce their access to future tasks. The recommendation tool provides only optional, non-binding supporting information and does not represent task allocation on the basis of individual behaviour.

c) Practical examples for AI systems falling within the use case but exempted under the filter mechanism of Article 6(3)

- **AI system compiling performance records for reporting**
  A manufacturing company uses an AI system to automatically collect from the company's timekeeping application and organize employee monthly attendance records into structured reports and dashboards that the AI system sends to managers at a fixed date. The system does not monitor employees' attendance, generate performance scores, make recommendations, or flag employees, it merely consolidates existing information that was entered by employees in the timekeeping application. Managers continue to perform qualitative evaluations independently. Although the system operates in employment monitoring and falls under the use case of point 4(b) of Annex III, it does not engage in monitoring nor does it make evaluative judgments and falls under the exception for AI systems intended to perform a preparatory task listed in Article 6(3)(d) AI Act.

- **AI system refining human-drafted promotion evaluations**
  A consultancy firm uses an AI-enabled writing assistant to refine managers' promotion reports after the evaluations are fully completed. Managers decide on recommendations, draft justifications, and assign ratings based on company criteria before the AI system improves language clarity, ensures consistency with corporate style, and flags potentially biased wording. At the end of the process, the manager is required by internal policy to double-check the revised evaluations. The system does not change outcomes, scores, or create new content; its role is supportive. Although the system relates to promotion decisions, it does not influence decision-making and falls within the exception for AI systems intended to improve the result of a previously completed human activity listed in Article 6(3)(b) AI Act.

3.5. Access to and enjoyment of essential private services and essential public services and benefits

(279) The access to and enjoyment of certain private and public services and benefits is an area in which the use of AI systems deserves special consideration. Such use may bring about benefits and improve efficiency and the quality of services. Such use may also seriously impact the access to and enjoyment of such essential services if the use of the AI system results in discriminatory or inaccurate outcomes or pose other risks to fundamental rights, as explained in Recital 58 AI Act.

3.5.1. Horizontal issues and overview of use cases

(280) Point 5 of Annex III lists four high-risk use cases within the area of the access to and enjoyment of essential private services and essential public services and benefits that are classified as high-risk:

(a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services;

(b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud;

(c) AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance;

(d) AI systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of, emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems.

(281) While the AI Act does not define essential public and private services, Recital 58 AI Act explains that these should be understood as services and benefits that are necessary for people to fully participate in society or to improve their standard of living.

3.5.2. Point 5(a): Evaluation of the eligibility of a natural person for essential public assistance benefits and services, and the granting or denying such benefits and services

(282) Point 5(a) of Annex III classifies as high-risk AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services. Such use may result in the system taking or supporting decisions by or on behalf of public authorities that evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as grant, reduce, revoke, or reclaim such benefits and services. If not developed or used correctly, AI systems intended to be used for such purposes may include biases or errors, possibly falsely evaluating a natural person as ineligible to receive benefits, singling them out for further inspections, or putting them in a less prioritised category. To address such risks, such systems are classified as high-risk and subjected to safeguards to ensure that they work as intended and are accurate, safe, and do not discriminate.

(283) For such an AI system to be classified as high-risk pursuant to point 5(a) of Annex III AI Act it must be intended to be used by or on behalf of public authorities: (i) to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services; or (ii) to grant, reduce, revoke, or reclaim such benefits and services; or (iii) for both purposes.

(284) The conditions that an AI system must fulfil to be classified as high-risk pursuant to point 5(a) of Annex III and related concepts are analysed in more detail in the following subsections.

i. The concept of 'public authorities' and 'on behalf of authorities'

(285) Point 5(a) of Annex III provides that the AI system must be intended to be used by public authorities or on their behalf.

(286) The AI Act does not define the concept of public authorities. Inspiration may be drawn from the CJEU case-law on the concept of a public authority. In its case law, the CJEU has defined the concept of public authorities (for the purposes of Directive 2003/4) as administrative authorities that form part of the public administration or the executive of the State at any level, which includes legal persons governed by public law set up by the State and which it alone can decide to dissolve[60]. Additionally, entities that are governed either by public law or private law are also administrative authorities in case they perform services of public interest and are 'vested with special powers beyond those which result from the normal rules applicable in relations between persons governed by private law'[61]. EU institutions, bodies, and agencies are also public authorities.

(287) As regards the terms 'on behalf of" used in point 5(a) of Annex III reference is made to Section 2.5. above.

ii. The concept of 'essential public assistance benefits and services'

(288) Recital 58 AI Act clarifies that essential public assistance benefits and services are those benefits and services for which natural persons apply, or which natural persons receive that are necessary for them to fully participate in society or to improve their standard of living. Such natural persons will typically be dependent on the benefits and services for which they apply and be in a vulnerable position in relation to the competent public authorities. The recital gives an illustrative list of the main types of such public services and benefits that could be considered to fall within the scope of point 5(a) of Annex III. These include[62]:

1. Healthcare services (such as long-term care services);

2. Social security benefits (such as sickness benefits; maternity and equivalent paternity benefits; invalidity benefits; old-age benefits; survivors' benefits; benefits in respect of accidents at work and occupational diseases; death grants; unemployment benefits; pre-retirement

[60] Case C-279/12, Fish Legal EU:C:2013:853, para 51: 'Entities which, organically, are administrative authorities, namely those which form part of the public administration or the executive of the State at whatever level, are public authorities for the purposes of Article 2(2)(a) of Directive 2003/4. This first category includes all legal persons governed by public law which have been set up by the State and which it alone can decide to dissolve.'

[61] Case C-279/12, Fish Legal EU:C:2013:853, para 52: 'The second category of public authorities, defined in Article 2(2)(b) of Directive 2003/4, concerns administrative authorities defined in functional terms, namely entities, be they legal persons governed by public law or by private law, which are entrusted, under the legal regime which is applicable to them, with the performance of services of public interest, inter alia in the environmental field, and which are, for this purpose, vested with special powers beyond those which result from the normal rules applicable in relations between persons governed by private law.'

[62] Services and benefits are mentioned in Regulation (EC) No 883/2004 on the coordination of social security systems, 2019 Council Recommendation on access to social protection for workers and the self-employed, the 2023 Council Recommendation on adequate minimum income for active inclusion, and the 2008 Commission Recommendation on the active inclusion of people excluded from the labour market.

benefits; family benefits; long-term care benefits; minimum income benefits; housing benefits; benefits to access essential services (e.g. water, energy, digital communications));

3. Social services (such as social assistance services, employment and training services, housing support and social housing, childcare).

(289) Certain public support measures, which are not public benefits or services as such do not qualify as essential according to the use case listed in point 5(a) of Annex III. For example, tax remission is excluded from that use case, since it is not a service or benefit as such, even if it may provide financial support for beneficiaries.

iii. The concept of evaluating the eligibility of a natural person

(290) There are various types of public assistance benefits and services provided in the Member States, all with differing ways to evaluate a natural person's eligibility to claim them. The evaluation of eligibility should be understood as evaluating and deciding on the possibility of a natural person to receive the benefit or service, but also in terms of the level of benefit or service received. Such an evaluation is generally based on some pre-defined criteria and will be carried out prior to the decision to grant or deny the benefits of services at issue. Once eligibility is determined, the actual decision to grant or deny the benefits or services will be taken. The evaluation for eligibility may also be carried out after a preliminary decision has been taken to grant or deny such benefits and services. In such a situation, the decision to grant or deny will be confirmed by evaluating the person's eligibility. This may in turn lead to situations in which a natural person has received too many assistance benefits and needs to pay them back or has received too few assistance benefits and they need to be supplemented.

iv. The concept of 'grant or denial' of public assistance benefits and services

(291) A range of decisions concerning the grant or denial of public assistance benefits and services may fall within the use case listed in point 5(a) of Annex III. This follows from the use of the terms 'grant, reduce, revoke, or reclaim', which includes all possible scenarios related to such decisions. For the sake of clarity, it should be noted that Recital 58 AI Act also mentions the denial of public assistance benefits and assistance. While this is not explicitly stated in point 5(a) of Annex III, a holistic approach suggests that an AI system intended to be used to deny a natural person public assistance benefits and/or services (and not just a reduction, revocation or reclamation of previously granted benefits and/or services) also falls within the use case listed therein.

v. The link between the eligibility evaluation and the grant or denial of essential public assistance benefits and services

(292) AI systems intended to be used by or on behalf of a public authority solely to evaluate the eligibility of a natural person to receive essential public assistance benefits and services will be classified as high-risk, even if the system is not subsequently used to grant or deny those benefits and services. It is in fact often the case that AI systems are used solely for this purpose, without the system taking decisions regarding the grant or denial of benefits or services. Similarly, an AI system intended to be used solely to grant, deny, reduce, revoke, or reclaim such benefits and services also falls within the use case, without the need for that system to be involved in the prior eligibility evaluation.

(293) AI systems intended to be used by or on behalf of public authorities to grant a natural person essential public assistance benefits and services following a positive evaluation of their eligibility, thereby improving their standard of living and livelihood, will also be classified as high-risk pursuant to point 5(a) of Annex III. That remains true if the grant follows an incorrect evaluation of a natural person's eligibility for such benefits and services, which consequently may lead to the denial, reduction, revocation, or reclamation of the benefits and services previously granted, having a negative impact on the person's standard of living and livelihood.

a) Practical examples of AI systems falling within the high-risk use case of point 5(a)

Automated decisions determining eligibility

- An AI system intended to decide on the grant of unemployment benefits in individual cases. The system analyses whether the person qualifies for the benefit, during which period and in which amount, and makes a recommendation to a case handler about the eligibility and the receiving of the benefits. Such an AI system is high-risk, because it is intended to evaluate a natural person's eligibility, and makes a recommendation on the granting or denial of these benefits.

- An AI system intended to assess a natural person's eligibility for social benefits following an application. The system processes application data and cross-references external databases, after which it generates a decision on the applicant's eligibility for social benefits based on the given data. Such an AI system is high-risk, because it is intended to evaluate a natural person's eligibility and generates a decision on their elgibility.

- An AI system intended to be used by public administrations to evaluate a natural person's eligibility for social housing or unemployment benefits through a scoring system that is not a prohibited practice covered by Article 5(1)(c) AI Act. The system draws on demographic, behavioural, and financial data to predict the likelihood of fraud or long-term dependency. Such an AI system is high-risk, since it aids in the evaluation of a natural person's eligibility and materially influences decision about whether the applicant will receive the benefits and services.

Prioritisation

- An AI system intended to evaluate applications for social housing. The system evaluates the profiles of applicants for eligibility, urgency level and prioritisation for specific social housing units based on income, household size, age, employment status and location. The system can substitute or influence human decision-making and is high-risk, since it has a direct impact on access to essential housing benefits.

- An AI system intended to prioritise the allocation of home-care services. Such systems may be used by local authorities to determine the distribution and prioritization of limited in-home care hours among eligible persons. Such an AI system is high-risk, since it materially influences the access to essential care services for elderly persons or persons dependent on such care, thereby potentially affecting their fundamental rights and well-being.

- An AI system intended to assess the eligibility of applications for access to unemployment support or income support schemes, administered by public authorities, and prioritise those applications accordingly in a context of limited resources or processing capacity. Such an AI system is high-risk, since it evaluates applications for essential public assistance benefits and

services and it materially influences the granting, timing or effective access to such benefits and services through prioritisation.

Supportive tools for human review determining eligibility or access

- An AI system intended to analyse applications for essential public assistance benefits submitted by natural persons (e.g. sickness benefits) in order to detect potential irregularities and/or inaccuracies, or fraud indicators and to flag applications for further investigation by a public authority. When an application is flagged, a human case handler takes over to assess whether the claim is fraudulent. Such an AI system is high-risk, since it is used in the context of evaluating eligibility for essential public assistance benefits and materially influences access to such benefits. In particular, flagging determines whether applications are subject to further scrutiny, delay, suspension or potential refusal and is therefore instrumental to decisions affecting the granting, continuation or effective access to those benefits.

- A chatbot intended to answer legal questions of a case handler that are specifically related to the evaluation of an application of a natural person to receive essential care benefits or services administered by a public authority. The case handler can grant or refuse the benefits to which the natural person applied, while remaining responsible for the final decision, based on the answers given by the chatbot that are personalised to the specific case/individual eligibility assessment. Such an AI system is high-risk, since the case handler's decision on the eligibility of the natural person to receive care benefits or services is materially influenced by the legal answers given by the chatbot.

- An AI system is intended to assess applications for healthcare in order to determine whether an in-depth examination of the application should be carried out by an external body. Even if the decision to forward is taken by a case handler, such an AI system is high-risk, since the system preliminary assessment acts as a decisive step for further examination determining the access to healthcare services.

Proactive invitation with an eligibility check

- An AI system intended to be used by public authorities for health preventive screenings to suggest personalised invitations for preventive screening (such as mammograms), based on population segmentation, performing also an evaluation of the eligibility for the preventive screening. Such an AI system is high-risk, since it evaluates the eligibility of a person to do a preventive screening (a healthcare service), even if this is done through a proactive invitation.

b) Practical examples of AI systems falling outside the high-risk use case of point 5(a)

Proactive invitations without an evaluation of the eligibility

- AI systems intended to proactively identify persons in need of preventive care. Such an AI system falls outside the use case of point 5(a) of Annex III, since it only identifies persons in need of preventive care and does not determine the eligibility of the identified persons, provided that the system's outputs are not used to prioritise, exclude or otherwise influence access to such a service.

- AI systems intended to match persons with the public support services that fit them best based on their needs, using anonymised data to suggest and pre-fill applications for support services. Such an AI system falls outside the use case of point 5(a) of Annex III, since it is not intended to evaluate the eligibility of a natural person, but to support the delivery of public support services.

Case-handler allocation

- AI systems intended to merely inform by which body or competent person an application for essential public assistance benefits is (further) to be assessed. Such an AI system falls outside the use case of point 5(a) of Annex III, since it only recommends who should assess the application, without an actual evaluation of the eligibility.

Eligibility checks and reimbursement of costs of legal persons

- AI systems intended to assess applications or claims from companies for reimbursement of costs, but not from natural persons. Such an AI system falls outside the use case of point 5(a) of Annex III, since it does not assess applications or claims from natural persons.

c) Practical examples of AI systems falling within the use case but exempted under the filter mechanism of Article 6(3)

Chatbots answering factual questions of a case handler

- A chatbot intended to answer factual questions of a case handler that are related to the evaluation of an application of a natural person to receive healthcare benefits (such as the age of the natural person). The case handler can grant or deny the benefits to which the natural person applied, based on the answers given by the chatbot. Such an AI system falls within the use case of point 5(a) of Annex III, since the case handler's decision on the eligibility of the natural person to receive healthcare benefits depends on the answers given by the chatbot. However, since the system only provides existing and factual information in a structured manner, without evaluating this information for the eligibility of a natural person's application for healthcare benefits, and the case handler must review the information made available by the chatbot to ensure that the decision is not based solely on the output of the AI system, it falls under the exception for AI systems intended to perform narrow procedural tasks listed in Article 6(3)(a) and (d) AI Act.

Supportive tools for human review

- AI systems intended to summarise medical reports which will be used by a case handler as the basis for their decision to grant or deny healthcare benefits. Such an AI system falls within the use case of point 5(a) of Annex III, since it is intended to be used for the access to healthcare services. However, since the system is limited to summarising the information in the reports and the case handler must review the relevant information in the reports before taking a decision, it falls under the exception for AI systems intended to perform narrow procedural tasks listed in Article 6(3)(a) and 6(3)(d) AI Act.

Language tools

- AI systems intended to translate applications for public assistance services made in a foreign language. Such an AI system falls within the use case of point 5(a) of Annex III, since it is intended to be used for the evaluation of a natural person's application for public assistance benefits. However, since the translation of applications for assistance benefits and services is an unavoidable step in the process, but it is not decisive for the evaluation of the eligibility of those applications, the system falls under the exceptions for AI systems intended to perform narrow procedural and preparatory tasks listed in Article 6(3)(a) and (d) AI Act.

- AI systems intended to be used in conversations between a case handler and a natural person who wants to apply for public assistance services and benefits by converting speech into text. The system creates a summary of the conversation that will be used to make a decision concerning the eligibility of a natural person. Such an AI system falls within the use case of point 5(a) of Annex III, since it is linked to the evaluation of a natural person's application for public assistance benefits and services. However, in so far as the case handler is present during the conversation and is able to check the summary made by the system, so that the output is only a supporting but not decisive element for his or her decision, the system falls under the exception for AI systems intended to perform only narrow procedural tasks listed in Article 6(3)(a) and 6(3) (d) AI Act.

3.5.3. Point 5(b): AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score

(294) Point 5(b) of Annex III classifies as high-risk AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score. The rationale for the inclusion of this use case in Annex III is that the determination of creditworthiness or a credit score often determines access to essential private services, so that the use of an AI system in that context may give rise to risks for the health, safety or fundamental rights of the natural person seeking such access, especially in cases of discrimination as described in Recital 58 AI Act.

i. Creditworthiness evaluation and credit-scoring

(295) Point 5(b) AI Act covers AI systems intended to be used for two distinct use cases: the evaluation of creditworthiness and the establishment of a credit score. The AI Act defines neither use case.

(296) The evaluation of creditworthiness refers to the assessment of a natural person's ability and willingness to fulfil its contractual obligations to pay for the services provided or the credit granted. Such an evaluation may be based e.g. on demographic data (such as age, the level of education or the place of residence) and/or on financial data including payment behaviour, credit history and income and financial variables. A creditworthiness evaluation will normally be carried out by financial institutions for the purpose of obtaining a loan, but it may be carried out in other sectors and for other essential private or public services. A creditworthiness assessment may, for example, be carried out to assess a person's eligibility or access to public assistance benefits and services. In such a case, the AI system should be classified as high-risk pursuant to point 5(a) of Annex III. A credit score may be established for several purposes.

(297) The establishment of a credit score refers to the creation and building of a representation of a natural person's creditworthiness. The establishment of such a score may be based on e.g. demographic data and/or financial data including payment behaviour, credit history and income and financial

variables. The score produced by the system may take various forms, such as a number, a ranking, or a label. A credit score may be established for several purposes. Where an AI system is intended to be used to establish such a score for the purpose of determining the access to financial resources or essential services such as housing, electricity, and telecommunication services, it should be classified as high-risk regardless of other purpose the AI system may have. In that case, the assessment for compliance with the requirements for high-risk AI systems should be limited to the intended high-risk purpose and should not extend to other purposes.

(298) It should be noted that point 5(b) of Annex III only classifies AI systems as high-risk when they are intended to be used for the assessment of creditworthiness of and the establishment of a credit score for natural persons; it does not establish as such a right to obtain credit or access to financial resources or any other essential private service. The conditions that an AI system must fulfil to be classified as high-risk pursuant to point 5(b) of Annex III and related concepts are analysed in more detail in the following subsections.

ii. The relationship between 'to evaluate the creditworthiness' and 'to establish a credit score' as well as 'pricing'

(299) To classify as high-risk pursuant to Article 5(b) of Annex III, an AI system must be intended to be used either to evaluate creditworthiness or to establish a credit score of natural persons, or both. Although establishing a credit score is often part of evaluating creditworthiness, it is sufficient that an AI system is intended to be used for one of those purposes to be classified as high-risk. Each use case in itself may influence the decision-making process and have an impact on the access to the essential private service at issue. For example, both the creditworthiness evaluation and the credit score establishment may directly influence how interest rates are priced or calculated for a borrower. Nevertheless, to qualify as high-risk pursuant to point 5(b) of Annex III, it is not necessary that the system is also intended to be used to calculate a certain price or interest rates.

(300) By contrast, an AI system intended to be used for pricing is not covered by the use case listed in point 5(b) of Annex III, even if it relies on data obtained from a creditworthiness assessment or credit-scoring. However, an AI system which combines the two functionalities in one system in an integrated process (assessing the creditworthiness of natural persons and the credit pricing) will qualify as such a high-risk use case.

iii. Essential private services

(301) A private service is essential if it is necessary for people to fully participate in society or to improve their standard of living. Recital 58 AI Act clarifies that essential private services include access to financial resources and provides, as examples, housing, electricity, and telecommunication services. For other services to be considered an essential private service, they must be equally important to natural persons and the improvement of their standard of living and the exclusion of natural persons from access to such services must have a comparable significant impact on their life, health, livelihood and participation in society as the services mentioned in that recital. Examples of such services may include health and long-term care, other utilities, such as gas and water services, and transport services.

