DEBRIEFING

REGULATION ON ARTIFICIAL INTELLIGENCE (AI Act)

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)

Berlin, 08.08.2024

Law / Legal Act: 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)
Publication Date: 12.07.2024
Entry into force: 01.08.2024
Reference: REGULATION (EU) 2024/1689
Applies to: Developers, importers, distributors and operators of AI systems and models.
Content: The Regulation sets out a comprehensive framework for dealing with artificial intelligence. It addresses both the development of AI models and systems and their use.

What does the Regulation govern?

The AI Regulation provides the EU with a comprehensive legal framework for the use and development of artificial intelligence. The Regulation follows a risk-based approach, which means that the requirements for an application are stricter depending on an assessment of the associated risk. To this end, the Regulation defines different risk groups for AI systems. Applications that pose an unacceptable risk are prohibited by the Regulation. The AI Regulation also contains provisions for general-purpose AI models. In addition, a framework for regulatory sandboxes shall be established, particularly to support SMEs in testing their AI systems.

What needs to be considered?

I. General provisions for AI systems

The provisions listed under Section 1 apply to providers who place AI systems on the market or put them into operation in the Union, as well as to deployers, manufacturers or importers of AI systems.

1. Subject matter and scope of application

a. In accordance with Article 1 (1), the purpose of the Regulation is to improve the functioning of the internal market and to promote the uptake of human centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety and fundamental rights, including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation.
b. In accordance with Article 2, the Regulation applies to providers of AI systems and AI models as well as deployers, importers and distributors of AI systems. It also applies to product manufacturers placing on the market or putting into service AI systems, together with their product and under their own name or trademark, as well as authorised representatives of providers, which are not established in the Union, and affected persons that are located in the Union.
c. **The Regulation does not apply to AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes. It also does not apply to systems developed and put into service for the sole purpose of scientific research and development.**
d. **In accordance with Article 2 (12), the Regulation does not apply to AI systems released under free and open-source licences,** unless they are placed on the market or put into service as high-risk AI systems or as an AI system that falls under Article 5 or Article 50.

2. General requirements for AI systems

a. In accordance with Article 50 (1), AI systems intended to interact directly with natural persons must be designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious to the person due to the situation.
b. In accordance with Article 50 (2), the output of generative AI systems shall be marked in a machine-readable format and shall be detectable as artificially generated or manipulated (watermarking). The same applies in accordance with Article 50 (4) to deployers of systems that generate or manipulate image, audio or video content constituting a deep fake. Exceptions are provided for in the area of law enforcement.
c. Deployers of an emotion recognition system or a biometric categorisation system shall also inform the natural persons exposed thereto of the operation of the system, and shall process the personal

data in accordance with Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680. Exceptions apply in accordance with Article 50 (3) for the area of law enforcement.

II. Provisions for AI systems with high-risk

The provisions listed under Section II apply to deployers, providers, distributors and importers of high-risk AI systems.

1. Classification rules in accordance with Article 6

a. AI systems shall be considered to be high-risk where both of the following conditions are fulfilled:
   i. The AI system is intended to be used as a safety component of a product, or the AI system is itself such a product, covered by Union harmonisation legislation listed in Annex I;
   ii. The product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonisation legislation listed in Annex I.

b. In addition, AI systems referred to in Annex III shall be considered to be high-risk.

c. In accordance with Article 6 (3), by way of derogation, an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making. In accordance with Article 6 (3d), systems that perform "profiling" of natural persons shall always be considered to be high-risk.

d. The Commission shall, after consulting the European Panel on Artificial Intelligence Board (the "Board"), and **no later than 2 February 2026**, provide guidelines specifying the practical implementation of Article 6 in line with Article 96, together with a comprehensive list of practical examples of use cases of AI systems that are high-risk and not high-risk.

