Matheson

Is your AI system high-risk?

Key takeaways from European Commission's draft guidelines

Authors: Marie McGinley, Davinia Brennan, Sarah Jayne Hanna
Co-Authors: Kristina Radits (Solicitor), Celeste Cannon (Trainee)

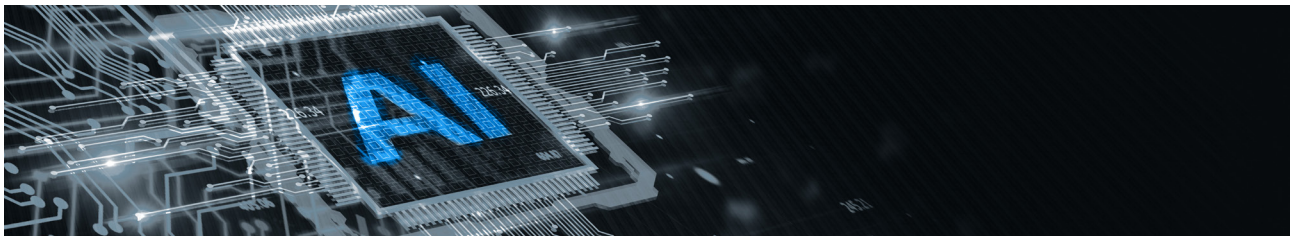
Matheson

Introduction

The European Commission recently published the eagerly anticipated draft guidelines (the "**Guidelines**") on the classification of high-risk AI systems under Article 6 of the EU Artificial Intelligence Act ("**AI Act**"). The Guidelines, though not legally binding, seek to support providers and deployers of AI systems in assessing whether an AI system should be classified as high-risk, as well as competent market surveillance authorities, thereby facilitating the uniform application and effective enforcement of Article 6 AI Act. The Guidelines set out the Commission's interpretation of certain concepts that are relevant for classification purposes, and, in accordance with Article 6(5) AI Act, provide practical examples of AI systems that may or may not be classified as high-risk under Article 6 AI Act.

The scope of the Guidelines is limited only to whether an AI system is high-risk or not. The Guidelines will be complemented in the future with other Commission guidelines aimed to facilitate compliance with the requirements for high-risk AI systems and the obligations for providers and deployers.

The Guidelines are divided into three sections, including (1) the general principles for assessing high-risk classification; (2) high-risk AI systems embedded into regulated products under Article 6(1) AI Act; and (3) stand-alone high-risk AI systems under Article 6(2) AI Act. This article provides an overview of each section of the Guidelines and the key takeaways that businesses should consider when assessing whether their AI systems should be classified as high-risk.



1. The General Principles

The Guidelines note that the scope of use cases falling within the "high-risk" category are limited and proportionate, covering only those AI systems that pose a significant risk of harm to the health and safety of individuals, or may have an adverse impact on fundamental rights.

Two routes to classification as high-risk

The Guidelines highlight that an AI system can be classified as high-risk in two scenarios:

(i) under Article 6(1), where it is a system which is intended to be used as a safety component of a product, or the AI system itself is a product, covered by the EU harmonisation legislation listed in Annex I, **and** the product whose safety component is the AI system or the AI system itself is required to undergo a third-party conformity assessment; or

(ii) under Article 6(2), where the system falls into one of the use cases listed under the areas in Annex III AI Act.

The system must be an AI system

A pre-condition to an assessment of whether an AI system is high-risk, is whether the system qualifies as an "AI system" within the meaning of Article 3(1) AI Act. That provision defines an AI system as *"a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"*. Accordingly, not every software application or automated decision-making system falls within the scope of the AI Act.

More information on how the Commission interprets the definition of an AI system is available in the Commission's guidelines on the definition, which were adopted pursuant to Article 96(1)(f) AI Act (available here).

Intended purpose(s) of the AI system

The Guidelines emphasise that the "intended purpose" of an AI system plays an important role in its classification as high-risk. According to Article 3(12) AI Act, the "intended purpose" of an AI system means "the use for which that system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials, and statements, as well as in the technical documentation". Providers must therefore ensure that such purposes are comprehensively described in their technical documentation, as well as other related materials (eg, contractual arrangements, promotional or sales materials, and policies etc). In this regard, the intended purpose must be distinguished from "reasonably foreseeable misuse" of an AI system, defined in Article 3(13) AI Act, which is, by definition, a use outside the intended purpose of the system.