(302) When it comes to the type of financial services[63] that could constitute essential private services, it may be necessary to draw further distinctions based on the general reference to access to financial resources and examples of essential private services mentioned in Recital 58 AI Act. Besides the determination of access to financial resources, only financial services equal or similar to the following services should be considered as essential private services: providing a bank account[64]; payment services, including when credit (e.g. temporary overdraft) is provided as an ancillary feature to support a transaction; the offering of loans and credit; the offering of extension of a credit line or of credit card limit; the offering of mortgage; and public financial services as further described in paragraph 297. For the purpose of the credit-scoring and creditworthiness assessment use case in point 5(b), this list of essential private services does not give rise to an entitlement of the natural persons to those services.

(303) Some public authorities or public financial institutions offer financial services, such as financial support schemes with a credit element (e.g. subsidised loans, guarantees, repayable advances) where creditworthiness may be assessed beforehand. Those public financial services may include publicly backed low-interest or zero-interest loans for first time home buyers or for home renovations, for certain groups of people at risk of exclusion, or be provided in the form of student support schemes or social microcredit schemes. Those public financial services are also considered essential private services within the meaning of point 5(b) of Annex III.

(304) In contrast, the following financial services are not considered essential private services: the acquisition of stocks and securities; access to margin trading; access to complex financial instruments; premium credit cards; and special loans, such as leisure/travel loans.

(305) Since it is the intended use of an AI system that matters when assessing whether it should be classified as high-risk under the use case listed in point 5(b) of Annex III, it is for the provider to demonstrate to the competent market surveillance authority that its system is solely intended to be used for non-essential private services if it wishes that system not to be so classified. If the system is intended to be used for both essential and non-essential private services, it will be classified as high-risk.

iv. Fraud detection exception

(306) Point 5(b) of Annex III specifies that AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score should not be considered high-risk if they are used for the purpose of detecting financial fraud. AI systems may detect anomalous behaviour in credit applications or suspicious patterns in applicant data that could indicate fraud. A typical example of such a system is a tool that uses AI to detect misused, forged, or altered personal identification documents (such as ID cards, driver's licenses, etc.) or other forged or modified documents (such as income statements, bank statements, and the like).

(307) For the exception to apply, fraud detection must be the main intended use of the AI system, preceding all other purposes for which the AI system may be used. This will be the case, for

[63] For example, Article 2(b) of the Distance Marketing of Financial Services Directive (2002/65/EC), considers 'financial services' to include all banking, credit, insurance, pension, investment and payment services.

[64] In practice a creditworthiness assement is not necessarily carried out before opening a bank account. The examples listed only become relevant where an AI system is intended to be used for such an assessment.

example, where the AI system is mainly used for pattern recognition and anomaly detection, rather than for assessing a person's ability or willingness to repay a loan.

(308) If an AI system is intended to be used for fraud detection, that system should be considered to fall outside the use case of point 5(b) of Annex III, even if its output may be used for the creditworthiness assessment or establishing the credit score.

(309) AI systems intended to be used for anti-money laundering and for countering the financing of terrorism ('AML/CFT') are not covered by the exception, since those activities are regulated by other EU legislation and they are not related to financial fraud. Such systems are nevertheless out of scope to the extent their intended use does not cover the assessment of creditworthiness. Nevertheless, AI systems intended to be used for AML/CFT may classify as high-risk AI systems under Point 5(b), if the AI system is functionally linked and simultaneously intended to be used for the evaluation of creditworthiness or to establish a credit-score.

a) Practical examples of AI systems falling within the high-risk use case of point 5(b)

Credit scoring for consumer lending and mortgages

- An AI system intended to create a numerical representation of a natural person's creditworthiness, based on their payment behaviour and income, that is intended to support the decision-making on a consumer credit or a mortgage, which qualify as essential private services.

Credit scores used by third parties other than the deployer

- An AI system intended to establish a credit score deployed by a credit agency, whose resulting scores are shared with a third party for decisions whether to grant a loan/mortgage or access to housing, healthcare or telecommunication services to a natural person. To fall within the use case of point 5(b) of Annex III, it is not necessary that the deployer of the system is identical to the party using the credit score for its decision-making.

b) Practical examples of AI systems falling outside the high-risk use case of point 5(b)

Customer classification and personalised marketing

- An AI system intended to classify customers, for example, to fulfil information obligations, to provide tailored information to customers, to assess the suitability of a product or to make personalised marketing offers, so long as the classification does not play a part in the assessment of the creditworthiness of a natural person.

- An AI system intended to perform advanced segmentation to gain a deeper understanding of customer groups and how they use certain services based on demographic and behavioural data. The same may be true for pricing simulations, that are used to test how changes in pricing might affect customer behaviour, competitiveness or profitability, if they are distinct from the AI

system carrying out a creditworthiness assessment. Even though their outputs may be used further downstream, they represent an earlier step in the value chain.

Support before or after a credit decision

- An AI systems intended for customer support related to the assessment of their creditworthiness should not be classified as high-risk under point 5(b) of Annex III, since they do not assess the creditworthiness or establish a credit score of a natural person. These AI systems may assist applicants in understanding or completing the credit application form (e.g. by explaining terminology) or provide dynamic feedback on how specific answers may influence the likelihood of approval. If they are not intended to be used as part of the creditworthiness assessment or credit-scoring process, since they merely support the applicants to prepare their credit application but do not participate in the formal credit-scoring assessment, they fall outside the use case of point 5(b).

- An AI system intended to be used to handle and manage complaints following a decision on loans or health and life insurance, so long as it does not at the same time constitute an evaluation of the creditworthiness or the establishment of a credit score. Such systems usually represent a separate stage of the credit application process where individuals challenge a decision on the credit provision or creditworthiness assessment.

Monitoring of credit exposure

- An AI system intended solely for monitoring credit exposures for internal prudential purposes (to track and analyse credit-related activity, assess borrower risk and detect early warning signs of default or financial distress) after credit is granted should not be classified as high-risk under point 5(b) of Annex III.

Evaluation of a collateral

- AI systems intended to evaluate collateral, so long as the AI system is intended to be used solely in relation to the collateral asset, for instance by assessing its features, its risk factors and/or its feasibility to be sold.

Providing credit or extended margin for leveraged trading products

- An AI system may be intended to be used by financial intermediaries to evaluate the extension of margin credit (whereby clients borrow capital against their existing securities) to existing or prospect clients. Despite being capable of determining access to financial resources to natural persons, such AI systems should not be classified as high-risk under point 5(b) of Annex III, if they are solely intended to be used for providing or extending margin credit as a non-essential private service.

3.5.4. Point 5(c): AI systems intended to be used for risk assessment and pricing in the case of life and health insurance

(310) Point 5(c) of Annex III classifies as high-risk AI systems intended to be used for risk assessment and pricing in relation to natural persons for health and life insurance. Recital 58 AI Act explains that such systems can have a significant impact on a person's livelihood and, if not properly

designed, developed, and used, can infringe their fundamental rights and can lead to serious consequences for their life and health, including financial exclusion and discrimination. The conditions that an AI system must fulfil to be classified as high-risk pursuant to point 5(c) of Annex III and related concepts are analysed in more detail in the following subsections.

i. Definition of risk-assessment and pricing

(311) The high-risk use case listed in point 5(c) of Annex III covers two types of AI systems in relation to natural persons for health and life insurance: those that perform a risk assessment and those that price insurance premiums, or both. To qualify as high-risk system under point 5(c) of Annex III it is not necessary that the system is intended to be used solely for these use cases.

(312) Risk assessment should be understood to entail the evaluation of a natural person's risk profile to determine whether to offer, deny, revoke or deliver services related to health and life insurance, in particular full/partial insurance coverage, including the establishment or change of policy terms and conditions (e.g. coverage, exclusions, deductibles, policy limits). The AI system may carry out the risk assessment with a view to any of the steps of access and enjoyment of these insurance services as described above.

(313) Pricing should be understood to refer to the methodologies and criteria used to determine insurance premiums as an integral part of policy terms and conditions. Usually, a risk assessment will be a prerequisite for pricing. However, the AI system need not be intended to be used both for the risk assessment and pricing, since a system performing an assessment may result in access being denied or the performance of an insurance contract being affected in a manner that justifies its classification as high-risk, set out in Recital 58 AI Act.

ii. In the case of health and life insurance

(314) To be classified as a high-risk pursuant to point 5(c) of Annex III, the AI system must be intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance. Other insurance services (e.g. car or motor insurances, home insurance etc.) are not covered by the use case. Insurance-based investment products as defined in Article 4(2) of Regulation (EU) No 1286/2014 are not to be understood as health or life insurance within the meaning of point 5(c) of Annex III.

(315) This means that the AI system's intended purpose (risk assessment or pricing) should be to provide information for a potential decision on the access and enjoyment of a health or life insurance policy. The access to and enjoyment of health and life insurance is not restricted to those cases resulting in the conclusion of an agreement. It covers all steps leading to the conclusion or denial of an insurance policy, including its revocation, or changes to its terms and conditions.

(316) The notion of health and life insurance may differ across Member States for the purpose of point 5(c) of Annex III. The term life insurance may be understood to cover the classes of insurance listed in Annex II of Directive 2009/138/EC. In contrast, point 5(c) of Annex III should not be understood as covering classes of non-life insurance listed in Annex I of Directive 2009/138/EC, with the exception of those listed under points 1 and 2 under Section A of that Annex (classification of risks according to classes of insurance). The risks referred to in those points (e.g. accident, including industrial injury and occupational diseases, as well as sickness) should be considered to be covered

by health insurance services within the meaning of point 5(c) of Annex III, since they usually cover the costs of medical treatment.

(317) The term health and life insurance should also be considered to cover private long-term care insurance, since that constitutes a health insurance service within the meaning of point 5(c) of Annex III. Such insurance has a significant impact on a person's livelihood and can lead to serious consequences for their life and health similar to health and life insurance in line with recital 58 AI Act. It should also be considered to cover personal pension products in so far as these can have a significant impact of a person's livelihood in old age.

(318) Credit life insurance contracts should also be considered to fall within the scope of point 5(c) of Annex III, since they constitute life insurance regardless of their function as payment protection insurance (credit insurance). Credit life insurance is typically offered when a person borrows a significant amount of money, such as for a mortgage, car loan, or large line of credit. The policy pays off the loan in the event the borrower dies. In relation to that type of insurance, the risk assessment may take the form of an evaluation of the creditworthiness or the establishment of a credit score of the natural person-borrower.

(319) The health and life insurance covered by point 5(c) of Annex III may be offered on a private or public basis (see above). For example, an AI system intended to be used by a health insurance company based on public law will also fall within the scope of point 5(c) of Annex III, so long as that system is intended to be used to carry out a risk-assessment or pricing with regards to natural persons.

(320) Privately serviced health insurance is seen as an essential private service within the meaning of point 5 of Annex III, even if the Member State in which it is offered has a public health care system that offers universal health care. In this case, the private health insurance would constitute an addition to that public care, for example to cover more treatment options or access to private treatment.

iii. Fraud detection

(321) In contrast to the use case listed in point 5(b) of Annex III, point 5(c) does not provide an exception for fraud detection. Therefore, an AI system intended to be used for risk assessment or pricing in the case of health and life insurance will be classified as high-risk even if it also has a feature that can be used for fraud detection. Only where that feature can be considered to constitute a distinct system in its own right will that system fall outside the scope of point 5(c) of Annex III, while the system intended to be used for risk assessment and pricing in the case of health and life insurance will be classified as high-risk. This is in line with Recital 58 AI Act, which clarifies that systems used for fraud detection should not be classified as high-risk in general.

a) Practical examples of AI systems falling within the high-risk use case of point 5(c)

Risk assessment and pricing

- An AI system intended to be used by an insurer that reviews applications for life insurance, so long as it qualifies as a risk assessment as defined above. This is usually the case if the AI system

processes data provided by the applicant, such as age, health status, family history, lifestyle habits and occupation and relies on mortality tables, that estimate the probability of death for each applicant within a given period. This processing guides whether the insurer accepts the application and what conditions apply.

- An AI system intended to be used by an insurer to predict the expected annual medical cost for a risk group. The AI system may calculate and add expenses for administration and a profit margin. The final figure becomes the premium charged to members of that group.

b) Practical examples of AI systems falling outside the high-risk use case of point 5(c)

Claims management

- AI systems intended to be used for claims management in case of health insurance products in case the insured event happens. This is because these systems are intended to to verify whether a claim is valid under the policy terms or to determine the amount to be paid, they do not fall within the use case of point 5(c) of Annex III. These use cases are distinct from carrying out a risk assessment or pricing, even though their outcome might affect the enjoyment of the health insurance. In the same vein, those systems may fall outside the use case of point 5(c) of Annex III if they are intended to be used in claims management to improve the quality of claims processing and decision-making by contributing to the accuracy, by inter alia the validation of claimant information against various databases.

Product design for life insurance

- AI systems intended to be used in product design for life insurance fall outside the use case of point 5(c) of Annex III, if they are not intended to be used for risk assessment and pricing in individual cases. Those AI systems typically support a data-driven approach to product design by analysing large volumes of demographic, behavioural, and socio-economic data. By identifying emerging customer needs, risk patterns, and coverage gaps, the AI system enables insurers to create tailored life insurance products that are both relevant and competitively priced. For example, these AI systems can detect underserved segments and recommend product features or pricing models suited to their profiles. Scenario simulations and predictive modelling may help to assess the potential impact of new product offerings before launch, reducing development time and market risk. Those AI systems usually represent a prior and separate stage in the value chain of insurance companies. The product design may set the framework on what insurance products are offered and within which pricing framework. However, there is no evaluation of a natural person's risk profile involved to determine whether to offer, decline, revoke or deliver services related to health and life insurance.

3.5.5. Interplay with other Union legislation: Article 144 of Regulation (EU) No 575/2013 (Capital Requirements Regulation) and Article 120 of Directive /2009/13/8 EC (Solvency II Directive)

(322) If an AI system intended to be used to evaluate the creditworthiness of natural persons or establish their credit score is also intended to be used for prudential purposes provided for by Union law to

calculate credit institutions' and insurance undertakings' capital requirements, it will still be classified as high-risk under points 5(b) and (c) of Annex III. This follows from the clear specification in that provision that AI systems intended to be used for the use case listed therein shall only be exempted from high-risk classification if they are intended to be used for the purpose of detecting financial fraud.

(323) The statement in Recital 58 AI Act that AI systems provided for by Union law for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under the AI Act clarifies that AI systems used for those purposes fall outside the use case of point 5(b) of Annex III if they are not intended also to be used for the assessment of creditworthiness of and the establishment of a credit score for natural persons. An example of such a system falling outside the use case of point 5(b) of Annex III is an AI system intended to be used by a financial institution to calculate solely the risk-weighted exposure of portfolios of loans to natural persons under the internal ratings-based approach (IRB) pursuant to Article 143 of Regulation (EU) No 575/2013, but the same system is not intended to be used for credit scoring or the evaluation of creditworthiness of natural persons. Such (normally) internal AI systems are not high-risk in and of themselves as a result of the use test mentioned in Article 144(1)(b) of Regulation (EU) No 575/2013[65] and in Article 120 of the Solvency II Directive.

(324) In this light, it should be recalled that it is not relevant what the main purpose of an AI system is for high-risk classification purposes. Provided one of the purposes of the system is the use case listed in point 5(b) of Annex III, the AI system should be classified as high-risk, regardless of the fact that the same AI system is also used for internal ratings and default and loss estimates under the IRB approach for the purpose of calculating own funds requirements.

(325) If, however, financial institutions use different AI systems for both operations (e.g. a bank uses an AI system for credit-scoring that takes the IRB system as an input or uses an IRB system that takes the credit scoring as an input, but deviates in some elements from the IRB system), the AI system used for IRB purposes should not be classified as high-risk, since it is only the credit-scoring system that is intended to be used for the use case listed in point 5(b) of Annex III, AI Act. The same principles apply to insurance undertakings that widely use internal models and where those models play an important role in their system of governance in accordance with Article 120 of the Solvency II Directive.

(326) Whether there are one or two underlying AI systems within the meaning of the use cases listed in Annex III requires a case-by-case assessment. Market surveillance authorities and providers must identify the underlying AI system(s) and their boundaries based on the definition of an AI system under Article 3(1) AI Act, drawing inspiration from the Guidelines on the definition of an artificial intelligence system[66]. This may require, inter alia, describing the hardware and software components of the AI system, as well as its objectives and its functionalities with a view to inputs and outputs, and its interface with other AI systems or its environment.

---

[65] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012.

[66] Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) (OJ L, 2024/1689).

(327) Where financial institutions, as a provider of a high-risk AI system falling within the use case of points 5(b) of Annex III, implement model changes of already approved IRB systems in a non-live production environment, this should not be considered as putting the AI system into service pursuant to Article 3(11) AI Act until approval is granted, since until then there is no intention, in practice, to deploy the AI system as implemented in the non-live environment.

(328) In any case, high-risk AI systems placed on the market or put into service by financial institutions before the date of application of the high-risk rules are grandfathered and do not need to comply with the requirements and obligations, unless as from that date those systems are subject to significant changes in their design (see Article 111(2) AI Act and Section V below, as well as the relevant Union legislation on prudential requirements). For this purpose, the definition of material change to the credit-scoring within the IRB Approach as set out in the relevant Union legislation will be relevant in the context of the assessment of whether a high-risk AI system in point 5(b) of Annex III is subject to a significant change in design under Article 111(2) AI Act.

3.5.6. Point 5(d): Evaluation and classification of emergency calls or the dispatching or establishing prioritisation of emergency first response services

(329) Point 5(d) of Annex III classifies as high-risk AI systems intended to evaluate or classify emergency calls by natural persons or to be used to dispatch or to establish priority in the dispatching of emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems. If not developed or used correctly, the use of such systems can have risks concerning very critical situations for the life and health of persons and their property. To address those risks, such systems are classified as high-risk and subjected to safeguards to ensure they work as intended and are accurate, safe and do not discriminate.

(330) Five types of AI systems fall within the uses cases listed in point 5(d) Annex III:

(i) AI systems intended to be used to evaluate and classify emergency calls by natural persons;

(ii) AI systems intended to be used to dispatch emergency first response services;

(iii) AI systems intended to establish priority in the dispatching of emergency first response services;

(iv) AI systems intended to be used to dispatch emergency healthcare patient triage systems;

(v) AI systems intended to be used to be used to establish priority in the dispatching of emergency healthcare triage systems.

(331) AI systems that fall within the use cases of point 5(d) of Annex III AI Act and that qualify as a medical device pursuant to Article 2(1) of Regulation (EU) 2017/745 (the Medical Devices Regulation) or as radio equipment pursuant to Article 2(1)(1) of the Radio Equipment Directive fall within the scope of Annex I AI Act and shall also be classified as high-risk pursuant to Article 6(1) AI Act if they meet the conditions of this provisions (See Section III above). If Article 6(1) AI Act is not applicable, AI systems within the scope of the use cases in point 5(d) are classified as high-risk pursuant to Article 6(2) and Annex III of the AI Act.

i. The meaning of 'emergency calls'

(332) The AI Act does not define the notion of 'emergency calls'. Inspiration may be drawn from Article 2(31), (36) and (38) of Directive (EU) 2018/1972 (the European Electronic Communications Code)[67]. Those provisions define the notions of 'call', 'public safety answering point' ('PSAP'), and 'emergency communication'. As regards the latter, emergency communication is classified as '*communication by means of interpersonal communications services between an end-user and the PSAP with the goal to request and receive emergency relief from emergency services*', which is not limited to only calls but can also include text messaging and video. A PSAP is '*a physical location where an emergency communication is first received under the responsibility of a public authority or a private organisation recognised by the Member State*'[68].

ii. The meaning of 'emergency first response services'

(333) The AI Act does not define the notion of 'emergency first response services'. Such services are generally a Member State competence[69] and Member State legislation designates the organisations and types of services that should be considered emergency first response services. In addition, inspiration may be drawn from Article 2(39) of the European Electronic Communications Code, which defines 'emergency service' as those services '*recognised as such by the Member State, that provide immediate and rapid assistance in situations where there is, in particular, a direct risk to life or limb, to individual or public health or safety, to private or public property, or to the environment, in accordance with national law*'. Point 5(d) of Annex III and Recital 59 AI Act provide as examples of such services police, firefighters and medical aid. Such services may also include ambulance services, operation centres for information management relating to, for example, disaster risk management and forecasting, and organisations providing search, rescue, and evacuations.

iii. The meaning of 'emergency healthcare patient triage systems'

(334) Emergency healthcare patient triage systems may qualify as medical devices in so far as they fulfil the definition of a medical device in Article 2(1) of the Medical Devices Regulation. If such systems meet the conditions in Article 6(1) AI Act, they will be classified as high-risk pursuant to that provision and Annex I AI Act and require streamlined and consistent compliance with sectoral laws (see Section III above).