2. Requirements for the risk management system

a. In accordance with Article 9, the establishment of a risk management system is mandatory for high-risk AI systems. This shall be documented, maintained and systematically reviewed and updated on a regular basis throughout the entire lifecycle of the system. Among others, it includes the following aspects:
   i. The identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when used in accordance with its intended purpose;
   ii. The estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its

intended purpose or in the context of reasonably foreseeable misuse;

iii. The evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72;

iv. The adoption of appropriate and targeted risk management measures designed to address the risks identified.

b. In accordance with Article 6 (5), the identification of specific risks shall be eliminated or reduced as far as technically possible.

3. Data governance requirements in accordance with Article 10

a. In accordance with Article 10, high-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets. These shall fulfil the requirements of Article 10 (2).

b. In addition, the data shall be relevant, sufficiently representative and, to the best extent possible, free of errors and complete in view of the intended purpose.

c. In accordance with Article 10 (5), personal data may be processed exceptionally to correct distortions.

4. Documentation und transparency

a. In accordance with Article 11, compliance with the requirements for high-risk AI systems shall be documented. This documentation shall contain, at a minimum, the elements set out in Annex IV.

b. SMEs, including start-ups, may provide the elements of the technical documentation specified in Annex IV in a simplified manner. To that end, the Commission shall establish a simplified technical documentation form.

c. As described in Article 12, high-risk AI systems shall technically allow for the automatic recording of events over the lifetime of the system.

d. In accordance with Article 13, high-risk AI systems shall be designed and developed in such a way to ensure their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately.

5. Requirements of human oversight

a. High-risk AI systems shall be designed and developed in such a way that they can be effectively overseen by natural persons during the period in which they are in use.

b. The oversight measures shall be commensurate with the risks, level of autonomy and context of use of the high-risk AI system, and shall comply with the requirements of Article 14.

c. In accordance with Article 14 (5), for remote biometric identification systems, additional human oversight measures shall apply.

6. Cybersecurity

a. The cybersecurity requirements for high-risk AI systems are set out in Article 15, which requires high-risk AI systems to be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle.

7. Obligations of providers of high-risk systems

a. In accordance with Article 16, providers of high-risk AI systems shall ensure that their high-risk AI systems are compliant with the requirements set out in Chapter III, Section 2.
b. Providers of high-risk AI systems are obliged by Article 17 to have a quality management system in place. This shall be documented and cover the aspects specified in Article 17. In accordance with Article 18, the documentation shall be kept for ten years after the high-risk AI system has been placed on the market or put into service.
c. Under Article 21, providers of high-risk AI systems shall, upon a reasoned request by a competent authority, provide that authority with all of the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the relevant requirements.
d. Article 72 requires providers to establish and document a post-market monitoring system in a manner that is proportionate to the nature of the AI technologies and the risks of the high-risk AI system.
e. In accordance with Article 22, prior to making their high-risk AI system available on the Union market, providers established in third countries shall, by written mandate, appoint an authorised representative which is established in the Union.
f. In accordance with Article 23, importers of high-risk AI systems shall assess and ensure compliance with the provisions of the Regulation.
g. In accordance with Article 25, where a significant change is made to a high-risk AI system by any distributor, importer, deployer or other third-party, they shall be considered to be a provider of the system.
h. In accordance with Article 49, the Commission shall, in cooperation with the Member States, establish and maintain an EU database of high-risk AI systems in accordance with Article 71, in which such systems shall be registered.

8. Obligations of deployers of high-risk AI systems

a. In accordance with Article 26, deployers of high-risk AI systems shall ensure that they use such systems in accordance with the instructions for use accompanying the systems. They shall also assign human oversight to natural persons who have the necessary competence, training and authority.
b. In accordance with Article 26 (7), before putting into service or using a high-risk AI system at the workplace, deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system.

c. In accordance with Article 6 (2), prior to deploying a high-risk AI system into service – except for high-risk AI systems used in the area listed in Annex III paragraph 2 – deployers that are bodies governed by public law, or are private entities providing public services, shall perform an assessment of the impact on fundamental rights that the use of such system may produce. This assessment of the impact on fundamental rights shall perform the assessments mentioned in Article 27.
d. If the high-risk AI system is a system for post-remote biometric identification for law enforcement purposes, the deployers are subject to the additional requirements in Article 26 (10).