Importantly, the Guidelines note that if the instructions for use, contractual arrangements, terms of service etc, present the AI system as broadly applicable across a generality of contexts and functions, and do not consistently limit its application or exclude high-risk uses, the system's intended purpose will be deemed to also encompass high-risk use cases and therefore qualify as high-risk. Furthermore, merely asserting (for example, in the terms of service) that high-risk uses are excluded will not be sufficient to avoid the system from being considered high-risk, where the provider's overall presentation, examples, or product positioning effectively provides for or promotes such uses. Any limitations of use must therefore be clearly, concretely, and coherently described across all materials.

Third parties becoming "providers" under Article 25 AI Act

The Guidelines reiterate the possibility under Article 25 AI Act of distributors, importers, deployers or other third parties becoming subject to provider obligations if they: (i) put their name or trademark on a high-risk AI system already placed on the market or put into service, (ii) make a substantial modification to a high-risk AI system that has already been placed on the market or put into service in such a way that it remains a high-risk system; or (iii) modify the intended purpose of an AI system (including a general-purpose AI system) which has not been classified as high-risk, in such a way that it becomes high-risk under Article 6 AI Act.

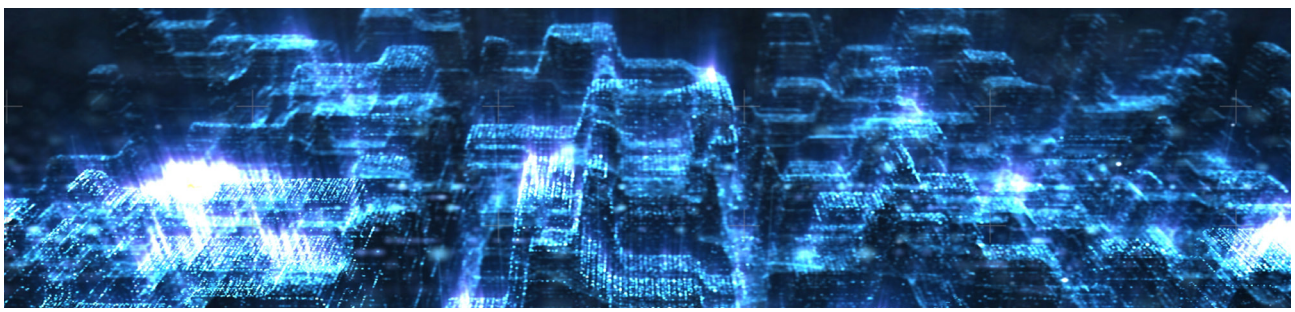
Businesses should therefore be alert to this provision and ensure that they tread carefully when modifying any elements of the AI system or seeking to put their name on it so as to avoid inadvertently becoming a provider and having to comply with the corresponding (and onerous) obligations.

Timeline for application of high-risk AI system rules

The Guidelines refer to the recent provisional agreement between the European Parliament and Council on the AI Digital Omnibus Regulation (2025/0359/EU), discussed here (the "**Proposal**"), which proposes extending the timeline for implementation of rules on high-risk AI systems from 2 August 2026 until:

- **2 December 2027** for stand-alone high-risk AI systems under Article 6(2) and Annex III of the AI Act; and
- **2 August 2028** for high-risk AI systems embedded into regulated products under Article 6(1) and Annex I of the AI Act.

This postponement is necessary to give the European Commission additional time to put in place the necessary technical standards, tools and guidelines needed to clarify the application of the high-risk AI rules (including these Guidelines) and help businesses comply with their new obligations.



2. High-risk AI systems embedded into regulated products under Article 6(1) and Annex I AI Act

The Guidelines note that, in line with the AI Act's risk-based approach, only AI systems that present significant risks to health, safety, or fundamental rights are classified as high-risk. Accordingly, not all AI systems that are components of regulated products, or that are regulated products themselves, are high-risk AI systems. Only a sub-set of such products qualify as such, namely those that fulfil the cumulative conditions in Article 6(1) AI Act.

For example, the Guidelines recognise that many consumer AI systems will not meet these conditions, such as smart home appliances (eg, thermostats, refrigerators, washing machines) that are designed for comfort, convenience or optimisation, as their malfunctioning is unlikely to result in a risk to health and safety of individuals or damage to property.

There are two cumulative conditions under Article 6(1) AI Act that must be satisfied for an AI system to be classified as high-risk. Firstly, the AI system must be intended to be used as a safety component of a product, or the AI system itself must be a product, covered by the EU sectoral legislation set out in Annex I of the AI Act; **and** secondly, the product is required to undergo a third party conformity assessment.

Condition 1 - What is a safety component?