(335) Emergency healthcare patient triage systems that do not constitute medical devices shall be classified as high-risk pursuant to Article 6(2) and point 5(d) of Annex III AI Act.

iv. The meaning of 'forecasting' and 'disaster monitoring'

(336) AI systems can also be used for forecasting or predicting situations where emergency first response services will be needed in the absence of emergency calls from natural persons, e.g. systems alerting

[67] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast). This Directive is currently being revised, with a proposal from the Commission expected in Q1 2026.

[68] Directive (EU) 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

[69] Article 196 of the Treaty on the Functioning of the European Union.

to a situation where emergency first response services are needed. Such systems will only fall within the scope of point 5(d) of Annex III where they are specifically intended to be used to decide when or where to dispatch emergency first response services.

a) Practical examples of AI systems falling within the high-risk use case of point 5(d)

Analysing calls and prioritising interventions

- An AI system intended to be used in emergency response centres where 112 calls are classified to assign the level of urgency and to route responders, using natural language processing. Such an AI system is high-risk, since the system is intended to evaluate and classify the calls, and to establish prioritisation in the dispatching of emergency first response services, including the actual dispatching of the services.

- An AI system is used to analyse emergency calls received by the police and to prioritise interventions according to the urgency and seriousness of the situation through the extraction of relevant information, such as relevant key words. The system assesses the urgency of the situation and the response to be given. Such an AI system is as high-risk, since it is directly involved in the evaluation, prioritisation and dispatching of incoming calls made by natural persons, and the system assesses which response should be given.

Supportive tools for human review

- An AI system intended to provide real-time decision support for emergency first response services call-talkers, effectively enhances human decision-making skills by acting as an assistant to the call-taker, listening for signs or signals of life-threatening emergencies in what the caller is describing. The AI system uses real-time automatic speech recognition technology, creating high-quality transcripts and during the call, the data is analysed and compared with historical data collected from previous emergency calls. Such an AI system is high-risk, since it evaluates the call made by a natural person by assisting the emergency first response services call-taker by helping to classify the call on the basis of the severity of the situation through the listening for keywords that might indicate a medical emergency.

- AI systems intended to determine the nature and severity of emergency situations in incoming calls that are put in a queue before they are picked up. The AI system's role is to identify the emergency as life-threatening and alert the human call-taker if the waiting incoming call needs to be prioritized, while the decision to perform an automated triage or prioritise dispatch remains with the human call-taker. Such an AI system is high-risk, since it evaluates and classifies emergency calls into those that are life-threatening and those that are not.

Emergency triage systems

- AI systems used in emergency departments that are intended to prioritise patients, without performing clinical assessment medical acts or diagnostic functions . Such an AI system is high-risk, since it is intended to be used to establish priority in the dispatching of emergency healthcare patient triage systems.

- AI systems intended to be used as chatbots to trigger emergency medical emergency services in medical institutions without performing clinical assessment medical acts or diagnostic functions.

Rapid alert systems

- An AI system intended to be used to support decisions on allocating resources and pre-positioning assets to combat wildfires, where the system not only predicts the likelihood and the direction of wildfire evolution across an area's protected forests, but also automatically triggers the dispatching of emergency first response services or provides clear recommendation of staff allocation in order to contain the wildfire. The system does not replace human decision-making but supports staff. Such an AI system is high-risk, since it is specifically intended to trigger emergency first response services, as well as to decide when and/or where to dispatch emergency first response services. The impact of such system is related to its decisive role for the dispatching of resources and to locations, which are decisions made in critical situations for the life and health of persons and the protection of their property.

Language tools

- AI systems intended to be used as a mental health crisis triage chatbot, which uses natural language processing to assess severity and urgency of chat-based contacts with emergency mental health services without performing clinical assessment or diagnostic functions. Such an AI system is high-risk, since it directs mental health intervention responses, carries a risk of misclassification and provides a first emergency triage function.

b) Practical examples of AI systems falling outside the high-risk use case of point 5(d)

Transcribing emergency calls

- An AI system intended to transcribe poor-quality emergency calls, or calls where callers may be panicked or unable to communicate, identifying relevant keywords and transcribing them automatically, thereby saving time that the call-taker would otherwise spend asking the caller to repeat themselves. Such an AI system falls outside the use case listed in point 5(d), since it aids the emergency first response services call-taker in the evaluation of a call made by a natural person by focusing on specific keywords related to emergency first response services, but does not evaluate or classify the call.

Forecasting

- AI systems that analyse various sets of data for fast indications of potential disasters before emergency first response services are made aware through emergency communications. These systems can for example identify flood-prone regions and suggest mitigation strategies, model potential wildfire spread patterns based on wind, temperature and vegetation density, process social media feeds to detect when a new topic is trending and monitor weather conditions and seismic activity. Such an AI system falls outside the use case listed in point 5(d), since it is not intended to decide when and/or where to dispatch emergency first response services, but rather resembles systems that are intended for the general forecasting of potential disasters, without a link to dispatching emergency first response services.

Enhanced learning and training

- An AI driven simulation platform used to provide realistic training environments. The system creates among others scenario-based training for first responders, allowing them to practice responses to floods, wildfires and cyberattacks, followed by automated debriefings and response recommendations. Such an AI system falls outside the use case listed in point 5(d), since it is intended to provide a learning environment with realistic scenarios. In practice, such systems are not used to evaluate and classify incoming real-time calls from natural persons, nor do they actually dispatch or prioritise emergency first response services. The experience and information gained within this environment is valuable for the development of an AI system which is to be used for the intended purposes listed in point 5(d) of Annex III of the AI Act, but is not considered high-risk for learning purposes.

Identification of patients

- AI systems intended to be used to securely identify patients undergoing medical procedures, using biometric parameters. Such an AI system falls outside the use case listed in point 5(d), since the system is not intended to be use for one of the intended purposes listed therein.

AI systems related to the connectivity of the service

- AI systems intended to convey traffic on the network of received emergency calls or the lack of connectivity. Such an AI system falls outside the use case listed in point 5(d), since it is not inherently responsible for triggering harmful outcomes, even if it may affect the availability of services.

Estimated healing time

- AI systems intended to estimate the healing time for room- and bed-management in a hospital. Such an AI system falls outside the use case listed in point 5(d), since it is not intended to be use for one of the intended purposes lists therein.

Medical appointments

- AI systems intended to schedule medical appointments. Such an AI system falls outside the use case listed in point 5(d), since it is not intended to be use for one of the intended purposes listed therein and it does not relate to life-threatening emergencies.

c) Practical examples of AI systems falling within the use case but exempted under the filter mechanism of Article 6(3)

Preparatory tools for prioritization

- An AI system intended to interpret weather risk data, such as of wildfire or flood, in advance of a probable emergency and to provide preparatory intelligence for the prioritisation of resources, such as pre-positioned firefighters or flood prevention devices, and their allocation pre-emptively. Such an AI system falls within the use case listed in point 5(d), since it is intended to be used for establishing priority in the dispatching of emergency services. However, since the

system performs a preparatory task to an assessment relevant for the prioritisation that will be evaluated and confirmed by human analysts and the competent commander, it falls under the exception in Article 6(3)(d) AI Act.

Supportive tools for human review

- AI systems intended to provide situational awareness of an emergency site to first responders, such as of where patients and casualties are located and what is e.g., their body temperature. This could be a system held by the on-site commander that gathers and combines the respective data from human first responders, from autonomous rescue robots or drones, and other sensor data (e.g., radioactivity or toxins). Such an AI system falls within the use case of point 5(d) of Annex III, since it is linked to emergency healthcare patient triage systems. However, since the system merely provides existing and factual information in a structured manner, without evaluating this information for the prioritisation or triage of the patients and casualties, it falls under the exceptions for AI systems intended to perform narrow procedural and preparatory tasks in Article 6(3)(a) and (d) AI Act.

3.6. Law enforcement

(337) As explained in Recital 59 AI Act, given their role and responsibility, actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty, as well as other adverse impacts on fundamental rights guaranteed in the EU Charter of Fundamental Rights. Therefore, the AI Act designates law enforcement as one of the areas in which specific applications of AI systems may entail considerable risks to the health, safety, and fundamental rights of natural and legal persons.

(338) Point 6 of Annex III AI Act lists five high-risk use cases in which AI systems intended to be used in the area of law enforcement are classified as high-risk. These use cases were considered by the Union legislature as situations in which accuracy, reliability and transparency are particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress (Recital 59). As explained in Section 2.6 above, the fact that an AI system is classified as a high-risk AI system under these use cases should not be understood to mean that the use of the system is lawful under other acts of Union law or under national law compatible with Union law.

3.6.1. Overview of use cases and horizontal issues

(339) Point 6 of Annex III AI Act covers AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices, or agencies in support of law enforcement authorities, in so far as such use is permitted under relevant Union or national law. The following use cases are classified as high-risk:

(a) AI systems intended to be used to assess the risk of a natural person becoming the victim of criminal offences;

(b) AI systems intended to be used as polygraphs and similar tools;

(c) AI systems intended to be used to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences;

(d) AI systems intended to be used to assess the risk of a natural person offending or reoffending, not solely on the basis of the profiling of natural persons, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups;

(e) AI systems intended to be used for the profiling of natural persons in the course of the detection, investigation or prosecution of criminal offences.

i. The concept of 'law enforcement authority'

(340) The term 'law enforcement authority' is decisive for determining whether an AI system falls within the scope of the high-risk use cases listed in point 6 of Annex III AI Act. The definition of 'law enforcement authority' in Article 3 (45), points (a) and (b), AI Act is identical to the definition of 'competent authority' in Article 3(7) of Directive (EU) 2016/680 (Law Enforcement Directive, hereinafter 'LED'). Pursuant to that definition, the concept of 'law enforcement authority' should be understood to comprise (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

(341) Given the diversity of legal systems across Member States, the concept of 'law enforcement authorities' in Article 3 (45) AI Act should be interpreted using a functional approach. This means that the classification of a body or entity as a law enforcement authority will depend not on the formal designation of the body or entity as such, but on whether the tasks it performs, as granted by law, are of a law enforcement nature, i.e. the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, but not of an administrative nature.

Examples[70] of law enforcement authorities within the meaning of the AI Act include the following bodies, where they carry out a law enforcement tasks (prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties[71]):

- the police,
- public prosecutors,
- probation and parole services,
- penitentiary (prison) services.

For authorities with mixed competences, point 6 of Annex III should not apply merely because the authority has certain law-enforcement powers. It applies only where the AI system is intended to be used by or on behalf of that authority in the exercise of its law-enforcement functions, and where the

[70] The definition of a 'law enforcement authority' varies across EU Member States' national laws, therefore, this list is for orientation purposes only.

[71] Further discussion as to the concept and the activities covered can be found in the Commission Guidelines on prohibited artificial intelligence practices, points 319-325.

intended use falls within one of the use cases listed in point 6 of Annex III. See further paragraph 348 below.

(342) For the purposes of the AI Act, judicial authorities acting in criminal matters, or other authorities that exercise judicial functions or constitute part of the judicial system in criminal matters, should be considered as both 'judicial authorities' within the meaning of point 8 of Annex III, as well as 'law enforcement authorities' within the meaning of point 6 of that Annex. This interpretation of the concept of 'law enforcement authorities' as including 'judicial authorities' is specific to the AI Act, in particular regarding the scope of use cases in points 6 of Annex III. This is because the definition of 'law enforcement authorities' in Article 3 (45) AI Act is identical to the definition of 'competent authorities' used in Article 3(7) LED and the concept should be interpreted in a consistent manner. The scope of the notion 'law enforcement authorities' under the AI Act is without prejudice to the interpretation of the same or similar concepts in other Union acts.

(343) Customs authorities in some of the Member States should be considered, in certain cases, as law enforcement authorities, particularly where they prevent, investigate, and detect customs-related crimes. In such instances, those authorities will operate within a law enforcement framework, so that an AI system that is intended to be used in those instances will be classified as high-risk if it falls within one of the use cases listed in point 6 of Annex III AI Act. In contrast, where customs authorities act in an administrative, rather than in a law enforcement, capacity, an AI system intended to be used by those authorities in that capacity will not be classified as high-risk because the use cases listed in point 6 of Annex III related only to law enforcement activities (see Section iii. Exclusion of AI systems used in administrative proceedings below).

(344) Law enforcement authorities should be distinguished from national intelligence authorities (sometimes called national intelligence units, security services, or secret services), although in some instances these authorities will exercise overlapping competences. In some Member States, national intelligence authorities may also provide support to law enforcement authorities in the exercise of their competences. Where a national intelligence authority performs law enforcement functions prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, an AI system intended to be used by such an authority in the exercise of those functions may be classified as high-risk pursuant to Article 6(2) AI Act if it falls with one of the use cases listed in point 6 of Annex III. Otherwise, Article 2(3), second subparagraph, AI Act expressly excludes from its scope AI systems that are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities. Recital 24 AI Act clarifies how the notion 'exclusively' used in that provision should be interpreted and in which instances an AI system used for such purposes may nevertheless fall within the scope of the AI Act if it is used also for law enforcement purposes[72].

(345) Where a provider places on the market or puts into service an AI system that is intended to be used by both law enforcement authorities and national intelligence authorities, such system should be classified as high-risk AI system (however, national intelligence authorities would not be subject to deployers obligations as they are excluded from the AI Act scope). The same applies if law enforcement authorities and national intelligence authorities jointly develop a project and create an AI system, in so far as the AI system is also intended to be used in the context of law enforcement.

[72] See further Guidelines on prohibited artificial intelligence practices, Section 2.1.5.

By contrast, if the system is intended to be used only by intelligence authorities acting exclusively outside law enforcement activities, it would not fall under the AI Act.

ii. 'Union institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf"

(346) The use cases listed in point 6 of Annex III AI Act refer not only to law enforcement authorities and entities acting on behalf of law enforcement authorities, but also to Union institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf.

(347) As a result, those use cases should be considered to cover, e.g.: Europol (the European Union Agency for Law Enforcement Cooperation), which supports law enforcement agencies across Member States in fighting serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy; Eurojust (the European Union Agency for Criminal Justice Cooperation), which brings together prosecutors and judges from across the Union and beyond in an effort to effectively tackle all forms of serious cross-border crime; and the EPPO (the European Public Prosecutors Office), which investigates, prosecutes, and brings to judgment crimes against the financial interests of the Union. The use cases listed in point 6 of Annex III AI Act may also apply to Frontex (the European Border and Coast Guard Agency) to the extent that its activities constitute law enforcement activities.

iii. Exclusion of AI systems used in administrative proceedings

(348) The use cases listed in point 6 of Annex III AI Act refer only to AI systems intended to be used in relation to law enforcement activities. AI systems specifically intended to be used for administrative activities, for example, by tax and customs authorities (e.g., those related to customs duties, tariffs, or compliance checks that are not punitive in nature), as well as by financial intelligence units carrying out administrative tasks analysing information pursuant to Union anti-money laundering law, should not be classified as high-risk pursuant to that provision (Recital 59). The same logic applies by analogy to administrative entities at EU level working in these domains.

(349) In the case of AI systems intended to be used by customs authorities, they should not be classified as high-risk pursuant to point 6 of Annex III AI Act, so long as their intended use is limited to such administrative proceedings, such as import and entry procedures, export and exit procedures, and transit procedures. However, as noted above, where an AI system is intended to be used for a purpose that falls within a high-risk use case, the system should be classified as a high-risk AI system.

An example of such a use case is a customs risk management system which outputs are used by customs officers to assess the likelihood that goods crossing a border do not comply with applicable legal requirements. Such a system will not fall under one of the use cases listed in point 6 of Annex III. In general, such systems are not designed to prevent, investigate, detect or prosecute criminal offences, but to flag possible non-compliance with Union and national rules on agricultural and food safety, plant and animal health, intellectual property rights, product safety, environmental, waste management rules, protection of cultural goods, etc. On the other hand, where AI systems are also used to detect instances that qualify as criminal offences, they should be classified as high-risk if they fall within one or more of the use cases in point 6.

(350) As explained in paragraph 218 of the Guidelines on prohibited artificial intelligence practices, for offences that are not regulated by Union law, the national qualification of the offence is subject to scrutiny by the CJEU, since 'criminal offence' is an autonomous concept of Union law and should be interpreted consistently across Member States. The CJEU has concluded, in a different context, that the classification of offences by the Member States is not conclusive in that respect[73]. Relevant criteria used to assess the nature of an offence (criminal or not) may be found in the relevant case-law of the CJEU and of the European Court of Human Rights ('ECtHR')[74]. Administrative offences are excluded from the scope of point 6 of Annex III.

iv. The concepts of risk assessment and profiling of natural persons (points 6(a), 6(d), and 6(e))

(351) Point 6 of Annex III AI Act lists three distinct use cases concerning AI systems intended to be used to assess the risk or profiling of natural persons by law enforcement authorities.

(352) These three use cases serve three types of purposes. First, point 6(a) concerns potential victim risk assessment or profiling, specifically the use of AI systems intended to be used to assess the risk that a natural person may become a victim of criminal offences, which entails a forward-looking, preventive and protective function. Second, point 6(d) concerns the risk assessment or profiling of a potential offender or group of potential offenders, specifically AI systems intended to be used to assess concrete person(s) to evaluate their (potential) criminal behaviour. Third, point 6(e) concerns more general profiling relevant in cases where profiling is applied in the context of the detection, investigation and prosecution of criminal offences, for instance to identify a list of potential suspects singling them out from the general population or from a specific group using certain criteria.

(353) Article 6(3), last paragraph, AI Act provides that AI systems falling within one of the use cases listed in Annex III should always be considered high-risk where it performs profiling of natural persons. This means that, even if the AI system fulfils the conditions for the filter mechanism in Article 6(3) AI Act, it will nevertheless be classified as high-risk if it performs profiling of natural persons.

(354) If an AI system analyses data at the group level rather than at the individual level, and thus no personal data is processed in that context, such use would not constitute profiling as defined in Article 3(4) LED (i.e. for profiling to exist, automated processing of personal data consisting of the

[73] See, for example, CJEU, judgment of 14 November 2013, Marián Baláž, Case C-60/12, EU:C:2013:733.

[74] According to the CJEU's case law, it is for national courts to determine whether a non-criminal penalty may be regarded as 'criminal' in light of the so-called 'Engel criteria', See: ECtHR, judgment of 8 June 1976, Engel and Others v. the Netherlands, Application nos. 5100/71, 5101/71, 5102/71, 5354/72 and 5370/72, CE:ECHR:1976:0608JUD000510071, paragraph 82. Originally developed by the European Court of Human Rights (ECtHR) and subsequently endorsed by the CJEU, these criteria are alternative and not cumulative. When examining whether a penalty has a criminal nature, the competent national court should assess: (1) the classification of the relevant provisions under domestic law; (2) the very nature of the offence; and (3) the severity of the penalty. In evaluating the nature of the offence, aspects taken into account include inter alia whether the proceedings are instituted by a public body with statutory powers of enforcement; whether the legal rule has a punitive or deterrent purpose; whether the legal rule seeks to protect the general interests of society usually protected by criminal law; whether the imposition of any penalty is dependent upon a finding of guilt. Regarding the severity of the penalty, relevant reference is the maximum potential penalty provided in the national law. These criteria are alternative and not necessarily cumulative. See European Court of Human Rights, Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (criminal limb), updated 29 February 2024. See also CJEU, judgment of 5 June 2012, Bonda, Case C-489/10, EU:C:2012:319, paragraphs 37ff.; CJEU, judgment of 26 February 2013, Åkerberg Fransson, Case C-617/10, EU:C:2013:105, paragraph 35.

use of personal data to evaluate certain personal aspects relating to a natural person is required)[75]. In contrast, applying the profile to individual persons would amount to profiling, since it would directly affect them and influence their personal situation.

(355) It is important to note that the use cases listed in points 6(a), 6(d), and 6(e) of Annex III AI Act do not cover the analysis or mapping of locations or geographic areas. Consequently, an AI system designed to predict risk areas during mass events (e.g. sport events, concerts) would not be classified as high-risk if it does not profile individuals, but relies solely on geographical and non-personal data, or density of people in a certain area. However, if the AI system possesses emotion recognition capabilities to identify, e.g., anger and aggressiveness, the system would fall under the use case of point 1(c) of Annex III AI Act.