9. **The provisions on high-risk AI systems shall apply to the systems listed in Annex III from 2 August 2026 and to the systems listed in Annex II from 2 August 2027.**

III. Prohibited AI practices in accordance with Article 5

The provisions listed under Section III concern deployers and providers of certain AI systems that can be used for the use cases listed in Article 5. The use cases listed in the following paragraph are prohibited by the AI Act.

1. Manipulation

a. In accordance with Article 5 (1), the following AI practices shall be prohibited: the placing on the market, the putting into service and the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting the behaviour of a person or a group of persons, in addition to systems that exploit any of the vulnerabilities of a natural person or a specific group of persons (such as due to disability or age).

2. Social Scoring

a. In accordance with Article 5 (1c), the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age shall be prohibited if this results in detrimental or unfavourable treatment of certain natural persons or groups. This applies in cases where the data used is not relevant to the intended use.

3. Emotion recognition

a. In accordance with Article 5 (1f), the placing on the market and putting into service of AI systems for the purpose of inferring the emotions of a natural person in the areas of workplace and education institutions shall be prohibited, except where the use of the AI system is intended to be put in place for medical or safety reasons.

4. Profiling and categorisation

a. Article 5 (1d) prohibits systems whose purpose is to make risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics. There are exceptions for criminal activities that are already based on objective and verifiable facts. Article 5 (1g) also prohibits 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.

5. 'Real-time' remote biometric identification systems in public spaces

a. In accordance with Article 5 (1h), the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is generally prohibited. However, this prohibition does not apply in connection with the search of missing persons, the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or genuine and foreseeable threat of a terrorist attack. There are also exceptions for the localisation or identification of a person suspected of having committed a criminal offence, provided that the offence is punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

b. In accordance with Article 27, the use of 'real-time' remote biometric identification systems in publicly accessible spaces shall only be authorised if the law enforcement authorities have completed a fundamental rights impact assessment. This may be waived in urgent cases. In addition, Article 5 (3) requires the consent of the competent judicial authority or an independent administrative authority.

c. Member States are authorised by Article 5 (5) to adopt stricter legislation for the use of remote biometric identification systems in accordance with Union law.

6. **The provisions on prohibited practices will apply from 2 February 2025.**

IV. Provisions for general-purpose AI models

The provisions listed under Section IV apply to providers and users of general-purpose AI models.

1. General provisions

a. In accordance with Article 53 (1a), providers of general-purpose AI models shall draw up technical documentation containing at least the information set out in Annex XI for the purpose of providing it, upon request, to the AI Office and the national competent authorities. Providers of AI system who intend to integrate the general-purpose AI

model into their AI systems shall be provided with at least the elements set out in Annex XII.

b. Providers are required under Article 53 (1c) to put in place a policy to comply with Union law on copyright and related rights and, in particular, to identify and comply with a reservation of rights expressed in accordance with Article 4 (3) of Directive (EU) 2019/790, including through state-of-the-art technologies.
c. In accordance with Article 53 (2), the obligations shall not apply to providers of AI models that are released under a free and open-source licence that allows for the access, usage, modification and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available. This exception shall not apply to general-purpose AI models with systemic risks.

2. Classification rules for models with systemic risk
a. In accordance with Article 51, a general-purpose AI model shall be classified as an AI model with systemic risk if it:
    i. Can be considered as high impact models on the basis of appropriate tools, indicators and benchmarks. This applies, for example, when, based on a decision made by the Commission, *ex officio* or following a qualified alert from the scientific panel, such capabilities are determined considering the criteria set out in Annex XIII.
    ii. In addition, in accordance with Article 51 (2), high level impact capabilities shall be presumed to exist when the cumulative amount of computation used for its training measured in floating point operations (FLOPs) is greater than 10^{25}. This value can be adjusted by the Commission and supplemented with additional criteria.