The definition of a "safety component" in Article 3(14) AI Act is key in determining whether condition 1 is satisfied. The Guidelines note that this definition can be understood as laying down two alternative scenarios in which an AI system may be classified as a "safety component". On one hand, that will be the case where the system fulfils a safety function, or on the other hand, where the system's failure or malfunctioning would endanger the health and safety of persons or property.

(i) Safety Function

Under the first scenario, the Guidelines confirm that an AI system constitutes a safety component of a product and fulfils a "safety function" where its intended purpose, as determined by the provider (and described in the system's documentation and materials), is to prevent or mitigate risks to health and safety of persons or property. In this regard, the Guidelines provide indicative examples of in-scope and out-of-scope functions. For example, functions related to performance optimisation, service efficiency, comfort, convenience or quality control of non-safety related aspects will not be considered safety functions.

(ii) Failure or malfunctioning endangering health and safety of persons or property

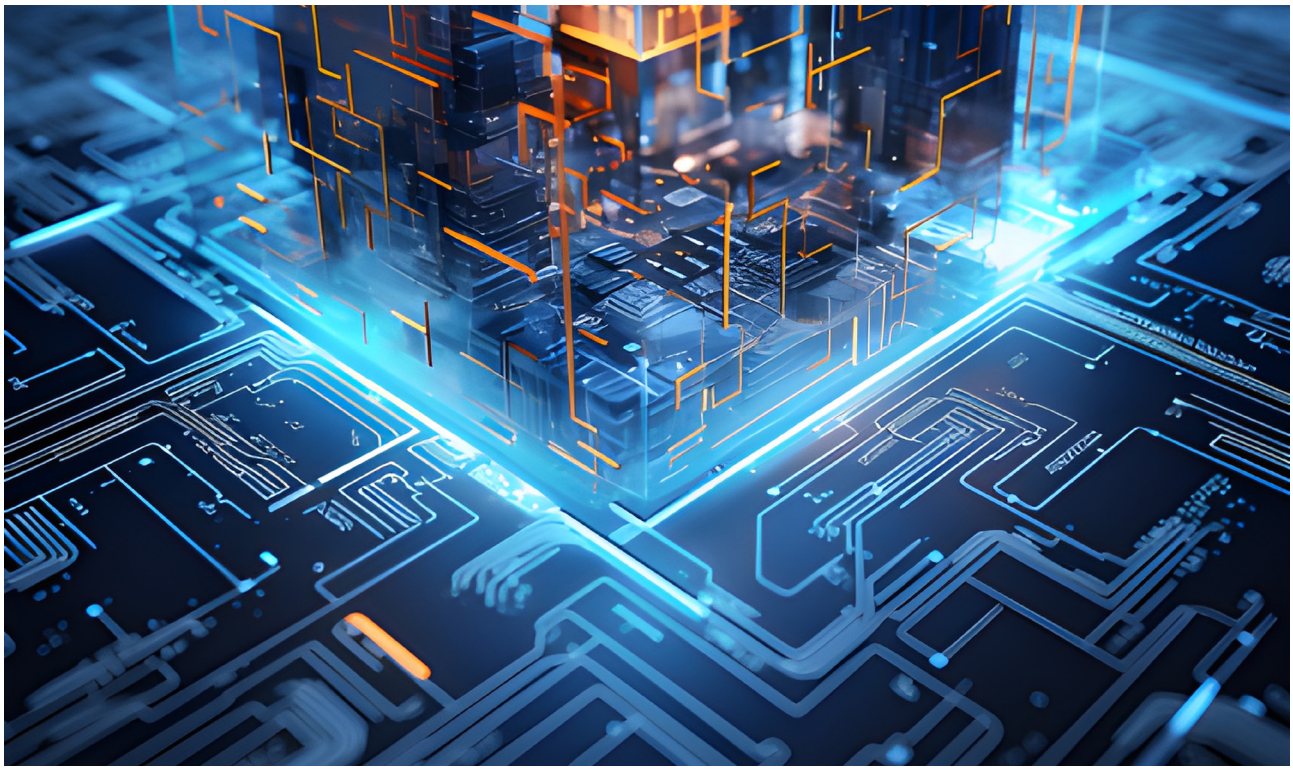
Under the second scenario, an AI system constitutes a safety component of a product where its failure or malfunctioning could endanger the health and safety of persons or property. This scenario ensures that safety relevance is assessed not only based on the intended purpose of the system, but also by reference to the hazards associated with the product and the degree of influence the AI system exercises over those hazards.