For example, a police authority deploys an AI system to assess the threat level for terrorism (e.g. 'low," 'moderate," 'substantial") in a district housing government buildings based on threat indicators from intelligence reports, number of recent incidents, and political developments. In such a case, no profiling is performed on natural persons, since the assessment is not tied to evaluating the personal characteristics of any identified natural person, and the output of the system (i.e., the estimated threat level) applies collectively to all persons present in the district. Such a threat level assessment is also not applied to single out individuals considered as potential suspects or victims. The AI system would therefore not be classified as high-risk pursuant to point 6 of Annex III AI Act.

3.6.2. Point 6(a): Assessing the risk of a natural person becoming the victim of a criminal offence

(356) To fall within the use case listed in point 6(a) of Annex III, the AI system must fulfil the following cumulative conditions:

(i) The system must be intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf;
(ii) The system must be intended to be used to assess the risk related to a natural person as a victim (i.e. not an object, geographic location, event, or organisation); and
(iii) The person must be a potential future victim of criminal offences (not other risks such as accidents or administrative breaches).

(357) AI systems intended to be used to assess the risk of a natural person becoming the victim of criminal offences are typically designed to support preventive and protective law enforcement strategies. Such AI systems analyse various personal and contextual data related to individuals in order to assess their risk or vulnerability to certain criminal situations. They process information, such as personal histories, official reports, social or family circumstances, to produce evaluations of the likelihood that an individual may become a victim of a specific crime.

(358) The AI Act does not define the term 'victim'[76]. For the purposes of point 6(a) Annex III AI Act, this term can be understood to refer to a natural person who is inferred or identified by an AI system

[75] See more details on profiling in Section 2.7.2.
[76] Article 2(1)(a) of Directive 2012/29/EU (the Victims' Rights Directive; Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA. OJ L 315, 14.11.2012,

as being exposed to a probability or risk of suffering harm, including physical, mental or emotional harm or economic loss, resulting from conduct that, if materialised, constitutes a criminal offence.

(359) The classification of such AI systems as high-risk is based on the potential impact those systems can have on safety, security or fundamental rights. Such AI systems can be both useful in protecting the fundamental rights of potential victims (e.g. to protect a person from bodily harm) while improper functioning or use could trigger increased surveillance, welfare checks, damage to reputation, cause negative psychological consequences or stigmatisation. The proper functioning of such systems is therefore of material importance, since flaws or misuse can lead to a risk of underassessment and false negatives that, combined with overreliance by law enforcement authorities, may result in withholding of preventive measures or protection (e.g. in case of assessing the protection needed by an alleged victim of gender-based violence).

a) Practical examples of AI systems falling within the use case of point 6(a)

Domestic violence risk assessment systems

- Domestic violence risk assessment systems intended to be used to analyse victim statements, police reports, previous incidents, restraining order data, social services records and other data to determine the level of risk faced by a (potential) victim of domestic violence should be considered to fall in the use case listed in point 6(a) of Annex III. Such AI systems are a classic example of a tool that is used by law enforcement authorities to assess the risk of a natural person becoming the victim of a criminal offence. They influence critical interventions, including police protection measures and legal actions, which can either prevent harm from arising or, if flawed, leave victims vulnerable to further abuse. The use of such AI systems involves profiling, so that they cannot benefit from the filtering mechanism laid down in Article 6(3) AI Act.

- An AI-based risk assessment system intended to be used by judicial authorities in criminal court proceedings to estimate the probability of severe or repeated domestic intimate partner violence, for instance when issuing or maintaining restraining orders. As such risk assessment involves profiling, the exemption under Article 6(3) AI Act cannot be applied.

Vulnerability exploitation risk assessment systems

- Human trafficking vulnerability detection systems intended to be used to assess a risk of an individual being trafficked, especially in cross-border, labour exploitation or migration contexts, or in the case of young individuals from particularly vulnerable backgrounds, should be considered to fall in the use case listed in point 6(a) of Annex III. Such systems aggregate indicators such as age, lack of valid documentation, traveling with an unrelated adult, signs of control by others, and links to high-risk sectors, to produce a score indicating the likelihood of future human trafficking. Those systems involve individual risk assessment and have potential consequences for fundamental rights. The use of such AI systems involves

pp. 57–73) provides a definition of the term 'victim'. It should, however, be noted that the definition in the Victims' Rights Directive is retrospective, in that it refers to a person who has already suffered harm, whereas the use case in point 6(a) of Annex III to the AI Act is forward-looking. Similarly, or the definition of 'victim" for the purposes of gender based violence can be found in Directive (EU) 2024/1385 on combating violence against women and domestic violence. OJ L, 2024/1385, 24.5.2024.

profiling, so that they cannot benefit from the filtering mechanism laid down in Article 6(3) AI Act.

b) Practical examples of AI systems falling outside the use case of point 6(a)

AI systems predicting location-focused risks

- AI systems intended to be used to analyse the risk that a specific environment/location will see offending and victimisation (i.e., people in certain areas will become victims of crime) should be considered to fall outside the use case listed in point 6(a) of Annex III. Being environment/location-focused, such a system does not explicitly assess risks to specific persons (victims) except by virtue of them being in a risky area. However, if the system is intended to be used to predict the potential risk of a specific person or persons committing a crime in that area, such a system would fall within the use case listed in point 6(d) of Annex III.

- Situational awareness and risk assessment AI systems intended to be used to support law enforcement during the initial stages of responding to a reported crime scene should be considered to fall outside the use case listed in point 6(a) of Annex III. Such a system can be deployed via a robot or drone, and is designed to process visual and contextual inputs to detect critical elements, such as presence of armed individuals, weapons or environmental hazards. Since the aim of the system is to evaluate the immediate environment, rather than assessing the risks related to specific individuals based on personal or contextual data, it should not be classified as high-risk on that basis alone. However, if the system also had biometric capabilities, it could fall within the use case listed in point 1 of Annex III (see Section 3.1. above).

AI systems predicting risks of accidents or administrative breaches

- AI systems intended to be used to identify road segments or times where accidents are likely to occur, thus where people are at risk of becoming victims of road traffic accidents, should be considered to fall outside the use case listed in point 6(a) of Annex III. For such a system to fall within that use case, it should be intended to be used to analyse the risk of becoming the victim of criminal offences and not of accidents. Moreover, such systems are location-focused and do not analyse risks linked to concrete persons.

- AI-based video analytics intended to be used to predict overcrowding, stampedes, or structural hazards at large gatherings should be considered to fall outside the use case listed in point 6(a) of Annex III.

- AI flood-risk and wildfire-spread models intended to be used to identify populations at risk of becoming victims of accidents/catastrophes should be considered to fall outside the use case listed in point 6(a) of Annex III. See also Section 3.6.5. on the use case listed in point 5(d) of Annex III.

3.6.3. Point 6(b): Polygraphs and or similar tools

(360) Point 6(b) of Annex III classifies as high-risk AI systems intended to be used as polygraphs, also known as lie detectors, or similar tools. Such systems are intended to be used to assess whether a person is telling the truth by measuring physiological responses, such as heart rate, blood pressure, respiration, and skin conductivity.

(361) Systems similar to polygraphs include voice stress analysis that examine vocal patterns for signs of deception; eye-tracking and pupillometry that monitor eye movements and pupil dilation linked to cognitive stress; brain-imaging techniques that detect brain activity associated with lying; and behavioural analysis tools that use AI to interpret micro-expressions, body language, or speech cues.

(362) Such systems pursue a different purpose from the emotion recognition systems falling within the use case listed point 1(c) of Annex III Polygraphs are designed to infer deception and in law enforcement context are mostly used during questioning, whereas emotion recognition systems analyse biometric cues to infer emotional states (e.g. sadness or anger), typically without direct physical contact, making them relevant for such tasks as risk prediction or prioritisation of video material (see Section 3.1.4. above and Section 7 in the Guidelines on prohibited artificial intelligence practices). AI systems intended to be used as polygraphs or similar tools may include emotion recognition functionalities, since fear may serve as a proxy for lie detection. In such a case, the AI system may be considered to fall within the scope of the use case listed in point 1 of Annex III.

a) Practical examples for AI systems falling within the scope of point 6(b)

- AI systems intended to be used to analyse facial micro-expressions to assess the credibility of answers during an interrogation. Likewise, AI systems measuring eye-tracking and pupillary responses while a suspect answers questions. The role of such systems in decision-making and profiling excludes them from benefitting from the exceptions listed in Article 6(3) AI Act.

b) Practical examples for AI systems falling outside of the use case point 6(b)

- AI systems intended to be used to monitor police officers' fatigue or stress levels (via wearable sensors or facial analysis) for occupational health and safety reasons. Such systems should also be considered to fall outside the use case listed in point 1(c) of Annex III, as further clarified in Recital 18 AI Act (see Section 3.1.4); being intended to be used for medical and safety reasons, they are also excluded from the prohibited practice listed in Article 5(1)(f) AI Act.

- AI systems intended to be used by law enforcement authorities that transcribe interviews and flag changes in tone (e.g. higher tone, slower/faster speaking pace), without drawing conclusions about the truthfulness of statements made. It should, however be checked whether a particular use case would not amount to emotion recognition system and thus fall under point 1 of the Annex III of the AI Act.

– AI systems that flag irregularities in how different polygraph examiners interpret similar cases, highlighting inconsistencies for law enforcement authorities. Such system is not a polygraph itself, but is intended to be used to interpret the work of polygraph examiners.

3.6.4. Point 6(c): AI systems intended to be used to evaluate the reliability of evidence

(363) Point 6(c) of Annex III classifies as high risk AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities, to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences. The provision refers to 'evaluation of reliability of evidence' and as such focuses only on this specific task and only in the course of an open criminal investigation or prosecution.

(364) In the context of law enforcement activities, evaluating the reliability of evidence means assessing how trustworthy, accurate, and credible the evidence is in the case it is used in investigations, arrests, or prosecutions. This encompasses, in particular, the court-proof verification of the authenticity of evidence prior to conducting in-depth investigations or making arrests or other prosecussion action. The core function of AI systems covered by this use case is the evaluation of evidentiary reliability. This may include, for instance:

– authenticity verification;

– data integrity checks;

– source reliability assessment;

– evaluation whether the evidence aligns with other available information or is internally consistent.

(365) This does not include AI systems that are intended to be used for working with the information collected, but that are not intended to be used for the evaluation of reliability of evidence. Examples of such tasks that are not falling under the scope of 'evaluation of reliability of evidence' (and thus are outside of point 6 AI Act), include collecting, arranging and structuring of information, data extraction and linking, document clustering, timeline reconstruction, visualisation, indexing of documents, duplicate detection, search in its various forms (including, for example, keyword-based queries, similarity/fuzzy, knowledge-graph search, and multimodal and semantic retrieval across text, audio, image or video, translation and transcription, as well as data structuring and standardisation.

a) Practical examples of AI systems falling within the use case of point 6(c)

Authenticity verification

– AI-enabled digital forensics solutions for image, audio and video analysis intended to be used by law enforcement authorities to detect whether digital images, audio recordings or videos have been altered or manipulated (e.g. to confirm the authenticity of CCTV footage or

smartphone recordings that were presented as evidence; to verify if collected pictures are not deepfakes).

Data integrity checks and source reliability assessment

- AI systems intended to be used by law enforcement authorities to determine and evaluate alterations of documents , or forged signatures.

- AI systems intended to be used for evaluating the authenticity of digital evidence retrieved from mobile or other devices, including by analysing digital traces (e.g. metadata such as geolocation records, file creation and modification histories) and by flagging elements requiring closer human examination.

- AI systems intended to be used to assist competent law enforcement authorities in assessing the reliability of evidence, including from human sources, such as the credibility of informants or witnesses, by analysing factors such as the internal consistency of statements, their coherence with verified facts, and the accuracy of information provided by the same source in past cases.

b) Practical examples of AI systems falling outside the use case of point 6(c)

Image enhancement and data recovery

- AI systems intended to be used for forensic reconstruction, image enhancement, or data recovery from devices. Such systems do not evaluate the reliability of evidence, but assist human experts by processing, restoring, or extracting data that can then be examined and relied upon.

AI systems reconstructing crime scenes

- AI systems intended to be used to map or reconstruct crime scenes or to provide visualisations or models based on data collected (photos, measurements, etc.). Such systems help investigators better understand the spatial relationships and sequence of events at a crime scene without assessing evidence reliability.

Pattern detection

- AI systems intended to be used to detect patterns in investigations and notify law enforcement authorities thereof (e.g. identifying similar break-in methods in recent thefts or notify of similar victim profile in recent homicides). Such systems do not evaluate the reliability of evidence, but find correlations or patterns that might otherwise go unnoticed and help law enforcement focus their investigations or spot potential links between cases.

Content flagging and searches

- AI systems intended to be used to detect child sexual abuse material online, without evaluating the reliability of it as evidence. The primary function of such a system is to identify, flag and filter content that potentially violates the law.

- AI-enabled solutions intended to be used by law enforcement authorities for screening child sexual abuse material online and the classifying thereof in the following groups for prioritisation: (i) new material; (ii) material already registered in the database; and (iii) deepfake pictures. Such systems do not evaluate the reliability of evidence, but are designed to support investigative workflows by filtering or preselecting large volumes of incoming material. The application of Article 6(3) of the AI Act in this use-case is without prejudice to the potential qualification of the AI system at issue as high-risk system under other use cases listed in Annex III of the AI Act (e.g. point 6(a) of Annex III).

- AI systems intended to be used by law enforcement authorities to analyse online advertisements in the sex industry and to flag those most likely to be linked to human trafficking. Such systems do not evaluate the reliability of evidence, but are designed to identify, flag and filter content that potentially violates the law.

- AI systems intended to be used to match the ballistic markings on a bullet to markings registered in a reference database for the purposes of identifying whether a particular weapon was used for committing a crime. Such systems do not evaluate the reliability of evidence,

but constitute a means of file handling or of searching a database by evaluating the similarities between evidence material and a reference database.

c) Practical examples of AI systems falling within the use case but exempted by the filter mechanism in Article 6(3) AI Act

- AI systems that are used in the course of evaluation of evidence but only classify documents, pictures, videos or other material selected to be analysed for authenticity into categories and thus structure the evaluation of evidence where that categorisation does not impact the assessment of the reliability of those documents as evidence. Such systems fall under the exception for AI systems intended to perform narrow procedural tasks in Article 6(3)(a) AI Act.

- An AI system that is used in the course of evaluation of evidence and is indexing and tagging financial documents collected to be evaluated for reliability of evidence (e.g. to be checked with bank account flows; or to be checked for existence of names or objects). Such system fall under the exceptions for AI systems intended to perform narrow procedural or preparatory tasks in Article 6(3)(a) and (d) AI Act.

3.6.5. Point 6(d): AI systems assessing offending or reoffending of concrete person(s)

(366) Point 6(d) classifies as high-risk AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities, to assess the risk of (a) concrete person(s) offending or reoffending, provided that assessment is not based solely on profiling or evaluating their personality traits, or by looking at their past criminal behaviour or the past criminal behaviour of the groups to which that person belongs. In other words, the use case in point 6(d) includes AI systems intended to be used to assess the risk of a person committing a crime or reoffending, without prejudice to the prohibition set out in Article 5(1)(d) AI Act. Each of the conditions of the use case listed in point 6(d) of the Annex III AI Act shall be examined in the subsections below.

ii. The concept of 'not solely on the basis of" (i) profiling, (ii) assessment of personality traits and characteristics, and (iii) assessment of the past criminal behaviour of natural persons or groups as alternatives

(367) The use case listed in point 6(d) of Annex III captures predictive and behavioural AI systems that are intended to be used to assess the risk of a natural person offending or re-offending. It explicitly excludes AI systems that are based solely (i) on profiling as per Article 3(4)LED, (ii) on the assessment of personality traits and characteristics, which are already prohibited under Article 5(1)(d) AI Act (see Section 5 of the Guidelines on prohibited artificial intelligence practices)[77]or (iii) on the assessment of past criminal behaviour of natural persons or groups. Recital 59 AI Act clarifies that the use cases listed in point 6(d) of Annex III are to be interpreted as alternative. If at

[77] Article 5(1)(d) AI Act prohibits AI systems assessing or predicting the risk of a natural person committing a criminal offence based solely on profiling or assessing personality traits and characteristics.

least one of these use cases is present, the AI system qualifies as high-risk, unless it falls under the prohibition set out in Article 5(1)(d) AI Act.

(368) The use of an AI system to assess the risk of a natural person offending or re-offending is not based solely on profiling where that system is 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. As recital 42 AI Act clarifies, this will be the case where a reasonable suspicion already exists in respect of the natural person concerned. Paragraphs 199 to 206 of the Guidelines on prohibited artificial intelligence practices contain further guidance on the notion of 'solely" in relation to profiling under Article 5(1)(d).

a) Practical examples of AI systems falling within the use case of point 6(d)

AI systems used when processing detained persons to assess the risk of offending/reoffending

- An AI system intended to be used during the initial processing of detained youth suspects by police to calculate a risk score that indicates the likelihood of reoffending, which is then used to make a decision on measures to be taken. The AI system does not autonomously make decisions; the outcome is considered alongside other information, and final decisions are made by the competent authorities. The AI system is intended to be used in support of law enforcement authorities for assessing the risk of a natural person re-offending and this assessment is done not solely on the basis of the profiling of natural persons as referred to in Article 3(4) LED, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups, as there are verifiable facts directly linked to a criminal activity (the assessment is performed post-detention).

AI systems used by probation officers

- An AI system intended to be used by probation officers to support assessments informing decisions on parole or conditional release, by evaluating factors such as criminal record, behaviour and progress during the custodial sentence, and other case-relevant supervision-related information. Like the example above, there are verifiable facts directly linking a person to a criminal activity (the person having already been convicted of a criminal offence).

AI systems used by penitentiary institutions

- An AI system used by a penitentiary institution to predict the likelihood of an offender re-offending based on prior criminal record, violence within the prison facilities, or socio-economic data. Like the examples above, there are verifiable facts directly linking a person to criminal activity (the person having either already been convicted of a criminal offence or being detained on suspicion of having committed such an offence).

AI systems used by criminal courts to assess the risk of offending/reoffending

- An AI-based risk assessment system intended to be used in criminal courts to estimate the likelihood of recidivism, violent reoffending, or the commission of further serious offences. Since such a risk assessment system involves profiling, the exceptions of Article 6(3) AI Act do not apply.

b) Practical examples of AI systems falling outside the use case of point 6(d)

Location focused AI-systems

- AI systems predicting locations and timeframes of likely crimes (e.g., burglary risk in a neighbourhood), without linking the prediction to identifiable individuals. The use case in point 6(d) concerns risk assessments of natural persons, not geospatial predictions.

c) Practical examples of AI systems falling within the use case but exempted by the filter mechanism in Article 6(3) AI Act

- An AI system that checks whether all required fields are completed in a probation officer's risk assessment form or flags inconsistencies in entered data (e.g., mismatched dates of offence or custody period). Such an AI system performs a preparatory task for the risk assessment and does not evaluate personal characteristics . It is also intended for a narrow procedural task (Article 6(3)(a) AI Act), since it only flags inconsistencies and would in any event fall under the exception for AI systems intended to perform a preparatory task listed in Article 6(3)(d) AI Act.

- An AI system that collects and pre-sorts prior convictions, probation reports, and other records to prepare a case file for human officers. Such a system performs a preparatory task for risk assessment and therefore qualifies for an exemption under Article 6(3)(d) AI Act.

3.6.6. Point 6(e): AI systems intended to be used for the profiling of natural persons in the course of the detection, investigation or prosecution of criminal offences

(369) Point 6(e) of Annex III classifies as high-risk AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities, for the profiling of natural persons as referred to in Article 3(4) LED in the course of the detection, investigation or prosecution of criminal offences. The inclusion of this use case in point 6 of Annex III affirms that profiling itself, when carried out through an AI system inter alia by law enforcement authorities in the criminal justice context, warrants a high-risk regulatory response, due to its potential to undermine the rights of due process, data protection, and equal treatment.