3. Provisions for AI models with systemic risk
a. Providers of models with systemic risk are obliged by Article 55 to identify and mitigate potential systemic risks. In addition, information on serious incidents and possible corrective measures shall be recorded. Furthermore, an appropriate level of cybersecurity shall be ensured for these AI models.
b. Providers of general-purpose AI models with systemic risk may rely on codes of practice within the meaning of Article 56 to demonstrate compliance with the obligations set out in Article 55 (1), until a harmonized publication is published.

4. **The provisions on general-purpose AI models are applicable from 2 August 2025.**

V. Innovation

Under Section V, provisions apply to providers of AI systems and models.

1. Regulatory sandboxes

a. In accordance with Article 57 (1), Member States shall ensure that their competent authorities establish at least one AI regulatory sandbox at national level, which shall be operational by 2 August 2026. The established AI sandboxes shall provide for a controlled environment that facilitates the development, training, testing and validation of AI systems for a limited time before their being placed on the market or put into service. Competent authorities designated by the Member States shall provide, as appropriate, guidance, supervision and support within the AI regulatory sandbox.

b. In accordance with Article 57 (7), the competent authority shall, upon request of the AI system provider, provide the AI system provider with a written proof of the activities successfully carried out in the regulatory sandbox. Providers may use such documentation to demonstrate their compliance with this Regulation through the conformity assessment process or relevant market surveillance activities. In this regard, the exit reports and the written proof shall be taken positively into account by market surveillance authorities and notified bodies, with a view to accelerating conformity assessment procedures to a reasonable extent.

VI. Governance and enforcement

1. Supervisory structure

a. In accordance with Article 64, the EU Commission shall establish an Artificial Intelligence Office (AI Office). In accordance with Article 88, the AI Office shall be responsible for enforcing the provisions on general-purpose AI models.

b. In accordance with Article 65, the Commission shall establish an AI Board. The Board shall be composed of one representative per Member State and shall, inter alia, ensure consistent and effective application of the Regulation.

c. In accordance with Article 67, the Commission shall establish an advisory forum to provide technical expertise and advise the AI Board and the Commission. The Advisory forum shall represent a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society and academia, and shall be appointed by the Commission.

d. In accordance with Article 68, the Commission shall establish a scientific panel of independent experts. It shall contribute to the development of tools and methodologies for evaluating capabilities of general-purpose AI models and systems, including benchmarks, and provide advice on the AI Office about models with systemic risks.

e. In accordance with Article 70, Member States shall establish or designate as national competent authorities at least one market surveillance authority. In particular, Member States shall be responsible for enforcing the provisions on high-risk AI systems.

2. Penalties

a. In accordance with Article 99, Member States shall lay down the rules on penalties.
   i. Non-compliance with the prohibition of the AI practices referred to in Article 5 shall be subject to administrative fines of up to EUR 35,000,000 or, if the offender is an undertaking, up to 7% of its total worldwide annual turnover for the preceding financial year.
   ii. Regarding non-compliance with the obligations for providers, deployers, importers or distributors related to high-risk AI systems or the prescribed transparency requirements, there shall be fines of up to EUR 15,000,000 or, if the offender is an undertaking, up to 3% of the total worldwide annual turnover of the preceding financial year.
   iii. The supply of incorrect, incomplete, or misleading information to notified bodies or competent national authorities in reply to a request shall be subject to administrative fines of up to EUR 7,500,000 or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year.
   iv. In accordance with Article 99 (7), the lower amount applies to SMEs and start-ups.
b. In accordance with Article 101, the Commission may impose fines on providers of general-purpose AI models, not exceeding 3% of their annual total worldwide turnover in the preceding financial year or EUR 15,000,000.

3. Timeframes

a. In accordance with Article 113, the Regulation shall apply in principle from 2 August 2026. This also applies to the provisions on high-risk AI systems in accordance with Annex III.
b. Article 5 on prohibited practices shall already apply from 2 February 2025.
c. The provisions on general-purpose AI models shall apply from 2 August 2025. Until then, Member States must also define their national supervisory structure for enforcement.
d. The provisions for high-risk AI systems listed in Annex I shall apply from 2 August 2027.