Such failure or malfunctioning can occur as a result of faults within the product itself or because of external influences. It may include incorrect outputs, loss of function or availability, timing or latency errors or misclassification that can lead to hazardous control decisions. However, the likelihood of such failure or malfunctioning must not be a mere theoretical possibility, but rather lead to endangering persons or property in the product context.

In this regard, the Guidelines provide an illustrative example of an AI system designed to optimise combustion efficiency in household gas appliances. While its intended purpose is efficiency and optimisation, its failure or malfunction may lead to carbon monoxide formation, explosion or fire, therefore qualifying it as a safety component. In contrast, if failure only resulted in discomfort, reputational harm, inconvenience or financial loss, the AI system would fall outside the high-risk classification.

Condition 2 - Third party conformity assessment

The second condition for the classification of an AI system as high-risk under Article 6(1) is that, pursuant to EU harmonised legislation listed in Annex I AI Act, the product of which the AI system forms a safety component, or the AI system itself if it is the product, must undergo a third-party conformity assessment.



The AI Act does not itself determine the applicable conformity assessment procedures for AI systems deemed high-risk pursuant to Article 6(1) AI Act. Instead, the AI Act relies on the choice of conformity assessment procedures established under the EU harmonisation legislation listed in Annex I AI Act. A conformity assessment is the process carried out by the manufacturer of demonstrating whether specified requirements relating to a product have been fulfilled.

The Guidelines highlight that, while the EU harmonisation legislation listed in Annex I may offer a choice of conformity testing options (eg, possibility to opt out of such assessment where harmonised standards have been applied under the Toys Safety Regulation), it cannot be used to determine the risk classification for the purposes of the AI Act. By way of further example, selection of Module A conformity assessment, which is intended for products of low complexity that present a low risk for public interest, will not prevent an AI system being classified as high-risk.

3. Stand-alone high-risk AI systems under Article 6(2) and Annex III AI Act

Article 6(2) AI Act classifies as high-risk certain stand-alone AI systems within eight broad areas that, in view of their intended purpose, are considered to pose a significant risk to health, safety or fundamental rights. These areas include: (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.

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 AI Act. As such, the only relevant determinant in assessing whether an AI system qualifies as high-risk under Article 6(2) AI Act is whether the intended purpose of the system includes one of the use cases listed in Annex III AI Act.

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').

Horizontal Issues for Annex III use cases

The Guidelines provide clarifications on certain horizontal aspects regarding the classification of AI systems as high-risk under Article 6(2), and Annex III.

These include the following:

- **The role of human involvement:** Human involvement has no impact on the classification of an AI system as high-risk, as it has no effect on the intended purpose of the AI system and area in which the system is used. 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 high-risk AI systems.
- **Limitations in some use cases to natural persons:** 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.
- **Complex AI systems:** Where several AI systems operate as a complex AI system (including agentic AI), so that their combined intended purpose or joint outputs materially influence an individual decision, the combined configuration is treated as a single system for the purpose of high-risk classification. The Guidelines note that this approach avoids circumvention of the high-risk classification rules, unless such complex AI systems are genuinely separable and eligible for exemption under Article 6(3) AI Act (as discussed below).
- **Intended Use:** The AI Act uses the term "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 (subject to certain exceptions). The Guidelines clarify that the meaning of "intended use" in Annex III is identical to the meaning of "intended purpose", as defined at Article 3(12) AI Act. Therefore, 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 cannot be classified as high-risk pursuant to Article 6(2) AI Act. In addition, it is not necessary for the AI system to be actually in use in a high-risk manner to gain high-risk classification. Rather the provider must assess the intended use before placing it on the EU market or putting it into service, and it is at that moment that the AI system, if it is high-risk, must be in conformity with the high-risk AI system rules.
- **"On behalf of":** 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 (ie, private entities) where a public authority outsources activities to those entities falling within those use cases. The Guidelines clarify that 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.

Filter exemption under Article 6(3) AI Act

As mentioned above, Article 6(3) AI Act provides for a 'filter mechanism', whereby AI systems falling within the scope of Article 6(2) and Annex III are exempted from being classified as high-risk where their intended use meets one of the four filter conditions listed in Article 6(3)(a)-(d). These exemptions apply on the basis that the intended use does not pose a significant risk to the health, safety or fundamental rights of natural persons. However, the Guidelines emphasise that the exemptions must be interpreted narrowly.

The filter mechanism only applies if the high-risk AI system under Article 6(2) and Annex II meets (i) one of the four filter conditions, (ii) does not perform profiling, and (iii) does not materially influence the outcome of the decision.