(370) This provision applies to AI systems intended to be used by law enforcement authorities in identifying potential suspects or other persons of interest (e.g. victims) in various criminal contexts in the course of profiling of a natural person. Such systems typically analyse diverse types of data, such as geographic information, registry data, witness descriptions, or online activity, to generate profiles or flags that assist in crime detection, investigation or prosecution.

a) Practical examples of AI systems falling within the use case of point 6(e)

AI systems intended to be used in assisting the identification of potential suspects

- AI systems assisting in identifying potential suspects where a child is reported missing that analyse the neighbourhood, persons living in the neighbourhood that are on the sex offenders' registry and their movements, as well as types of children they have abused earlier. The purpose of the AI system is to generate individualised risk inferences from behavioural patterns, thereby filtering persons as potential suspects. Such a system would involve profiling, since it performs the automated processing of personal data to evaluate and predict aspects of natural persons' behaviour. Where the assessment of potential involvement in criminal activities is supported bypast criminal behaviour and other verifiable facts, the system would not be solely based on profiling and assessing personal characteristics. It therefore falls within the use case of point 6(e) of Annex III AI Act, rather than the prohibition on predictive policing laid down in Article 5(1)(d) AI Act.

- AI systems assisting in identifying potential suspects based on descriptions of witnesses and other personal data. Such an AI system processes personal data to infer identity-linked traits and other personal aspects based on patterns, and to single out individuals as potential suspects.

AI systems intended to be used for targeted online monitoring

- An AI system that monitors online posts to classify users based on sentiment analysis, posting patterns, and networks, and assigning flags for potential extremist affiliation. The system automatically analyses communication patterns, language use, and behavioural indicators to classify persons as potential radicalised subjects. The system performs profiling, since it evaluates and predicts natural persons' characteristics and likely future behaviour for law enforcement purposes. This does not amount to social scoring as prohibited by Article 5(1)(c) AI Act, since the system is limited to targeted radicalisation monitoring within specific spheres or contexts.

b) Practical examples of AI systems falling outside the use case of point 6(e)

- AI systems analysing neighbourhoods and assigning criminality scores (predictive crime mapping systems) where they do not include profiling of individuals as per points 6(d) and (e) of Annex III.

- AI systems detecting suspicious transaction patterns that indicate money laundering or terrorist financing, even though that allows linking such transaction to personal profiles. However, borderline cases may arise where, in addition to focusing on transactions only (the structural, quantitative, or behavioural transactions data, e.g., transaction amounts, frequencies, intervals, geographic routing), such systems are combined with, or enriched by, personal data, thereby enabling the construction of individual profiles (e.g., names, account numbers).If the system assesses such personal characteristics, it should be classified as high-risk.

- An AI-enabled crime-linkage system analysing police crime reports and case files containing variables, such as time, place, modus operandi, suspect/victim descriptions, physical traits, clothing, vehicles, and socio-demographic indicators, with the purpose to identify patterns and similarities across different incidents, linking them into possible 'series' committed by the same offender(s). Its main outputs are alerts, crime link hypotheses, and forecasts of likely future offences (not linked to a particular individual).

3.6.7. Other AI systems falling outside the use cases of point 6 of Annex III

(371) The use cases listed in point 6 (and point 1) of Annex III, which are particularly relevant for law enforcement, do not encompass all AI systems used for law enforcement purposes. These use cases primarily address situations where AI systems are applied directly to natural persons or have the capacity to materially influence decision-making. Consequently, many AI applications employed by law enforcement that do not meet these criteria may fall outside the use cases covered by point 6 (and point 1).

(372) Below are some examples of AI systems used by law enforcement authorities that would not generally be classified as high-risk pursuant to Article 6(2) AI Act and point 6 of Annex III[78]. This list is provided for orientation purposes only and is not exhaustive, since there are many other AI systems used in law enforcement beyond those mentioned below.

- AI systems used for automating administrative tasks (e.g., administration and accounting, case management, equipment management, AI systems scheduling patrol shifts). Such AI systems are intended for purely ancillary administrative activities and therefore do not fall within the use cases listed in point 6 of Annex III.

- Chatbots on police websites providing general information, guiding users through the website. Such AI systems are intended for purely ancillary administrative activities and therefore do not fall within the use cases listed in.

- Automated number plate readers seeking to identify concrete vehicles. Such AI systems are not considered as biometrics within the meaning of point 1 and do not involve profiling withing the meaning of point 6 of Annex III, since the technology itself is vehicle-focused, not person-focused. However, how the data is used, stored, and interpreted can, at a later stage, create risks of surveillance overreach or privacy violations (e.g. if enabling the reconstruction of individuals' travel patterns).

- AI systems checking whether road safety rules are broken (e.g. speeding cars, running red lights, motorbike riders failing to wear a helmet, smartphone use while driving). Such AI systems do not fall within the use cases listed in in point 6 of Annex III, nor do they constitute biometrics within the meaning of point 1 of Annex III.

[78] As stated in Recital 52, for high-risk AI systems other than those that are safety components of products, or that are themselves products, it is appropriate to classify them as high-risk if, in light of 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 this Regulation.

- AI systems intended for the detection of objects (e.g. weapons, suspicious parcels, dangerous objects, stolen goods including cultural objects and fine art). Such AI systems do not fall within the use cases listed in point 6 of Annex III, nor do they constitute biometrics within the meaning of point 1 of Annex III.

- AI systems intended for the detection of unusual behaviour or movements, such as running, raised arms, a fighting stance, a physical position that could indicate someone is holding a weapon, etc., real-time or in video feeds (not identifying a person, but whether a process or behaviour is potentially unlawful).

- AI systems detecting gunshot sounds in real time. Such AI systems do not fall within the use cases listed in in point 6 of Annex III, since they function based on the detection of sounds and not people.

- AI systems used by custom authorities to assess consignments (goods crossing the border). Custom authorities checking consignments normally do not classify as law enforcement authorities within the context of point 6 of Annex III. In addition, those systems evaluate the compliance of goods with EU legislation based on verifiable data (e.g. container number, description of goods, routing, transport, payment method), not personal characteristics or behaviour or persons. In certain cases, such AI systems may also process information about the prior involvement of the importer or exporter in irregularities related to the import of goods, their affiliation to criminal organisations, or a criminal record for drug trafficking. Such systems, as noted in the Guidelines on prohibited artificial intelligence practices (para. 214), fall outside the scope of the prohibition in Article 5(1)(d)AI Act because any prediction of the likelihood of a natural person being involved in the import or export of illicit goods is not solely based on profiling, but on objective and verifiable information related to the goods and the importer or exporter's prior involvement in criminal activity and subject to a human review to determine whether the situation requires a customs control or risk mitigation action.

- AI systems used by customs and/or law enforcement authorities to analyse data related to the movement of goods and transport operations, such as shipping routes, frequency and patterns of consignments, anomalies in declared cargo, transport modalities, etc., to detect misuse of commercial transport systems to transport trafficked goods. Such AI systems do not fall within the use cases listed in point 6 of Annex III, since they do not seek to predict the likelihood of a natural person committing an offence or to profile a natural person. Rather, they review objective and verifiable data relating to the commercial transportation of goods to determine an anomaly that may require further investigation.

3.7. Migration, asylum and border control management

(373) Point 7 of Annex III AI Act lists four high-risk use cases of AI systems intended to be used in the field of migration, asylum, and border control management. As explained in Recital 60 AI Act, AI systems used in these fields affect people who may be in a particularly vulnerable position and whose treatment can determine access to a territory, international protection, residence, detention or return. Such uses therefore carry significant implications for the entry and stay of individuals in the territory of the EU and their safety and fundamental rights. Any deployment of an AI system in this field must also comply with the applicable EU rules and procedures on asylum, visas, and border-management and fully respect the GDPR/EUDPR and the Charter, including the principle

of non-refoulement and the right to international protection, as well as the Member States' obligations under the 1951 Refugee Convention and its 1967 Protocol. In the AI Act, the EU legislature has emphasised that accuracy, non-discrimination, and transparency are particularly important to safeguard fundamental rights, maintain public trust, and ensure effective remedies. As explained in Section 2.6 above, the fact that an AI system is classified as a high-risk AI system under these use cases should not be understood to mean that the use of the system is lawful under other acts of Union law or under national law compatible with Union law.

3.7.1. Overview of use cases and horizontal issues

(374) Point 7 of Annex III lists four high-risk AI systems intended to be used by or on behalf of competent public authorities, or Union institutions, bodies, offices or agencies, in the field of migration, asylum, and border-control management, in so far as such use is permitted under relevant Union or national law. In particular, that provision classifies the following use cases as high-risk:

(a) Polygraphs or similar tools;

(b) AI systems intended to assess a risk posed by a natural person who intends to enter or who has entered into the territory of a Member State (e.g., security, irregular-migration, or health risk);

(c) AI systems intended to assist a competent public authority in examining an asylum, visa, or residence application and associated complaints with regard to the eligibility of the natural persons applying for a status (including a related assessment of the reliability of evidence); and

(d) AI systems intended to detect, recognise, or identify natural persons in the migration, asylum or border-management context (with the exception of the verification of travel documents).

i. The concept of 'competent authorities" and 'on be

(375) The AI system use cases listed in point 7 of Annex III concern those systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies in the migration, asylum and border-management fields. This covers the national authorities designated pursuant to the EU or national law governing the field, as well as Union institutions, bodies, offices or agencies acting within their mandates under that law.

(376) Without prejudice to the assessment on the compatibility of the use of an AI system with the Charter and EU secondary law in this context, these authorities may potentially include the following non-exhaustive examples:

- Border-control authorities under Regulation (EU) 2016/399 ('the Schengen Borders Code')[79] and Regulation (EU) 2019/1896 ('the European Border and Coast Guard framework')[80]. These authorities perform checks at external borders and related tasks. The 'European Border

[79] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification) *OJ L 77, 23.3.2016, pp. 1–52*.

[80] Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard *OJ L 295, 14.11.2019, pp. 1–131.*

and Coast Guard" is composed of the national authorities responsible for border management and Frontex;

- Consular authorities and central visa authorities responsible for examining visa applications and taking visa decisions under Regulation (EC) No 810/2009[81] ('the Visa Code') and Regulation (EU) 2021/1134[82]('the VIS framework');

- Asylum authorities competent under Directive 2013/32/EU[83], and, as of 12 June 2026, Regulation (EU) 2024/1348 ('the Asylum Procedures Regulation')[84] which will replace the Directive; in particular 'determining authorities" responsible for first-instance examination of applications for international protection;

- Immigration/return/detention authorities acting under the Return Directive 2008/115/EC[85] including authorities issuing and enforcing return decisions and operating return/detention procedures;

- Competent authorities and other appeal or review bodies (including administrative appeal bodies and judicial authorities), where they examine appeals or associated complaints relating to asylum, visa or residence decisions under the applicable Union and national legal framework;

- Union bodies, offices and agencies acting within their mandate in the aforementioned fields, notably Frontex when acting under Regulation (EU) 2019/1896 ('the EBCG Regulation')[86], the European Agency for Asylum when acting under Regulation (EU) 2021/2303[87], and eu-LISA set up under Regulation (EU) 2018/1726 for the management/operation of large-scale IT systems (VIS, SIS, Eurodac) established under Regulation (EU) No 603/2013[88], as a Union system supporting asylum and migration management through biometric data processing, and as of 12 June 2026 under Regulation (EU) 2024/1358[89], which will replace Regulation (EU) No 603/2013.

---

[81] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) *OJ L 243, 15.9.2009, pp. 1–58.*

[82] Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 for the purpose of reforming the Visa Information System *OJ L 248, 13.7.2021, pp. 11–87.*

[83] Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (recast) *OJ L 180, 29.6.2013, pp. 60–95.*

[84] Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 establishing a common procedure for international protection in the Union *OJ L, 2024/1348, 22.5.2024.*

[85] Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals *OJ L 348, 24.12.2008, pp. 98–107.*

[86] Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard *OJ L 295, 14.11.2019, pp. 1–131.*

[87] Regulation (EU) 2021/2303 of the European Parliament and of the Council of 15 December 2021 on the European Union Agency for Asylum *OJ L 468, 30.12.2021, pp. 1–54.*

[88] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints (recast) *OJ L 180, 29.6.2013, pp. 1–30.*

[89] Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of 'Eurodac' for the comparison of biometric data *OJ L, 2024/1358, 22.5.2024.*

(377) Depending on the field, the following instruments may be relevant to determine the competent authority, including the competent EU institution, body or agency: Regulation 2024/1356[90] ('the Screening Regulation') as regards pre-entry screening and referral; the Asylum Procedures Regulation[91] as regards asylum procedures; Regulation 2024/1349[92] ('the Return Border Procedure') as regards return border procedures; and Regulation 2024/1351[93] ('the Asylum and Migration Management Regulation').

ii. Interplay with other Union rules

(378) The high-risk rules of the AI Act apply to AI systems classified as high-risk pursuant to point 7 of Annex III in addition to the rules on EU asylum, visa and border-management procedures. The intended use of an AI system must comply with those rules, and must therefore respect the applicable guarantees, including the principle of non-refoulement and effective access to the asylum procedure, as well as the Member States' obligations under the 1951 Refugee Convention and its 1967 Protocol Where an AI system, if deployed as a component and authorised within the infrastructure of systems such as the Visa Information System (VIS), the Schengen Information System (SIS), the European Dactyloscopy database (Eurodac), the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN), the Central Repository for Reporting and Statistics (CRRS) or EU Interoperability components, is designed to use data from those systems it must respect those instruments' purpose limits, access conditions and fundamental rights' safeguards.

iii. Interplay with biometric high-risk systems

(379) Where the functionality of an AI system falling within one of the use cases listed in point 7 of Annex III involves the processing of biometric data or techniques (e.g. face, fingerprints, gait), the system will also be classified as high-risk pursuant to point 1 of Annex III (Biometrics), if it falls in one of the use cases listed in point 1 (a),(b) or (c) and the considerations set out in section 2.3.1 apply. As a consequence, the system will be subject to a third-party conformity assessment, since it is classified as high-risk pursuant to point 1 of Annex III.

(380) AI systems intended to be used to verify travel or identity documents, including checking for morphing, unusual inks, copied signatures, or chip or Public Key Infrastructure (PKI) validity, fall outside the scope of the use case listed in point 7(d) of Annex III. By contrast, AI systems intended to be used to perform presentation-attack checks, including on-person liveness checks, used within person detection and recognition flows are not document-verification features and will generally be classified as high-risk under the use case listed in point 7(d) of Annex III, unless the system is used for RBI, in which case it will be classified as high-risk pursuant to point 1(a) of Annex III. In seamless border procedures, where travellers actively present themselves for one-to-one verification against their travel document, presentation-attack detection used solely as an anti-

[90] Regulation (EU) 2024/1356 of the European Parliament and of the Council of 14 May 2024 introducing the screening of third-country nationals at the external borders *OJ L, 2024/1356, 22.5.2024.*

[91] Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 establishing a common procedure for international protection in the Union *OJ L, 2024/1348, 22.5.2024.*

[92] Regulation (EU) 2024/1349 of the European Parliament and of the Council of 14 May 2024 establishing a return border procedure *OJ L, 2024/1349, 22.5.2024*.

[93] Regulation (EU) 2024/1351 of the European Parliament and of the Council of 14 May 2024 on asylum and migration management *OJ L, 2024/1351, 22.5.2024*.

spoofing safeguard remains part of that verification function and does not, on its own, classify the system as high-risk pursuant to point 7 of Annex III. Where the same functionality is used to support operational person detection, tracking or identification beyond verification, the system will be classified as high-risk pursuant to point 7 of Annex III, unless the conditions for classification pursuant to point 1 of Annex III are met, in which case that classification will apply.

(381) Classification as high-risk follows the intended use of the systems. AI systems intended to be used exclusively for search-and-rescue (lifesaving) do not fall within the border control use case and therefore will not be classified as high-risk pursuant to point 7 of Annex III. The same system intended to be used for migration or border control may be classified as high-risk pursuant to point 7 of Annex III, provided the system meets the other conditions of that point. Many AI systems can be used for both border control and search-and-rescue or navigation safety. Where a system's intended use includes both, the system will fall within the scope of the use cases listed in point 7 of Annex III because of its intended border-control use.

iv. Interplay with AI prohibited practices

(382) Where an AI system used by or on behalf of competent public authorities in the field of migration, asylum, and border-control management falls under one of the practices listed in Article 5 AI Act, its use should be prohibited. Where not all of the conditions of that provisions are met for a prohibition to apply, the system should be classified as high-risk, provided it falls within one of the use cases listed in point 1 or point 7 of Annex III AI Act.

(383) Article 5(1)(b) AI Act prohibits AI systems that exploit a natural person's vulnerabilities (age, disability, specific social or economic situation) with the objective or effect of materially distorting that person's behaviour in a manner likely to cause significant harm. Behaviour-analysis tools (e.g., those assessing voice-stress, micro-expressions, or gaze patterns) are not, in themselves, prohibited merely because they misinterpret stress or cultural expressions. Such misinterpretations may affect the assessment of evidence, but do not necessarily have the object or effect of distorting a natural person's behaviour.

(384) AI systems that, over a period of time, evaluate or rank migrants based on physiological reactions, behaviour (including online activity), or other personal data to derive a generalised trustworthiness or risk score, especially where used across contexts or to produce detrimental treatment, may amount to social scoring prohibited by Article 5(1)(c) AI Act.. Providers and deployers must also ensure that the use does not amount to prohibited social-scoring practice under Article 5(1)(c) AI Act.

(385) Tools that predict future criminal behaviour of persons at borders (e.g., 'criminal intent" from gaze/speech patterns) may fall within the prohibition listed in Article 5(1)(d) AI Act. Where the conditions of that provision are met, the prohibition applies. Where not all conditions of Article 5(1)(d) AI Act are met, the same tool may be classified as high-risk under point 7(b) of Annex III where its intended purpose is the assessment of a migration risk. Providers and deployers must ensure that the use does not amount to prohibited individualised crime risk assessments under Article 5(1)(d) AI Act.

(386) Deception or credibility analysis AI tools (e.g. micro-expression/voice-stress) used at borders are not considered RBI systems covered by the prohibition in Article 5(1)(h) AI Act, because they do

not establish the identity of natural persons via a database comparison. Such AI tools will generally be classified as high-risk pursuant to point 7 of Annex III.

(387) The deployment of an AI system for real-time RBI for law enforcement purposes in the vicinity of a border is only permitted if strictly necessary for the objectives listed in Article 5(1)(h)(i)-(iii) AI Act and if all the requirements of Article 5(2)-(5) AI Act are fulfilled. However, as explained in the Commission Guidelines on prohibited artificial intelligence practices, a border crossing point is not considered a publicly accessible space, so that the prohibition does not apply in that context, whereas the street leading to a border crossing point or a forest in the vicinity normally is such a space. Some spaces may have a dual function. For example, an airport is generally considered a publicly accessible space as regards its common areas, but the area dedicated to border control (where the customs officials stand, and passports or ID checks are carried out) is not and therefore the deployment of real-time RBI systems in such areas is excluded from the scope of the prohibition, but likely to be classified as high-risk pursuant to either point 1 or point 7 of Annex III AI Act.

3.7.2. Point 7(a): AI systems intended to be used as polygraphs or similar tools

(388) Point 7(a) of Annex III classifies as high-risk AI systems intended to be used in the field of migration, asylum and border control management as polygraphs or similar tools. Such AI systems are generally designed to analyse physiological, behavioural or biometric signals with the purpose of inferring deception by natural persons in migration, asylum or border-control settings. Where such systems are intended to be used by or on behalf of law enforcement authorities in those settings, they will be classified as high-risk pursuant to point 6(b) of Annex III.

(389) The high-risk classification under point 7(a) of Annex III reflects the serious consequences that such systems may have for decisions on entry, stay or protection, combined with documented risks of inaccuracy and bias. Such systems are considered high-risk when intended to be used in the migration, asylum and border control contexts even if the competent authorities may not take the final decision on entry, stay or protection. Even where a human makes the final decision, the output of the system may significantly influence that decision due to overreliance and automation bias.

(390) Polygraphs or similar tools cover a range of modalities, including analysis of voice patterns (voice-stress analysis), micro-expressions or facial muscle activity, gaze, posture, or body movements, thermal imaging of physiological responses, multimodal interview platforms combining these signals (see chapter 3.6.3 Point 6(b): Polygraphs and or similar tools). If any of the modalities are used by the AI system for purposes other than to infer or detect deception (e.g. for language or dialect detection), the system is unlikely to be classified as high-risk under point 7(a) of Annex III.

a) Practical example of an AI system falling within the use case of point 7(a) of Annex III

- Border guards deploy an AI system in secondary inspection at an external airport. During an officer-led interview, the system analyses the traveller's verbal and non-verbal responses and provides the officer with a supplementary credibility indicator.