The four conditions / exemptions for the 'filter' under Article 6(3) AI Act to apply are set out below.

a) **The AI system is intended to perform a narrow procedural task:** The Guidelines clarify that this condition may cover AI systems intended to categorise, change the format, structure or presentation of data, or change its metadata. However, AI systems that perform a value judgement of data relevant for decision-making, such as categorisation as 'useful' or 'not useful' for human assessment, or attributing a score or ranking to input data, would not be considered to perform only a 'narrow procedural task'.

b) **The AI system is intended to improve the result of a previously completed human activity:** The Guidelines note that the fact that the human activity should be completed for this exemption to apply, means that the AI system should not replace, nor autonomously perform, the human activity. Instead, in line with Recital 53 AI Act, the AI system should provide only an additional layer to a human activity, such as verifying or refining that activity (eg, systems for quality assurance that flag errors or contradiction in human work).

c) **The AI system is intended to detect decision-making patterns or deviations:** The Guidelines note that unlike the other exemptions, which exclude AI systems from high-risk classification only if the system is restricted to procedural or preparatory tasks or improvements, this exemption allows for a more substantial role for the AI system in the assessment process. However, it is not meant to replace or influence the previously completed human assessment without proper human review. 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.

d) **The AI system is intended to perform a preparatory task:** The Guidelines note that the reference to 'preparatory' means tasks that occur prior to the actual assessment process, and the AI system must not perform any actual assessments. Recital 53 AI Act provides as examples AI systems performing preparatory tasks such as indexing, searching, processing, and linking. In contrast, where the intended purpose of the AI system is to produce a specific recommendation or evaluation, it plays a decisive role in the assessment or decision and cannot be considered preparatory.

Whether an AI system may benefit from the filter mechanism in Article 6(3) AI Act depends on a self-assessment by the provider. Providers of AI systems seeking to avail of the filter mechanism must document a self-assessment before the AI system is placed on the market and register the AI system in the EU database pursuant to Article 71 AI Act (which is intended to ensure the traceability of exempted AI systems). The assessment should consider the intended purpose of the AI system; why the system qualifies as high-risk under Article 6(2) and Annex III; a description of the conditions under Article 6(3) which apply and why; and a description of why the system does not perform profiling. The assessment should be made available upon request of a market surveillance authority.

The eight high-risk areas listed in Annex III

The Guidelines provide a comprehensive overview of each of the eight high-risk areas listed in Annex III AI Act, and break down the use cases which would be considered in or out of scope or are capable of availing of the Article 6(3) exemption. Businesses operating their AI systems within these areas should therefore consult the Guidelines to ascertain whether their system would likely be classified as high-risk based on the examples provided.

Some of the most relevant areas listed in Annex III for businesses are discussed below (excluding, in particular, law enforcement (point 6), and migration, asylum and border control (point 7)).

Biometric data (Annex III, point 1)

Annex III, point 1, AI Act lists three high-risk use cases, including (a) remote biometric identification ("**RBI**"); (b) AI systems intended for biometric categorisation (according to sensitive or protected attributes or characteristics); and (c) those intended to be used for emotion recognition.

Importantly, the AI Act defines "biometric data" differently to the GDPR. In particular, it does not include the GDPR wording "which allow or confirm the unique identification", since the AI Act 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.

(a) **RBI:** Three cumulative conditions are necessary for an AI system to be a high-risk RBI, including: (i) its purpose must be biometric identification of a natural person; (ii) without their active involvement (typically at a distance / remotely); and (iii) the system must perform a comparison between the person's biometric data and biometric data contained in a reference database.

The Guidelines note, for example, that an AI system intended to be used to compare attributes in a picture (eg, taken from the internet or CCTV) with pictures taken from the internet and indexed in a database, to identify the person in the picture without their active involvement, would be high-risk. On the other hand, however, a CCTV facial recognition system at the entrance to a stadium to detect blacklisted individuals forbidden to enter via direct access control would not be high-risk (as it is not remote, but rather requires active participation from individuals). Similarly, AI systems for smart homes, intended to be used to authenticate or verify an individual and give access to the home (such as by scanning facial images or fingerprints at the entrance) would not be high-risk (as it is not remote).

(b) **Biometric categorisation:** An AI system will be considered high-risk where it is intended to be used for biometric categorisation according to sensitive or protected characteristics based on the inference of those attributes or characteristics. The Guidelines highlight that Recital 54 AI Act clarifies that sensitive attributes or characteristics are those protected under Article 9(1) GDPR.