- A consular authority uses an AI system that analyses an applicant's voice patterns and verbal responses during visa interviews conducted by consular officers, providing the officer with supplementary indicators relating to the veracity of the statements made.

(391) Such systems fall within point 7(a) because they function as polygraph-type tools used in migration, asylum or border-control procedures to assess truthfulness. The filter mechanism of Article 6(3) AI Act does not apply to the systems described in the example above, since the system generates evaluative outputs that directly influence the substance of an individual examination and cannot be considered a narrow procedural, preparatory or post-decision task under the exceptions listed in that provision.

(392) Additionally, such AI systems are not prohibited per se under Article 5(1)(b) AI Act, unless designed or used to materially distort behaviour of vulnerable persons in a significantly harmful manner. Additionally, such AI systems are not prohibited under Article 5(1)(h) AI Act, nor are they classified as high-risk under point 1(a) of Annex III because they are not RBI systems: they operate with the person's active involvement in a face-to-face interview (so not 'remote"), they do not perform one-to-many identity matching against a reference database (they infer credibility, not identity), and their processing is not aimed at establishing identity (in real time).

b) Practical examples of AI systems falling outside of the use case of point 7(a) of Annex III

- AI system that processes interview audio (as lie-detection tools do) but does not infer deception. Instead, it automatically transcribes the interview or translates responses into another EU language for the case file.
- AI system intended only to create neutral, non-prioritised summaries of interviews for the file, without credibility scoring or recommendations. This system falls outside point 7(a) of Annex III because the system does not assess deception.

c) Practical examples of AI systems falling within the use case but exempted under the filter mechanism of Article 6(3)

- An AI system intended to normalise audio/video signals (e.g. denoising, adjusting lighting, extracting facial landmarks) so that caseworkers can review recordings more easily. If the system does not produce or imply deception inferences, it could benefit from the exception for AI systems intended to perform a preparatory task listed in Article6(3)(d) AI Act.

3.7.3. Point 7(b): AI systems intended to be used for risk assessment of persons seeking to enter or stay

(393) Point 7(b) of Annex III classifies as high-risk AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assess a risk, including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State.

(394) The most important element in determining whether an AI system should be classified as high-risk pursuant to point 7(b) of Annex III is the intended purpose of the system to produce an individual risk score, category or flag that can influence decisions on entry, stay, detention, return or related measures. By contrast, AI systems that combine data streams into a higher-level summary (for example, by summing, averaging, or grouping data) to produce aggregate flow or staffing analytics,

where outputs are not linked to identified individuals, should not be classified as high-risk pursuant to point 7(b) of Annex III.

(395) AI systems that fall within the scope of the use case listed in point 7(b) of Annex III often amount to profiling because they assess a risk posed by a natural person. What matters is whether the system processes personal data in that context. In such a case, the system cannot benefit from the filtering mechanism in Article 6(3) AI Act. For example, AI systems that output a per-person risk flag or risk score, by using or inferring information about that person, conduct automated processing of personal data to evaluate or predict that person's behaviour or movements and thus perform profiling. In contrast, if anonymised data are processed by the system so that no individual is identified or identifiable, the system should not be considered to perform profiling. Low-level aggregation or linkability with other datasets can still make aggregated data (i.e. combined statistics on means, counts, rates) fall under the definition of personal data. AI systems that produce aggregate-only outputs that are never applied to identified or identifiable persons should be considered to fall outside the use case listed in point 7(b) of Annex III. However, if the system applies an aggregate indicator to a named or identifiable traveller to generate a risk flag or triage, its use involves personal data and constitutes profiling and therefore should be classified as high-risk pursuant to that provision.

(396) An AI system falling with the use case listed in point 7(b) of Annex III may only benefit from the filter mechanism in Article 6(3) AI Act where it performs a narrow procedural or purely preparatory function that does not itself amount to profiling and does not materially influence the substance or outcome of an individual risk assessment. However, combined configurations are assessed as a whole, not individually (see Section 2.3. above).

a) Practical examples of AI systems falling within the use case of point 7(b) of Annex III

Person-level migration or security risk scoring

- **Risk scoring for entry checks:** An AI system intended to analyse a traveller's personal history, travel patterns and watch-list matches to produce a 'risk score" used by border guards to decide whether to refer the person to second line checks.

- **Automated security risk flagging**: An AI system intended to compute per-person risk flags (security, irregular-migration, or health) during travel authorisation or visa processing, using indicators based on certain trends and screening rules, and to refer named travellers for further checks.

- **Visa risk scoring (case pattern):** An AI system intended to rank visa applicants by predicted overstay risk using nationality and similar proxies, leading to intensive tracks for specific groups. Such an AI system may fall under the prohibition listed in Article 5(1)(c) AI Act only if it amounts to generalised social behaviour scoring over time across contexts treating the person detrimentally.

- **Online search-based migration intent flagging**: An AI system intended to infer a named traveller's likelihood of irregular migration from their recent online search behaviour and to generate a risk flag for individual persons used at entry control. Such an AI system is not prohibited under the AI Act unless (i) it performs social scoring within the meaning of Article

5(1)(c) AI Act, by, for example, generating generalised trustworthiness ranking over time and across contexts treating the person detrimentally or (ii) it predicts criminal behaviour in a prohibited way within the meaning of Article 5(1)(d) AI Act.

These systems are intended to produce an evaluative output about an identified or identifiable person (for example, a score, a flag, or a rank) that is used to triage or channel that person for further checks or stricter treatment related to entry or stay in the Member State. Such outputs materially influence the substance of the assessment and are not tasks that qualify for the filter mechanism in Article 6(3) AI Act. Such tools may also be used to infer the risk to security that the individual intending to enter or who has entered the territory of a Member State may constitute.

Person-level health-risk flagging

– An AI system intended to assess whether an individual presents an infectious disease risk based on biometric readings and recent travel history, and to flag them for additional medical checks. This is a substantive evaluation about an identified or identifiable person that directly steers treatment at the border; they are not tasks that could qualify for the exception listed in Article 6(3) AI Act.

Object and itinerary signals mapped to person-level risk

– An AI system intended to process licence-plate reads and travel-time data in order to generate an individual alert that a named traveller presents a heightened risk of irregular migration, because their journey between two points was abnormally long, and to refer that person to secondary screening. The alert is specified and used as a risk indicator about a natural person, even if a second AI system or a human performs the final assessment. Although the initial signal originates from a vehicle or a route, the intended use is to generate an alert for a specific person and refer that person to second line checks. Once the system outputs a person-specific risk indicator used for triage, it materially influences the assessment and is not eligible for the filter mechanism in Article 6(3) AI Act.

Group-level risk indicators applied to individuals

– An AI system intended to derive group-level risk indicators from aggregate historical data (for example, overstay rates by route and season) and to apply those indicators to the personal data of named travellers to generate individual irregular-migration risk flags that are used to refer the person for enhanced checks.

AI system consisting of several non-high-risk components

– An AI system intended to derive group-level indicators from aggregate historical data (for example, overstay rates by route and season) is combined with a non-AI rule-based engine that applies those indicators to named travellers to generate per-person irregular-migration risk flags used to refer the travellers to secondary screening. Taken separately none of the modules is high-risk under point 7(b), the analytics module outputs only aggregate statistics and the rules engine is not an AI system. However, used together with the intended purpose of assessing a risk posed by a natural person, the combined set-up should be classified as high-risk; it is not eligible for the filter mechanism in Article 6(3) AI Act.

b) Practical examples of AI systems falling outside the use case of point 7(b) of Annex III

Aggregate or cohort-level analytics

- An AI system intended to process and aggregate large amounts of data to detect trends and patterns in migration, anticipate flows, or identify possible irregular migration networks at an aggregate level, where no natural persons are identified or identifiable from the aggregated data. Since the outputs do not concern identified or identifiable natural persons the system is not covered by use case listed in point 7(b) of Annex III.

- An AI system intended to process aggregate data (e.g. country of origin, route characteristics, real-time epidemiology) to flag an incoming group as having an elevated health risk and to trigger public-health measures (testing or quarantine). Since the system does not assess the risk posed by an identified or identifiable natural person, and the same measure is applied to all members of the cohort (e.g. everyone on a specific flight is tested), it falls outside the use case listed in point 7(b) of Annex III. If the data used to estimate the group risk is personal, the GDPR applies, but the system remains outside the scope of the use case. If the system, or combined configuration that includes the system, is intended to select specific individuals within the group for different treatment based on their individual features, then it should be considered to assess the risk posed by natural persons and falls within the use case.

Vehicle-focused screening without mapping to a person

- An AI system intended to process licence-plate reads and travel-time data in order to flag vehicles with unusually long journeys and route the vehicle to a general secondary lane for a technical inspection, without creating or implying a risk assessment about the driver or passengers. If the output is framed and used strictly as vehicle-level logistics, not as a personal risk indicator, it will not fall with the use case listed in point 7(b) of Annex III. If the border guards then also check the passengers as a standard operational consequence of a flagged vehicle, that does not convert the AI system's output into a person-level risk assessment.

- An AI system intended to monitor vehicles transiting a border crossing point to flag stolen vehicles for secondary checks does not assess risks posed by a natural person within the meaning of point 7(b) of Annex III.

Post-decision data cleaning

- An AI system intended to harmonise terminology and detect duplicate entries in completed risk-assessment records, after human assessment has been concluded. Such an AI system does not produce, nor is it intended to produce, a person-level risk output used in entry or stay decisions.

3.7.4. Point 7(c): AI systems intended to be used for assistance in examining asylum/visa/residence applications and associated complaints

(397) Point 7(c) of Annex III classifies as high-risk AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assist competent

public authorities in the examination of applications for asylum, visa or residence permits and with associated complaints as regards the eligibility of the natural persons applying for a status, including related assessments of the reliability of evidence. Such systems are classified as high-risk because they have the potential to materially influence the decisions of public authorities that affect people who are often in a particularly vulnerable position and errors, bias, or opacity may lead to severe, and sometimes irreversible harm (e.g., due to refusal of status or exposure to removal).

(398) Point 7(c) covers AI systems intended to assist competent authorities in examining the eligibility of applicants for asylum, visa or residence permits and in examining associated complaints that relate to the eligibility determination. This includes complaints concerning elements capable of affecting either the substantive assessment of the application (such as facts, evidence, or credibility) or the procedural fairness of the decision-making process (such as the right to be heard, interpretation, or reasoning). It does not cover complaints concerning general service quality, understood as complaints about organisational or logistical aspects of service delivery that do not affect the substance of the eligibility assessment or the procedural fairness of the decision-making process.

(399) The elements listed in point 7(c) of Annex III are alternative (asylum or visa or residence; applications or associated complaints), not cumulative. The terms 'including related assessment of the reliability of evidence' clarifies that reliability-of-evidence checks are illustrative, not exhaustive. The concept of 'assistance' is not limited to the decisions e.g. on application for international protection. It also covers earlier stages of the examination (e.g. steps that analyse interview content, documents or country-of-origin information and are relevant for the decision on the merits. Where the AI system's outputs materially influence the substance or outcome of eligibility determinations, such as by validating or challenging evidence, highlighting inconsistencies, prioritising issues, or pre-classifying status elements it should be classified as high-risk pursuant to point 7(c) of Annex III. For example, if an AI system derives its outputs from the substance of a live case (statements, documents, COI) and uses them to prioritise, flag, validate or challenge evidence, or to recommend next steps, it materially influences the examination and remains within point 7(c). While the filter mechanism in Article 6(3) may be relied upon for narrow procedural or purely preparatory tasks, the systems assessing reliability of evidence generally materially influence decision-making and should in principle be classified as high-risk (e.g. in case of detection of document morphing).

(400) Where a single integrated assistant is intended to assist in the examination of eligibility (and associated complaints) and its outputs can materially influence substance (e.g. by validating or challenging evidence, prioritising issues, or pre-classifying status elements), the overall AI system falls within the use case listed in point 7(c) of Annex III. If individual functionalities are truly separable and put into service independently (e.g. as stand-alone tools), each functionality may be assessed on its own for possible high-risk classification. Some modules can qualify for as the exceptions for AI systems intended to perform narrow procedural or purely preparatory listed in Article 6(3)(a) and (d) AI Act, while others remain high-risk. However, low-risk modules inside a single assistant that steers eligibility analysis, cannot benefit from the filter mechanism. Nor does embedding low-risk modules inside a single assistant that steers eligibility analysis bring the overall system under the filter mechanism. For the exception in Article 6(3)(c) AI Act to apply, the system must be intended to perform ex-post detection of patterns or deviations.

a) Practical examples of AI systems falling within the use case of point 7(c) of Annex III

Evidence appraisal and consistency analysis

- An AI system intended to assess the authenticity and consistency of documents or the plausibility of personal narratives and to provide credibility signals that the examiner relies on when determining eligibility of migrants to entry the country or asylum-seekers. These outputs validate or challenge evidence relied upon by the examiner and therefore assist the examination.

- An AI system intended to analyse phone data lawfully obtained from a device to validate routes, timelines or contacts and to produce signals used in an eligibility appraisal. This assists the authority's appraisal of evidence in the file.

- An AI system intended to detect document morphing, non-conforming inks, copied signatures or chip and public-key infrastructure validity as part of document verification as a step in the examination procedure for assessing eligibility for a visa, a residence permit or international protection.

Automated comparison of discrepancies against prior submissions

- An AI system intended to identify substantive or credibility-relevant discrepancies against prior submissions in order to assist the authority's subsequent examination of the application for asylum, a visa, a residence permit, or an associated complaint. Such an AI system assists the examination.

Origin inference used in the examination

- An AI system intended to analyse recorded speech to indicate a likely country or region of origin for use in the authority's eligibility reasoning and selection of country-of-origin information. The output assists the examiner when deciding whether information is treated as proven, contested, prioritised or further investigated in a specific person's file.

b) Practical examples of an AI system falling outside the use case of point 7(c) of Annex III

- An AI system intended to provide applicants with answers to frequently asked questions, to guide users to the correct forms, to schedule appointments, or to deliver application status notifications. Such an AI system does not assist the authority in examining eligibility or associated complaints, but its intended purpose is service delivery to migrant applicants.

c) Practical examples of AI systems falling within the use case but exempted under the filter mechanism of Article 6(3)

Narrow procedural tasks (Article 6(3)(a) AI Act)

- An AI system intended only to organise a case file by applying pre-defined categories for storage and retrieval (for example, 'identity documents", 'medical records", 'interview notes"), without ranking materials by importance or omitting any items. Applying fixed, predefined labels for storage and retrieval is a narrow procedural operation. The system does not evaluate evidence, set priorities, or influence the assessment.

- An AI system intended to check the completeness and formatting of visa applications, to sort or assign files for administrative handling based on public and objective criteria, while performing only technical and non-interpretative operations and without assessing the content of the application, determining the applicable procedural track, or otherwise steering the substance of the examination.

- An AI system intended to highlight verbatim differences between current and previous statements (for example, string-level contrasts), without generating any credibility assessment or recommending follow-up questions; where the system evaluates the significance of the differences or labels them as credibility concerns, the exception no longer applies.

- A pre-check tool that, under strict, objective rules (e.g., a visa facilitation agreement fixes the fee for applicants from a specific country), routes an applicant to payment of a fixed fee.

- AI system intended to check the completeness or format of travel authorisation or visa (ETIAS/VIS) files (e.g. required fields, document presence), without producing any risk score, flag or triage of individuals. Such a system performs narrow procedural tasks, rather than preparatory tasks, since it does not prepare or structure substantive content for the examination.

Preparatory tasks (Article 6(3)(d) AI Act)

- An AI system intended to transcribe interviews, translate interview transcripts or produce neutral summaries for the file, without advising on next steps or suggesting outcomes. A system that goes beyond these functions, for example by introducing elements not contained in the applicant's statements, making credibility assessments, or linking the applicant's statements to the applicable legal framework, will not benefit from the exception.

- An AI system that carries out large data scanning on electronic devices to extract metadata on the travel route taken by an individual. The system sets out a neutral output from the search providing all pieces of metadata relating to geolocation without preferring one piece of information over another. As such, it could be considered to carry out a preparatory task.

Improving a completed human activity (Article 6(3)(b))

- An AI system intended to harmonise terminology and correct grammar in a decision after the human assessment has been concluded, without introducing additional reasoning or altering the outcome. A system that infers or formulates legal or factual grounds not explicitly stated or re-evaluates credibility is not covered by the exception.

Ex-post pattern detection (Article 6(3)(c))

- An AI system intended to analyse past, completed eligibility files in order to detect decision-making patterns or deviations for quality-assurance reporting, without proposing outcomes in actual cases.

3.7.5. Point 7(d): AI systems intended to be used for detecting, recognising or identifying natural persons in migration, asylum or border control management contexts (excluding travel-document verification)

(401) Point 7(d) of Annex III classifies as high-risk AI systems intended to be used by or on behalf of competent public authorities, or by Union institutions, bodies, offices or agencies, in the context of migration, asylum or border control management, for the purpose of detecting, recognising or identifying natural persons, with the exception of the verification of travel documents. Such systems are classified as high-risk because they often apply biometric or identity recognition, where outputs can immediately trigger intrusive measures (extra screening, refusal of entry, restriction of movement, or detention) with limited time and a limited ability to contest. The combination of error rates, demographic bias, and opaque decision logic can therefore translate into wrongful identification and discriminatory treatment.

(402) High-risk classification under point 7(d) of Annex III is determined by the intended purpose; the place of deployment and the sensor modality are not decisive. Verification of travel documents is excluded from the use case listed in point 7(d) of Annex III. On-person checks used within person detection or identification, such as liveness or presentation-attack detection, may fall under that use case and, where biometric identification or categorisation is involved, under the use case listed in point (1) of Annex III.

(403) AI systems used exclusively for search and rescue are not border-control uses and therefore fall outside the the use case listed in point 7(d) of Annex III. Only functions that neither detect, recognise, or identify persons and that do not influence operational decision making may benefit from the exceptions listed in Article 6(3) AI Act.

a) Practical examples of AI systems falling within the use case of point 7(d) of Annex III

Identification of persons at border-crossing points

- An AI system using live facial recognition for identity checks at border-crossing points, comparing live camera feeds with biometric templates in connected systems and returning identity hits for operator action. Such a system is in scope because the intended purpose is to identify natural persons for border-control purposes, which falls under the terms ‘detect, recognise or identify’.

Detection that cues operational action at land or sea borders

- AI-combined satellite imagery services, surveillance towers or unmanned platforms that flag human presence for response for a border-control response acting on the persons detected.

Such a system is in scope because the intended purpose to detect people approaching a land border and to generate alerts that trigger patrol dispatch, apprehension or second-line checks.

- An AI system used for maritime surveillance that detects and tracks persons for migration management or border-control operations, including cueing interception or boarding. Such a system is in scope because the intended purpose is to detect and track natural persons for these operations, irrespective of whether the platform operates in territorial waters, the contiguous zone or on the high seas. What matters is the intended purpose, not its location. By contrast, if an AI system is tasked exclusively for safety of navigation or lifesaving, with its outputs not cueing a border control unit, but sent to a SAR (search and rescue) coordination, used only to prevent collisions or to coordinate search and rescue, not to initiate or support border-control actions, the system will be out of scope.

- An AI system intended to analyse sensor data to detect the presence or number of persons in vehicles (including hidden persons) and to generate alerts that prompt second-line checks. The system is in scope, since it concerns the detection of natural persons for border-control purposes, even without identification. The filter mechanism cannot apply because the alerts generated by the system drive operational action, which is neither a narrow procedural nor preparatory task.

Person-level monitoring in controlled facilities

- An AI system intended to monitor reception or detention areas, detect or track identified persons, and alert staff for intervention. The system detects or tracks natural persons in a migration-management setting and is therefore in scope. If the system only estimates scene-level anomalies (for example, a crowd surge or a loud-disturbance spike), without detecting or tracking persons and without person-specific alerts, it is out of scope.

b) Practical examples of AI systems falling outside the use case of point 7(d) of Annex III

AI systems that are not border-control or person-detection functions

- An AI system intended to detect persons in distress at sea exclusively to coordinate search-and-rescue operations, with no link to migration-management or border-control tasks. Such a system is out of scope because the intended purpose is lifesaving, not border control.

- An AI system intended to verify travel or identity documents (for example, chip or PKI validity, morphing or ink anomalies, copied signatures). Verification of travel or identity documents is excluded from this use case.

- An AI system embedded in a maritime or unmanned platform used by border authorities, where it is intended and technically limited to collision avoidance (for example detecting obstacles, including persons, only to prevent impacts and without generating alerts for interception, tracking, triage or any border-control response). Such a system is out of scope because its outputs are used exclusively for safety of navigation, not for migration, asylum or border-control management. Where an AI system with the same sensing or detection capability is intended to be used to cue or support border-control actions regarding persons, it will be in scope.

Analytics that do not detect, recognise or identify persons

- An AI system intended to analyse historical data to identify patterns of document fraud and to inform general indicators or staffing, without person detection. Such a system is out of scope, since its output does not detect, recognise or identify natural persons. If the patterns identified by the system are later applied to named individuals to triage them, the system would be in scope since it performs a person-level risk assessment.

- An AI system intended to estimate crowd size or gate occupancy to balance lanes and reduce queues. Such a system is out of scope, provided it is designed so that it does not detect, recognise or identify persons and does not generate person-level alerts.

c) Practical example of AI systems falling within the use case but exempted under the filter mechanism of Article 6(3)

- An AI system intended to stabilise, denoise or enhance video feeds without performing any detection, recognition or identification of persons and without producing cues for operational response. Such a system falls within the exception for AI systems intended to perform a preparatory task listed in Article 6(3)(d) AI Act.

3.8. Administration of justice and democratic processes

(404) Point 8 of Annex III AI Act identifies the administration of justice and democratic processes as one of the areas in which certain use cases of AI systems can pose significant risks to the health, safety and fundamental rights of natural persons. Recital 61 AI Act justifies the classification of such systems as high-risk due to their potentially significant impact on democracy, the rule of law and fundamental rights and freedoms, including the right to an effective remedy and to a fair trial.

3.8.1. Point 8(a): AI systems intended to be used to assist judicial authorities or in alternative dispute resolution

(405) Point 8(a) of Annex III classifies as high-risk AI systems intended to be used by judicial authorities or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution. Point 8(a) of Annex III therefore contains two distinct use cases: first, AI systems intended to be used by judicial authorities or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to concrete set of facts; and, second, AI systems intended to be used in alternative dispute resolution (for example intended for arbitration procedures) in researching and interpreting facts and the law and in applying the law to a concrete set of facts.

First use case: AI systems intended to be used to assist judicial authorities

i. Overview of use cases and horizontal issues

(406) The first high-risk use case listed in point 8(a) of Annex III concerns AI systems intended to be used by a judicial authority or on its behalf to assist that authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts. The classification of such AI

systems as high-risk aims to address the risks of potential biases, errors, and opacity when AI assists judicial decision-making. In line with Article 19 TEU and Article 47 of the Charter, Recital 61 AI Act underlines that '*the use of AI tools can support the decision-making power of judges or judicial independence, but should not replace it: the final decision-making must remain a human-driven activity*'. This reaffirms the essential role of judges in the administration of justice and the importance of their ability to decide independently.

(407) For an AI system to be classified as high-risk under the first use case of point 8(a) of Annex III AI Act, two cumulative conditions must be fulfilled: first, the AI system must be intended to be used by a judicial authority or on its behalf; second, the intended purpose of that system must be to assist the judicial authority in researching and interpreting facts and the law, and in applying the law to a concrete set of facts. These conditions and the concepts necessary to interpret them are analysed in more detail in the subsections below.

(408) As explained above, for the purposes of the AI Act, judicial authorities acting in criminal matters, or other authorities that exercise judicial functions or constitute part of the judicial system in criminal matters, should be considered as both 'judicial authorities' within the meaning of point 8 of Annex III, as well as 'law enforcement authorities' within the meaning of point 6 of that Annex.

ii. Judicial authority

(409) To fall within this use case, the AI system must be intended to be used by a judicial authority or on its behalf. The AI Act does not contain a definition of 'judicial authority'. While it follows from Recital 61 AI Act that this use case aims to primarily address AI systems that are intended to be used by judges, the term 'judicial authority' is broader and can also cover other authorities that exercise judicial functions or constitute part of the judicial system.

(410) The scope of the notion of a 'judicial authority' may vary between Member States. In many jurisdictions the term refers primarily to courts and judges exercising adjudicatory powers, such as district courts, regional courts, high courts, supreme courts and constitutional courts. Some Member States also have established special tribunals as judicial authorities.

(411) At the same time, point 8(a) of Annex III is not intended to cover the judicial administration, that is, institutions or bodies that are responsible for the management, governance, and support of the judiciary, rather than for the adjudication of cases themselves. The notion of judicial authority is also not intended to cover quasi-adjudicative bodies which, despite exercising decision-making functions, cannot be equivalated to judicial authorities. Thus, the notion of 'judicial authority' does not encompass bodies such as data protection authorities or competition authorities acting as administrative bodies. Their decisions, however, remain subject to judicial review by competent courts, in which case the use case listed in point 8(a) of Annex III may be relevant.

(412) The case law of the CJEU on the notion of 'judicial authority' may serve as guidance for determining whether the use case in point 8(a) of Annex III applies. According to the CJEU, a judicial authority is a body established by law, independent and empowered to make binding decisions in the administration of justice[94]; typically (but not necessarily exclusively) referring to

[94] Case C-64/16, Associação Sindical dos Juízes Portugueses EU:C:2018:117, para 38 : 'In that regard, the Court notes that the factors to be taken into account in assessing whether a body is a 'court or tribunal' include, inter alia, whether the body is established by law, whether it is permanent, whether its jurisdiction is compulsory, whether its procedure is inter partes, whether it applies rules of law and whether it is independent.'

courts or tribunals within the judicial system[95] and excluding institutions such as notaries[96]. A body may be classified as such when it is performing judicial functions, but not when exercising other functions, inter alia functions of an administrative nature. When it exercises administrative authority, without at the same time being called on to adjudicate in a specific case, it cannot be regarded as exercising a judicial function.

(413) For the purposes of Annex III AI Act, public prosecutors should generally be considered to fall within the use case for law enforcement authorities in point 6 of Annex III, since those use cases expressly include bodies responsible for the prosecution of criminal offences[97]. Whether they may also qualify as a 'judicial authority' for the purposes of point 8(a) of Annex III will depend on their institutional independence as provided for in the applicable law and the purpose for which the AI system is intended to be used by them. As regards their institutional independence, the CJEU's case-law on the role of public prosecutors in relation to Framework Decision 2002/584/JHA ('the European Arrest Warrant') may serve as inspiration[98]. The importance of such independence is highlighted in Article 5(3) and (6) AI Act, which require that judicial authorities act independently in the context of granting prior authorisation for the use of 'real-time' RBI systems in publicly accessible spaces[99].

iii. On behalf of a judicial authority

(414) The considerations set out in Section 2.5 above regarding the interpretation of the terms 'on behalf of' used in several use cases listed in Annex III are relevant for the first use case listed in of point 8(a) of Annex III. Consequently, AI systems 'intended to be used by a judicial authority or on their behalf' should cover AI systems that are intended both for the use of judicial authorities themselves, as well as by other entities in scenarios where a judicial authority may outsource certain of its

[95] Joined Cases C-508/18 and C-82/19 PPU, OG and PI, EU:C:2019:456, paras 50-51: 'In the first place, in that regard, it should be noted that the Court has previously held that the words 'judicial authority', contained in that provision, are not limited to designating only the judges or courts of Member State, but must be construed as designating, more broadly, the authorities participating in the administration of criminal justice in that Member State, as distinct from, inter alia, ministries or police services which are part of the executive (…). It follows that the concept of a 'judicial authority', within the meaning of Article 6(1) of Framework Decision 2002/584, is capable of including authorities of a Member State which, although not necessarily judges or courts, participate in the administration of criminal justice in that Member State.'

[96] Such CJEU position was reached in the context of the EU Succession Regulation. See Case C-80/19 E.E. ECLI:EU:C:2020:569, para 54, where it was noted that notaries do not have the competence to adjudicate on the issues in dispute between the parties. In another case CJEU stated that an authority must be regarded as exercising judicial functions where it may have jurisdiction to hear and determine disputes in matters of succession. That criterion applies irrespective of whether the proceedings for issuing a deed of certification of succession are contentious or non-contentious (judgment of 23 May 2019, WB, C-658/17, EU:C:2019:444, paragraph 56).

[97] Article 3(45) of the AI Act.

[98] See, e.g. Case C-509/18 PF, Joined Cases C-508/18 and C-82/19 PPU OG and PI, Case C-489/19 NJ, Joined Cases C-566/19 PPU and C-626/19 PPU JR and YC and Case C-414/20 PPU MM. In particular, Joined Cases C-508/18 and C-82/19 PPU OG and PI EU:C:2019:456, paras 88–89: 'It follows from the foregoing that, in so far as the public prosecutors' offices at issue in the main proceedings are exposed to the risk of being influenced by the executive in their decision to issue a European arrest warrant, those public prosecutors' offices do not appear to meet one of the requirements of being regarded as an 'issuing judicial authority', within the meaning of Article 6(1) of Framework Decision 2002/584, namely the requirement that it be guaranteed that they act independently in issuing such an arrest warrant. In the present case, it is, in that regard, irrelevant, for the reasons stated in paragraph 73 of the present judgment, that, in connection with the issuing of the European arrest warrants at issue in the main proceedings, no instruction in a specific case was issued to the public prosecutor's office in Lübeck or in Zwickau from the ministers for justice of the Länder concerned.'

[99] Paragraphs 392 & 394, Commission Guidelines on prohibited AI practices established by Regulation (EU) 2024/1689.

activities to a third party. If a judicial authority requests a third party (i.e. appoints or commissions a third party to perform an analysis under the authority, instruction or delegation of a judicial authority) to perform an analysis of case materia..l, and that third party uses an AI system for the purpose of that analysis, such use should be seen as the use of that AI system on behalf of the requesting judicial authority.

(415) Court appointed experts (such as technical experts, forensic experts, psychologists, social services) may in some cases be considered, for the purposes of the AI Act, as acting 'on behalf of a judicial authority' when they prepare reports requested by a judicial authority and these reports are intended to assists the judicial authority in the exercise of their adjudicative functions. In this regard the notion of acting 'on behalf of a judicial authority" should be limited to situations where the expert or third party is appointed, commissioned, instructed or delegated by the judicial authority to perform a specific task on its instructions and under its responsibility. The decisive element is not merely that the expert's report may be used in the proceedings, but that the task is carried out within the mandate given by the court and subject to its procedural control. Party-appointed experts should not fall within this notion, since they are instructed by a party rather than by the court.

(416) AI systems intended to be used by parties and their legal representatives, do not fall within the scope of point 8(a) of Annex III, as parties and their representatives are not acting 'on behalf of a judicial authority'. Therefore, AI systems intended to be used by attorneys to facilitate the submission of procedural documents to a judicial authority do not fall within the use case listed in point 8(a) of Annex III.

iv. 'Intended to be used to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts'

(417) Only AI systems that are intended to be used to assist a judicial authority in the performance of judicial tasks will fall within the use case listed in point 8(a) of Annex III. That assistance must consist of assisting a judicial authority (i) in researching and interpreting the facts and the law, or (ii) in applying the law to a concrete set of facts, or (iii) in both. This means that the intended purpose of the AI system must be to assist a judicial authority in either or both of these tasks.

(418) It is not required that an AI system necessarily assists both 'in researching and interpreting facts and the law' and 'in applying the law to a concrete set of facts'; these conditions are alternative. Both are distinct types of legal activities and the assistance of an AI system in either activity would lead to that AI system performing a function with a high significance for individual decisions. It is sufficient for the AI system to be intended to assist in either activity for it to classify as high-risk. The circumstances of use by the judicial authority are not decisive for high-risk classification. Moreover, the use case does not require that the AI system must be intended to actually perform the aforementioned tasks, but only to 'assist a judicial authority' in the performance of those tasks. This means that the AI system needs to assist the judicial authority in a manner that is relevant for its judicial decision-making. For example, an AI system could be considered to assist in applying the law to a concrete set of facts without recommending a judicial decision.

(419) The requirement of 'assistance" would not be fulfilled where the task lacks a sufficiently direct functional link to judicial reasoning or decision-making. Recital 61 AI Act explains that the classification of AI systems as high-risk should not extend to AI systems intended for purely

ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel and administrative tasks. In other words, the recital draws a distinction between AI systems that affect the exercise of judicial functions and those that merely perform administrative tasks. The latter category of systems are not intended to 'assist' a judicial authority in a way that is relevant for the high-risk classification.

(420) Even if an AI system could be considered to 'assist' a judicial authority to a degree that makes it eligible for the high-risk classification, providers may apply the filter mechanism in Article 6(3) AI Act if any of the conditions for such filtering are fulfilled, unless the AI system performs profiling.

v. 'Researching and interpreting the facts and the law'

(421) The concept of 'researching and interpreting the facts and the law' refers to the activity carried out by a judicial authority in the course of adjudication. It encompasses the examination and assessment of factual circumstances and the identification and interpretation of relevant legal provisions and jurisprudence. As such, it does not cover the mere retrieval of information. Thus, AI systems intended to be used as advanced search tools are, in general, not covered by point 8(a) of Annex III AI Act. Systems that merely organise documents, retrieve legal acts or case law, or perform keyword-based searches serve an auxiliary informational function. They facilitate access to legal sources, but do not themselves engage in legal reasoning or interpretation.

(422) However, beyond retrieval, an AI system may also assign a meaning, resolve an ambiguity, or draw legal conclusions from the retrieved sources (e.g. suggesting relevant precedents on the basis of presented facts of a case; identifying the relevant legal aspects and summarising the text; providing a legal reasoning that it infers from multiple sources). Such an AI system assists in researching and interpreting the facts and the law and thus is likely to be classified as high-risk pursuant to point 8(a) of Annex III.

vi. 'Applying the law to a concrete set of facts'

(423) The concept of 'applying the law to a concrete set of facts" refers to the core activity carried out by a judicial authority in the course of adjudication. It encompasses the subsumption of the presented facts under the applicable law and thus combines the assessment of the factual circumstances and the interpretation of relevant legal provisions and jurisprudence. This is to be understood broadly, meaning that this use case should be considered to cover both situations where the AI system assists in the full judicial assessment of a case, as well as in the assessment of its constituent elements.

a) Practical examples of AI systems falling within the use case of point 8(a)

Judicial decision/judgment drafting systems

- An AI system that analyses the factual circumstances of the case, submissions received, identifies applicable law and case law and then can generate drafts of judicial decisions/judgments or their parts, in particular the reasoning part and decision. Such an AI system falls within the use case of point 8(a) of Annex III, since it is intended to assist a judge in researching and interpreting facts and the law and also in applying the law to a concrete set of facts. Fulfilling one condition would be sufficient; however, in this case, both conditions are satisfied.

- An AI system that generates (draft) decisions in small claims cases (e.g. dispute values under a certain amount) or orders for payment (when there is no dispute that a certain amount is owned in a civil proceedings), relying on structured case data and legal templates. Such a system falls within the use case of point 8(a) of Annex III, since it is intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts. Due to its proximity to the decision-making and impact on the decision, the system does not qualify for any exception listed in Article 6(3) AI Act.

AI systems intended to be used for repetitive cases

- An AI system that is intended to support judges in handling identical or similar cases by (i) extracting relevant facts from the claim and clustering them based on recurring factual constellations across similar cases; (ii) researching a database of previous decisions to find similar cases and identify legal reasoning patterns; (iii) preparing suggestions and corresponding text modules for the final decision, based on outcomes of similar previous cases. Such an AI system would fall under point (8)(a) of Annex III AI Act. This follows because, for the purposes of high-risk classification, the system must be assessed in its combined configuration, the joint outputs of which may materially influence the outcome of the individual decision, rather than by isolating modules that, if considered separately, might either fall outside point 8(a) of Annex III or satisfy one of the conditions set out in Article 6(3). An AI system that solely performs the activity under (i) would be intended to perform a preparatory task within the meaning of Article 6(3)(d) and could thus qualify for an exemption under the filter.

AI systems selecting relevant precedents and law for a concrete set of facts

- An AI system that analyses the presented facts of the case (or their summary), then assists judges in identifying relevant laws and legal precedents and suggests how they apply to the facts of a case. Such an AI system directly assists in the core judicial task of interpreting and applying the law to a concrete set of facts and therefore falls within the use case of point 8(a) of Annex III. Due to its influence on decision-making, the system cannot benefit from any exception listed in Article 6(3) AI Act. However, for an AI system to 'assist in applying the law to a concrete set of facts', the system should select precedents and applicable law by analysing the presented facts. If the system simply performs AI-enabled searches of a database on the basis of the general area of law involved (e.g. family maintenance cases, financial crime, or attempted homicides) or keywords, such a system should be regarded as a search engine and therefore cannot be seen as intended to assist a judicial authority in researching and interpreting facts and the law, or in applying the law to a concrete set of facts.

b) Practical examples of AI systems falling outside the use case of point 8(a)

Speech-to-text systems

- An AI speech-to-text system used by a court to transcribe audio recordings of court proceedings and hearings, which then become part of the file. The system has the following functionalities: (i) it can take various audio file formats (or live audio) and produce textual transcripts, including automated speaker separation (distinguishing different voices) and insertion of punctuation;(ii) it

can correct terminology – for example, recognising legal terms or names and adjusting the vocabulary accordingly.

While the transcription of court hearings that become part of the file could be considered to assist a judicial authority to access testimonies of witnesses and parties to a proceeding, such a tool does not assist in researching and interpreting facts and the law[100]. The fact that recordings or transcripts generated by an AI system may later form part of the evidentiary record in judicial proceedings, and that inaccuracies may affect fundamental rights, does not in itself mean that the system is intended to assist a judicial authority in researching and interpreting facts and the law within the meaning of point 8(a) of Annex III. In this case, the system's intended purpose is limited to technical recording or transcription without analytical or evaluative functionalities.

The same would remain true if such an AI system is later used as technical assistance in information retrieval to help interrogate the court transcript (e.g., requesting to search 'when was topic X discussed" in order to find the location in the original audio file). That conclusion could be different where voice-to-text transcripts are further processed by an AI system to summarise or select the key arguments or produce further evaluations of relevance for the judicial decision-making, including when resulting in recommendations to judges.

AI systems facilitating communication with the public

- AI-enabled chatbots offered on the websites of courts to assist visitors to the website in finding relevant information. Such systems function as virtual assistants, and are designed to provide information to individuals about procedural steps, required documents, deadlines, and available remedies. They do not assist judicial authorities in researching and interpreting facts and the law or in applying the law to a concrete set of facts.

- An AI system designed to assist judicial authorities in drafting press releases or legal summaries on public interest cases. The system translates the technical language of a judgement into accessible summaries. Such a system performs ancillary administrative activities that do not affect the actual administration of justice in individual cases.

Case assignment systems

- An AI system assigning cases to judges taking into account their specialisation, workload, or holiday schedule. Such a system is intended to perform ancillary administrative activities that do not affect the actual administration of justice in individual cases. The evaluation could be different if the AI system also performs judicial assessments of a specific case regarding procedural prerequisite, such as whether a case should be heard in public session, whether the court has jurisdiction, or whether the case should be heard by a single judge or a panel.

[100] If such system is merely a voice-to-text AI system, it could also be deemed as an ancillary and administrative task that should not be seen as falling under high-risk use case under point 8(a) of Annex III, in line with Recital 61. Such applications fulfil a largely clerical and technical task that does not directly affect administration of justice in individual cases. Such systems facilitate record-keeping and documentation, but do not assist in judicial decision-making. Thus, they should not be equated with those AI systems that assist in assessing evidence, determining risk or drafting the reasoning of the decisions.

Processing and management of evidentiary submissions in judicial proceedings

- An AI-enabled system intended to assist a judicial authority in managing and searching large volumes of case evidence more efficiently. The functionality of the system includes: (i) providing a chronology of certain events that are documented in case evidence where the AI reconstructs timelines of events as documented across different pieces of evidence; (ii) searching and providing a reference to content within case evidence. Such an AI system is intended to assist a judicial authority in the organisation and access to factual material, without analysing, evaluating or drawing conclusions from that material. Such a system is not intended to assist in researching and interpreting facts and the law, nor in applying the law to concrete set of facts.