The Guidelines state that a practical example of an AI system falling within this category, would be an AI system used to categorise patients, to detect early symptoms of diseases that manifest themselves in mobility issues. Such an AI system captures patients' gait, infers their health data based on captured gait data, and assigns those individuals to pre-defined categories (eg, early stages, advanced stages of diseases). On the other hand, an AI system categorising customers based on their gender to offer/improve personalised advertising, by capturing and analysing keystrokes, would not fall within this category (as gender is not a sensitive or protected attribute or characteristic under Article 9(1) GDPR).

(c) **Emotion recognition:** An AI system that conducts emotion recognition (outside the prohibited practices) is 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"*. The Guidelines warn that serious concerns exist about the intrusive nature of emotion recognition systems, and the scientific basis of such systems, as the expression of emotions varies considerably across cultures and even within a single individual.

An example of an AI system falling within this high-risk category is one used for the gaming industry that is intended to measure a gaming experience (by tracking the player's body posture, facial expression etc.) to further improve the product. A further example is an AI system used in call centres to infer emotions of customers, by analysing their voices, and evaluating their vocal tone and volume to gauge customer satisfaction level. In contrast, the mere observation of readily apparent expressions, such as that a person is smiling is not emotional recognition.

Critical infrastructure (Annex III, point 2)

For an AI system to be classified as high-risk under Annex III, point 2, two conditions must be fulfilled. Firstly, the AI system must be intended to be used as a "safety component" by an entity identified by a Member State as a "critical entity" under the Critical Entities Resilience Directive. Secondly, the intended use must concern the management and operation of critical digital infrastructure, road traffic, or the supply of water, gas, heating or electricity.

The Guidelines note that the classification of an AI system as a "safety component" in critical infrastructure must be assessed primarily in light of the protective function performed by the AI system itself. As such, AI systems which are merely supportive, informational, organisational or optimisation-oriented (ie. optimise critical infrastructure's performance and operation eg efficiency, cost) and which do not themselves perform such a direct protective function do not qualify as high-risk.

The Guidelines highlight that Recital 55 AI Act makes a clear distinction between a safety component and a cybersecurity component. To fall within this high-risk category, an AI system must not be used solely for cybersecurity purposes (without a direct safety role). For example, an AI honeypot system intended to proactively identify and neutralise cyber threats on a real-time basis, or an AI system intended to support the detection of unauthorised access, are not high-risk under this category.

Education and Vocational Training (Annex III, point 3)

Annex III, point 3, AI Act sets out four high-risk AI system use cases intended to be used in the area of education and vocational training, including those:

a) determining access or admission to or assignment of individuals to institutions or programmes;

b) evaluating learning outcomes of individuals;

c) assessing the appropriate level of education a person will receive or be able to access; and

d) monitoring and detecting prohibited behaviours of students during tests.

The Guidelines highlight that AI systems in education often perform profiling of natural persons (in particular to analyse or predict a person's academic path) and may lead to automated decision-making under Article 22 GDPR, which should always be classified as high-risk, even if the system could otherwise avail of the filter mechanism under Article 6(3) AI Act.

Employment (Annex III, point 4)

Annex III, point 4, 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 AI systems used for (a) recruitment and selection (in particular to place targeted job advertisements, analyse and filter job applications, and evaluate candidates), and (b) managing work-related relationships.

(a) Recruitment & Selection

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.

The terms 'to evaluate candidates' used in point 4(a) of Annex III must also be understood broadly. 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" (eg, 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). In contrast, AI systems that merely analyse applications in a descriptive sense (classifying degrees into standard categories without applying evaluative weight) may fall outside the scope of high-risk uses as being a preparatory task.

Further high-risk examples include automated job matching or ranking tools (which could lead to a low ranking or exclusion of a certain gender or of candidates with disabilities), and AI systems which score applicant answers in a recruitment process. On the other hand, non-high-risk examples include AI systems designed to identify non-inclusive or discriminatory wording in job descriptions and AI systems that assist candidates in tailoring their CV to specific positions.

Examples of use cases which can benefit from the filter mechanism under Article 6(3) AI Act include AI systems used to verify professional accreditations, providing binary 'confirmed' or 'not confirmed' outputs, organise CVs in an internal database, automate scheduling of interviews and audit past hiring to analyse anonymised data to detect biases or inconsistencies.

(b) Managing Work-related relationships

An AI system may also classified as high-risk under Annex III, point 4(b), when used to make decisions affecting terms of work-related relationships, including the promotion or termination of work-related contractual relationships; to allocate tasks based on individual traits or behaviour; or to monitor and evaluate performance and behaviour in work-related relationships. 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.

The Guidelines explain that 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 systems, and subjecting them to the requirements and obligations provided in Chapter III AI Act.

The Guidelines provide examples of such high-risk AI systems, including a retail/logistics company that deploys an AI-enabler scheduler to assign shifts, rest periods, and on-call windows; or a ride-hailing platform that dynamically sets driver compensation based on driver acceptance rates, customer reviews and average completion times. On the other hand, a courier company that uses an AI system for tracking parcels in transit, detecting potential mistakes in labelling or distribution issues, and notifying the employee in charge of same, would not be considered high-risk. This is because the AI system's purpose is ensuring smooth workflow operations, contractual compliance and supporting workers in their tasks rather than evaluating workers' performance.

Access to and enjoyment of essential private services and essential public services (Annex III, point 5)

The Guidelines note that 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.

Eligibility for public benefits and services

Annex III, point 5(1)(a), classifies as high-risk AI systems intended to be used by public authorities or on behalf of public authorities to evaluate whether an individual is eligible for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce or revoke such benefits and services, or to prioritise allocation of such services.

The Guidelines note, for example, that an AI system intended to decide on the grant of unemployment benefits in individual cases would be considered high-risk, because it is intended to evaluate an individual's eligibility, and make a recommendation on the granting or denial of these benefits. On the other hand, an AI system intended to

proactively identify persons in need of preventative care would not be high-risk, since it only identifies persons in need of such care, and does not determine the eligibility of the identified persons. In addition, chatbots answering factual questions of a case-handler that are related to the evaluation of an application of an individual to receive healthcare benefits (such as the age of the applicant) would be exempt under the filter mechanism under Article 6(3) (a) and (d) AI Act, as such a system is intended to perform only narrow procedural tasks and preparatory tasks.

Evaluating Creditworthiness and credit scores

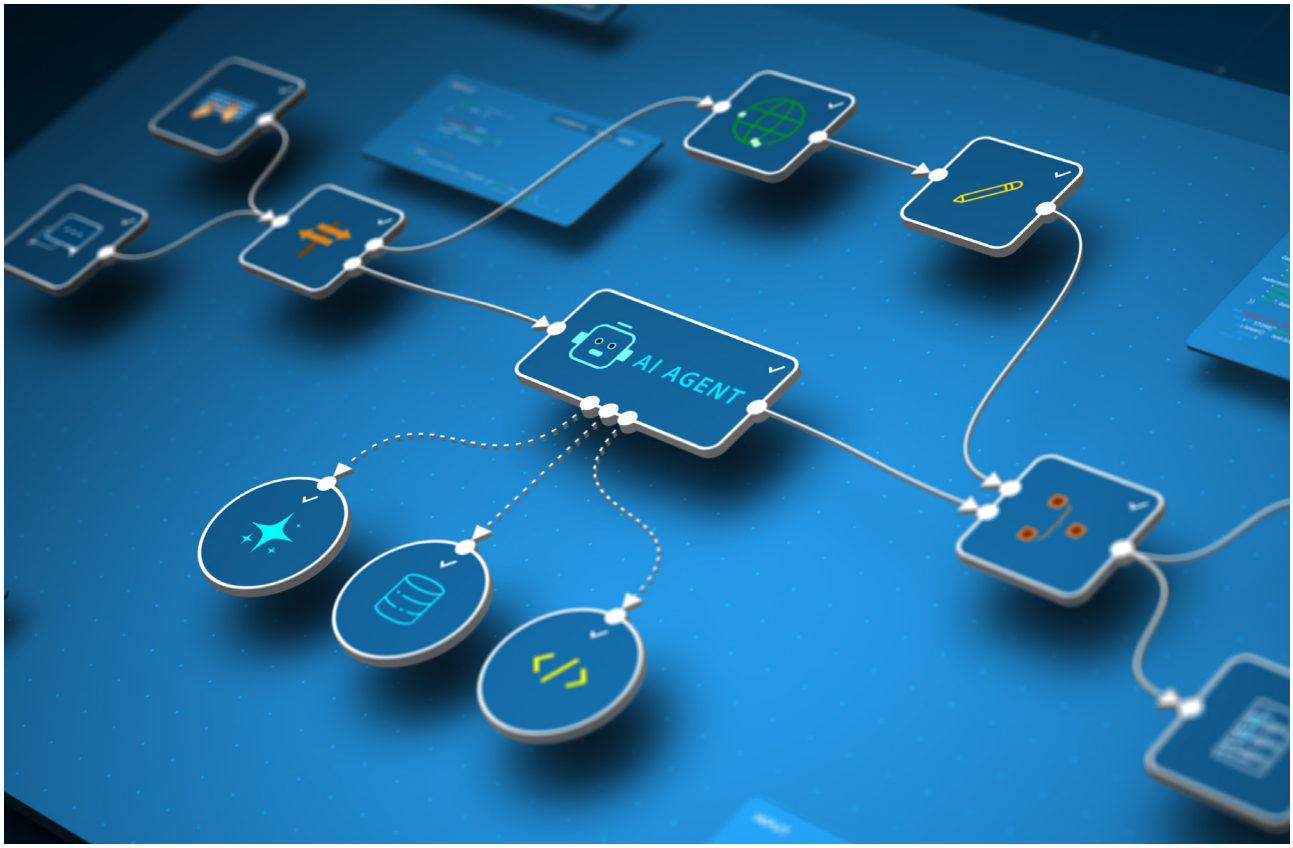
Annex III, point 5(1)(b), classifies as high-risk, AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score. Point 5(b) AI Act covers AI systems intended to be used for two distinct use cases: (i) the evaluation of creditworthiness and (ii) the establishment of a credit score. However, 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.