Other ancillary administrative activities

- AI systems intended for purely ancillary administrative activities that do not affect the adjudication of individual cases, such as the anonymisation or pseudonymisation of judicial decisions, documents, or data; internal communication between personnel; searching for delivery addresses and dispatching documents; verifying the payment of court fees; processing electronic signatures; verifying powers of attorney; and other similar administrative tasks.

c) Practical examples of AI systems falling within the use case but exempted by the filter mechanism in Article 6(3) AI Act

AI systems assisting in pre-classification of incoming applications or claims

- An AI system that analyses the content of the application or claim received by a court, as well as prior case law patterns to pre-classify the type of the case (e.g. contract law, inheritance case, etc.). In principle, such an AI system could be considered to assist in researching and interpreting facts and the law and thus fall within the use case of point 8(a) of Annex III. However, such an AI system would benefit from the exceptions for AI systems that are intended to perform a narrow procedural task or a preparatory task to an assessment listed in Article 6(3)(a) and (d) AI Act respectively. If the system also makes recommendations regarding the admissibility of the case (unless only technical checks), even if this is later reviewed by court staff, that system cannot benefit from those exceptions since it no longer can be considered to perform a narrow procedural task, due to the substantive assessment involved, nor a mere preparatory task, due to the proximity and impact on the final decision-making.

Metadata data extraction

- An AI system performing data analysis for the purpose of metadata extraction based on the facts of the file (e.g. extraction of procedural roles from the claim (parties, legal representatives, witnesses, experts, etc.) to support clerical work such as summons. Such a system would not normally be considered to be intended to assist in researching and interpreting facts and the law. Even if certain functionalities could lead to such a conclusion, the system would in any event benefit from the exception for AI systems intended to perform a narrow procedural task listed in Article 6(3)(a) AI Act.

Advanced search engines

- An AI system integrated in a public database of national case law used by public and by court personnel for searching for decisions using classical methods (Boolean operators, search through keywords, relevant legal basis, etc,); the creation of summaries of the published decisions and summaries of search results; and searching based on natural language (NLP). While such an AI system is intended to assist in researching and interpreting the law (inter alia judicial authorities) it is carrying out only narrow procedural tasks.

Language editing assistance

- An AI system intended for proofreading or improving the style of judicial decisions or judgments drafted by judges, without changing the content. It is doubtful whether such an AI system would be considered as an AI system intended to assist in applying the law to a concrete set of facts, because the degree of assistance appears negligible. In any event, the system would benefit from the exception for AI systems intended to improve the result of a previously completed human activity listed in Article 6(3)(b) AI Act.

AI systems suggesting factual questions

- An AI system is used after the judge has drafted the decision to compare the draft judgment with the case file and identify factual questions or aspects that the draft appears not to address. This may involve an interpretation of factual material. However, where the system merely carries out a compliance check, thus helping the judge to check whether all relevant factual aspects have been considered, and does not assess credibility, determine what happened, suggest how any factual question should be answered, or otherwise materially influence the judicial determination of the facts, it would performs a task intended to improve the result of a previously completed human activity (Article 6(3)(b) AI Act).

Second use case: AI systems intended to be used in similar ways in alternative dispute resolution

i. Overview of use cases and horizontal issues

(424) The second high-risk use case listed in point 8(a) of Annex III concerns AI systems that are intended to be used by alternative dispute resolution ('ADR') bodies in a similar way to AI systems that are intended to be used to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts. The classification of such AI systems as high-risk also aims to address the risks of potential biases, errors and opacity. The purpose of such classification is to ensure the same level of protection in the context of dispute resolution, regardless of whether an AI system is intended to assist such adjudication with legally binding effects within or outside the area of ordinary courts with constitutionally established adjudicative functions.

(425) For an AI system to be classified as high-risk under the second use case listed in point 8(a) of Annex III two conditions must be fulfilled: first, that system must be intended to be used by an ADR body where the outcome of the ADR proceedings produces legal effects for the parties; and, second, the intended purpose of the system must be to assist the ADR body in researching and interpreting facts and the law and in applying the law to a concrete set of facts.

ii. The concept of alternative dispute resolution

(426) ADR means adjudicating a dispute out of court with the assistance of an impartial ADR body. Examples of ADR include arbitration, mediation, conciliation, ombudsmen and complaints boards[101]. Inspiration for interpreting the concept of ADR may be found in Union legislation, such as Directive 2013/11/EU (the ADR Directive), as amended by the Directive 2025/2647, which regulates consumer ADR.

iii. Alternative dispute resolution body

(427) Point (8)(a) of Annex III refers to AI systems used in ADR 'in similar ways', which should be understood as meaning that the system is used for the same purposes as when it used by judicial authorities. Recital 61 AI Act clarifies that that should be understood as meaning that the system should be used by ADR bodies.

(428) The AI Act does not define which entities constitutes ADR bodies. For the ADR used in consumer disputes, inspiration may be found in Article 4(1)(h) of the ADR Directive[102], which defines an ADR entity as any entity, however named or referred to, which is established on a durable basis and offers the resolution of a dispute through an ADR procedure and that is listed[103] in accordance with Article 20(2) of that Directive.

(429) Beyond consumer protection, ADR bodies should be considered to include a wide set of entities that deal with civil, including commercial and labour, and other disputes. Such entities may include:

- Commercial arbitration institutions (e.g. national and international arbitration bodies) or investment dispute bodies that resolve disputes between businesses;
- Mediation centres for civil and commercial matters, established under the EU Mediation Directive (2008/52/EC)[104];
- Labour dispute resolution bodies, such as conciliation or mediation services in employment law;
- Equality bodies that offer alternative dispute resolution solutions in discrimination matters[105];

[101] For ADR in consumer disputes, see Alternative dispute resolution for consumers - European Commission.
[102] Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR). OJ L 165, 18.6.2013, pp. 63–79.
[103] https://consumer-redress.ec.europa.eu/dispute-resolution-bodies_en
[104] Directive 2008/52/EC of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters. OJ L 136, 24.5.2008, pp. 3–8.
[105] Council Directive (EU) 2024/1499 of 7 May 2024 on standards for equality bodies in the field of equal treatment between persons irrespective of their racial or ethnic origin, equal treatment in matters of employment and occupation between persons irrespective of their religion or belief, disability, age or sexual orientation, equal treatment between women and men in matters of social security and in the access to and supply of goods and services, and amending Directives 2000/43/EC and 2004/113/EC, OJ L, 2024/1499, 29.5.2024; Directive (EU) 2024/1500 of the European Parliament and of the Council of 14 May 2024 on standards for equality bodies in the field of equal treatment and equal opportunities between women and men in matters of employment and occupation, and amending Directives 2006/54/EC and 2010/41/EU, OJ L, 2024/1500, 29.5.2024.

- Professional disciplinary or regulatory bodies (e.g. in healthcare, legal professions, or engineering), which often operate ADR mechanisms to address disputes or complaints within professional practice.

iv. Producing legal effects for the parties

(430) While the wording of point 8(a) of Annex III is terse, Recital 61 AI Act clarifies that AI systems intended to be used by ADR bodies should be classified as high-risk where the outcome of the ADR proceedings produce legal effects for the parties. Accordingly, where the outcome of an ADR procedure is a voluntary agreement or non-binding recommendation, an AI system intended to be use in such a procedure will not fall within the use case listed in point 8(a) of Annex III, since the procedure do not produce legal effects for the parties.

(431) Whether ADR proceedings produce legal effects for the parties depends on the national law of the Member States. This should be verified on a case-by-case basis. For instance, arbitral awards generally have binding and final effect on the parties, similar to a court judgment. They are enforceable under national law and internationally recognised through the United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 10 June 1958)[106]. By contrast, in case of mediation and conciliation, the outcome is usually a voluntary agreement, which does not generally have binding legal force, but Directive 2008/52/EC ('the EU Mediation Directive') allows parties to stipulate that their agreement is made enforceable by a court or competent authority, giving it the same effect as a judgment.

(432) When it comes to consumer disputes, the ADR Directive explicitly acknowledges the ADR schemes that propose a solution (which the parties are free to accept), impose a solution (which can be binding upon parties, or even only binding upon trader), or bring the parties together with the aim of facilitating an amicable solution. In practice, the same ADR body may deliver more than one type of outcome, for example, depending on the parties' wishes. For the ADR proceedings to produce legal effects, it will suffice that the binding nature applies to either party (i.e. only the trader).

(433) The 2025 amendments to the ADR Directive have introduced additional safeguards for the use of automated decision-making in the decision-making process (actions which influence decisions on whether to deal with the dispute and decisions concerning the outcome of the dispute, and as excluding purely administrative or technical tasks). Namely, the parties shall be informed that automated means are used and have a right to request a human review of the outcome. These additional safeguards apply in parallel with the AI Act and are not limited to AI systems, covering also technologies falling outside the scope of the AI Act.

(434) Where the outcome of an ADR proceeding produces legal effects for the parties, an AI system whose intended purpose is to assist the ADR body in researching and interpreting facts and the law, or in applying the law to a concrete set of facts, shall be classified as high-risk pursuant to point 8(a) of Annex III. Practical examples of AI systems falling within the scope of this use case can be derived from the examples provided for AI systems intended to be used by judicial authorities above.

[106] https://www.newyorkconvention.org/english.

3.8.2. Point 8 (b): AI systems intended to be used for influencing the outcome of elections or referendum

i. Overview of use cases and horizontal issues

(435) Point (8)(b) of Annex III lists as high-risk AI systems intended to be used for (i) influencing the outcome of an election or referendum or (ii) the voting behaviour of natural persons in the exercise of their vote in elections or referenda. That provision clarifies that this use case does not include AI systems the output of which natural persons are not directly exposed to, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view. Recital 62 AI Act explains that the classification of AI systems falling within this use case as high-risk aims to address the risks of undue external interference with the right to vote enshrined in Article 39 of the Charter, and of adverse effects on democracy and the rule of law.

(436) For an AI system to be classified as high-risk under the use case listed in point 8(b) of Annex III AI Act, two conditions must be fulfilled: first, the intended purpose of the AI system must be to influence the outcome of an election or referendum, or to influence the voting behaviour of natural persons in the exercise of their vote in elections or referenda; second, natural persons must be directly exposed to the outputs of the AI system. These conditions and the concepts necessary to interpret them are analysed in the subsections below.

ii. Intended to influence the outcome of an election or referendum or the voting behaviour of natural persons

(437) Only AI systems intended to be used to influence the outcome of an election or referendum or the voting behaviour of natural persons, i.e. the AI system would have to be specifically intended to have an effect on the electorate's choice or turnout, fall within the scope of the use case listed in point 8(b) of Annex III. The focus of the use case is thus on underlying objectives: the system must be directed towards electoral influence, not merely be incidentally capable of it. Therefore, AI systems with non-intentional influence on the outcome of an election or referendum or the voting behaviour of natural persons, such as general content recommender systems that, amongst other content, also recommend political content and thus, de facto, have the potential to influence political opinions, should not be classified as high-risk. General-purpose AI systems, which offer sufficient safeguards against a use influencing electoral processes, e.g. a chatbot clearly replying that it cannot give any voting advice when asked by a user, or providing only neutral, factual, and informational content about elections (voting procedures (how, when, where), registration procedures; the institutional and legal framework; objective information on parties and candidates (e.g. references to their official websites); and general civic education on democratic processes) would also not fall under high-risk category as not being intended to influence the outcome of an election or referendum or the voting behaviour of natural persons.

(438) That the AI system should be intended to be used to influence the outcome of an election or a referendum or to influence the voting behaviour of natural persons in the exercise of their vote in elections or referenda means that the scope of the use case is both collective influence (the outcome of the elections or referenda as a whole) and individual influence (the behaviour of individual voters). Despite their alternative formulation, those two use cases are partially overlapping. That is because the influence of voting behaviour has as its necessary consequence an influence on the outcome of an election or referendum, whether by shaping the electorate's choices or by affecting voter turnout, and thus altering the distribution and the outcomes of votes. The wording of point

8(b) of Annex III explicitly ties the influencing of voting behaviour to the 'exercise of [a] vote in elections or referenda'.

(439) The inclusion of 'voting behaviour' in point 8(b) of Annex III clarifies that this high-risk use case covers AI systems which are intended to shape the decision-making of individual electors, even if the final outcome (the overall result) is not directly targeted. Without the reference to voting behaviour, a narrow reading could suggest that the high-risk rules only apply where there is a demonstrable risk of altering the collective outcome of an election or a referendum. However, such a reading would be contrary to the primary objective of including this use case for protecting democratic processes from undue external interference. Conversely, influencing the outcome of elections or referenda has a broader meaning, as it can go beyond voting and relate to other stages of the electoral process, such as redrawing the boundaries of constituencies.

iii. The scope of voting behaviour

(440) Point 8(b) of Annex III refers to 'voting behaviour of natural persons'. In this context, voting behaviour should be understood to cover both electoral choice and electoral participation. Therefore, 'voting behaviour of natural persons' should be understood as covering not only how individuals cast their votes (e.g., which party or candidate they support), but also whether they choose to participate in elections or referendum in the first place. Those terms also cover both active voting and abstentions (not turning out to vote or through casting a blank/invalid ballot).

(441) Point 8(b) of Annex III does not require that the voting behaviour of natural persons is effectively influenced. To fall within the use case, the AI system must be intended to be used for that purpose (incl. when being advertised to be used for a particular purpose). The actual result of the AI system after its deployment is immaterial.

iv. Link to elections or referenda

(442) The two use cases listed in point 8(b) of Annex III both explicitly refer to the outcome or exercise of a vote in elections or referenda. This should be understood as a requirement that the AI system is developed to be used in the context of an election or referendum. The notion of elections or referenda should be understood as encompassing those that may take place at the European, national, regional, or local level.

v. Applicability of the high-risk classification regardless of the type of intended deployer

(443) Point 8(b) of Annex III refers to AI systems intended to be used for a particular purpose, therefore requiring all providers of such AI systems to classify them as high-risk. The provision does not specify who provides, puts into service, or uses the AI system. The decisive factor is the intended purpose of the AI system as specified by the provider, not who the deployer will be.

(444) In practice, AI systems intended to be used to influence the outcome of elections or referendum, or the voting behaviour of natural persons, may be expected to be provided or put into service for use by the following types of deployers (non-exhaustive list):

- Political parties, political foundations, campaign organisations, and candidates in elections: these can be expected as the primary actors who would deploy AI systems to influence voting

behaviour or the outcome of an election or referendum. The exclusion clause in the second sentence of point 8(b) supports this.

Third parties (e.g. advocacy groups): these persons or bodies may also have an interest in influencing the outcome of an election or referendum or the voting behaviour of natural persons, or may do so in the interest of political actors. Media outlets in many cases fall outside the scope; however, this assumption may not hold in all situations, for example, where media outlets are affiliated to a campaign organisation or party-run, or where they offer voting advice applications.

vi. Natural persons are exposed to the output

(445) Point 8(b) of Annex III clarifies that it does not include AI systems to the output of which natural persons are not directly exposed, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view. This generally excludes AI systems used by political parties or candidates to increase back-office efficiency.

vii. Interplay between legitimate influencing of political opinions and foreign information manipulation and interference

(446) Political influencing is a legitimate activity which is part of the electoral context, insofar as it is in compliance with existing EU and national law. The high-risk classification of point (8)(b) of Annex III does not aim at restricting the development or use of AI systems for these purposes, but ensures that they are developed and used in a safe and trustworthy manner with safeguards to address risks to fundamental rights and democratic values.

(447) Manipulation or interference with elections, in particular foreign information manipulation and interference (FIMI), is an illegitimate activity and addressed by specific EU acquis, such as the Regulation (EU) 2024/900 (Political Advertising Regulation)[107], Regulation (EU) 2022/2065 ('the Digital Services Act')[108] and the European Democracy Shield[109][110]. The AI Act adopts a product safety approach and addresses a different layer, namely the safety and trustworthiness of AI systems which are legitimately used. Under the AI Act, only a certain number of AI practices that pertain to placing on the market, putting into service, or use of AI systems with unacceptable risk is prohibited; the classification of AI systems as high-risk does not serve that purpose.

[107] 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.*

[108] 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.*

[109] Joint Commission 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, JOIN(2025) 791 final.

[110] These EU instruments are complimentary. Thus, for instance, AI systems embedded in very large online platforms' services will be subject to transparency and risk management obligations under the Digital Services Act, and will be required to comply with the rules of Political Advertising Regulation and to the risk-based rules of AI Act.

a) Practical examples of AI systems falling within the use case of point 8(b) of Annex III

AI-enabled targeting of political ads

- An AI system intended to optimize the targeting and ad delivery of political advertising within the limits set by Regulation (EU) 2024/900 (Political Advertising Regulation) (including specialised recommender systems). Such AI system is intended to influence the outcome of an election or referendum by influencing the political opinions of potential voters. In many cases such systems will include profiling, and thus would not allow for the AI systems to be filtered under Article 6(3) AI Act.

AI-enabled chatbot intended to promote support for candidates or policies

- An AI-enabled chatbot (or a virtual spokesperson/agent) developed for use by political actors to interact with natural persons in a conversational manner, simulating political dialogue with voters to persuade them to support a candidate or policy[111]. Such an AI system falls within the use case of point 8(b) of Annex III, because it is within its intended purpose to impact political opinions of natural persons and, ultimately, the electorate's choice.

AI-enabled voter advice applications

- An AI system designed to recommend political parties or candidates based on an individual voter's views, for example asking natural persons interacting with the system a set of questions about political preferences, values, or political issues and then comparing the answers with the positions of political parties or candidates, presenting the 'closest match'[112]. Such an AI system generates personalised recommendations, which can steer preferences towards particular political parties or candidates and shape perceptions of political proximity to the potential voter.

b) Practical examples of AI systems falling outside of the use case of point 8(b)

Optimisation of political campaigns from an administrative or logistical point of view

- AI systems that optimise campaign staff (including volunteers) management; AI systems scheduling rallies, assigning party members to them or selecting topics to focus on. Such systems are excluded from high-risk classification by the second sentence of point 8 (b) of Annex III.

- AI systems analysing earlier party donor databases to predict likelihood of contributions for the current or future campaign. Such systems are excluded from high-risk classification by the second sentence of point 8(b) of Annex III.

- AI systems designed for generating political advertising content (e.g. generative AI systems that could be used to draft political slogans and communications to be reviewed and delivered by a

[111] This system would also be subject to transparency obligations under Article 50 of the AI Act.

[112] Whether a voter advice application qualifies as an 'AI system' depends on its underlying functionalities. A voter advice application would not qualify as an AI system if its operation were limited to rule-based or purely statistical matching without adaptive or inferential features (e.g. static questionnaires with fixed scoring). For the definition of AI system, please refer to the Commission Guidelines on the definition of an AI system.

political party), without further disseminating it. Such systems assist in preparation of political campaigning materials and are not 'intended to influence the outcome of an election'[113].

AI systems intended for monitoring, research and pattern recognition

- AI systems monitoring the activity of elected officials in submitting legislative proposals or amendments based on content provided by a parliament's web presence. This monitoring activity mainly serves informational purposes; it does not have as its direct purpose to influence the outcome of elections. This system falls outside the scope of point 8(b) of Annex III.

- AI systems deployed by sociological agencies for the purpose of collecting, analysing, and presenting information in an objective and transparent manner. Such AI systems do not fall under point 8(b) of Annex III, provided that their sole function is to inform the public or relevant stakeholders without seeking to influence electoral processes.

- AI systems used by academic institutions for modelling electoral behaviour for research purposes. Such systems are not intended to influence the outcome of elections. In any event, it is likely that such AI system would be excluded under Article 2(6) AI Act.

Technical assistance in vote counting

- AI systems for counting ballots automatically. If an AI system is used only for mechanical recognition and tallying of ballots (e.g. scanning, OCR), then it is functioning as a technical aid and should not be classified as high-risk as its intended purpose does not correspond to the one defined in point 8(b) of Annex III.

Chatbots to provide information on the elections

- An AI-enabled chatbot[114] designed to provide information to voters on behalf of election authorities, operating in a politically neutral way (e.g. providing information when the elections take place, where a person can vote, voting times, etc.)[115].

c) Practical examples of AI systems falling within the use case but exempted by the filter mechanism in Article 6(3) AI Act

- An AI system that checks the tone of campaign texts already written by humans, highlighting potentially unclear or counterproductive wording, wording conflicting existing party materials, or suggesting rewording to convey the sentiments or values prioritised by the party. While it could be argued that the AI system is intended to influence the outcome of an election by impacting the electorate's choice, such AI system could be exempted because it is intended to merely improve the result of a previously completed human activity (Article 6(3)(b)).

[113] This system would however be subject to transparency obligations under Article 50 of the AI Act.
[114] Please note that not all chatbots are AI systems. Please refer to the Commission guidelines on the AI system definition.
[115] This system would however be subject to transparency obligations under Article 50 of the AI Act.

V. Entry into application of the rules for high-risk AI systems

[see separated chapters]

VI. Review and update of the high-risk use cases and the Commission guidelines

[see separated chapters]