The Guidelines note that "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. Whilst the "establishment of a credit score" refers to the creation and building of a representation of a natural person's creditworthiness.

For example, credit scoring for consumer lending and mortgages is high-risk, whilst AI systems intended for customer support before or after a credit decision are not high-risk, as they do not assess the creditworthiness or establish a credit score of a natural person.

Risk assessment and pricing for life and health insurance

Point 5(c) of Annex III classifies as high-risk AI systems intended to be used for risk assessment and pricing in relation to individuals for health and life insurance. For example, AI systems used by an insurer to review applications for life insurance (so long as it qualifies as a risk assessment) are high-risk. However, AI systems used for claims management are not considered high-risk. This is because these systems are intended to verify whether a claim is valid under the policy terms or to determine the amount to be paid.



Administration of justice and democratic processes (Annex III, point 8)

Annex III, point 8, 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.

In particular, point 8(a) of Annex III 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.

The Guidelines note, for example, that judicial decision drafting systems are high-risk under point 8(a) of Annex III, since they are 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. However, 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, is not high-risk under point 8(a) of Annex III. In addition, AI systems intended to be used as advanced search engines, to retrieve case-law, or create case-summaries of published decisions, perform keyword searches, are generally not high-risk. However, beyond retrieval, an AI system that also assigns a meaning, resolves an ambiguity, or draws legal conclusions from the retrieved sources (eg, identifying relevant legal aspects or summarising text), is likely to be classified as high-risk.

Next Steps

The public consultation remains open until **23 June 2026** and stakeholders can submit their contributions here.

Given the onerous nature of high-risk obligations under the AI Act, it is crucial that providers and deployers of AI systems take steps to assess them in line with the Guidelines (albeit noting they are still in draft form) to determine whether they qualify as high-risk. To the extent that the filter exemption in Article 6(3) AI Act is relied on to avoid a high-risk AI system classification, organisations should ensure that their technical documentation and other related legal, product and materials accurately and consistently reflect the intended purpose of the system.

Contact Us

Matheson's Technology and Innovation Group are available to guide you through compliance with the AI Act. For more information, please contact any member of our Technology and Innovation Group or your usual Matheson contact.

Marie McGinley
Partner,
Head of Technology
and Innovation Group
Dublin
T +353 1 232 3722
E marie.mcginley@matheson.com

Davinia Brennan
Partner,
Technology and Innovation Group
Dublin
T +353 1 232 2700
E davinia.brennan@matheson.com

Sarah Jayne Hanna
Partner,
Technology and Innovation Group
Dublin
T +353 1 232 2865
E sarahjayne.hanna@matheson.com

Matheson

DUBLIN
70 Sir John Rogerson's Quay,
Dublin 2
Ireland

T: +353 1 232 2000
E: dublin@matheson.com

CORK
Penrose One,
Penrose Dock,
Cork, T23KW81
Ireland

T: +353 21 465 8200
E: cork@matheson.com

LONDON
7th Floor, Octagon Point,
5 Cheapside,
London EC2V 6AA,
UK

T: +44 20 7614 5670
E: london@matheson.com

NEW YORK
250 Park Avenue
New York,
NY 10177
United States

T: +1 646 354 6582
E: newyork@matheson.com

PALO ALTO
228 Hamilton Avenue,
3rd Floor,
Palo Alto, CA 94301
United States

T: +1 650 617 3351
E: paloalto@matheson.com

SAN FRANCISCO
95 Third Street
San Francisco
CA 94103
United States

T: +1 415 423 0540
E: sf@matheson.com