FIVERS

The EU Regulation 2024/1689 on Artificial Intelligence - FAQs

MEMORANDUM

SUMMARY

When has the EU Regulation on Artificial Intelligence been published?

The 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) has been published in the Official Journal of the European Union on 12nd July 2024.

The Regulation 2024/1689 is the world's first comprehensive law on AI and aims to address risks to health, safety, and fundamental rights. In addition, it protects democracy, the rule of law and the environment.

When shall the EU Regulation 2024/1689 (AI Act) come into force?

The Regulation 2024/1689 shall enter into force on 1st August 2024.

When will the provisions and obligations of the Regulation 2024/1689 (AI Act) be materially applicable?

The Regulation 2024/1689 will only be applicable from 2nd August 2026. However, some rules will apply after 6 or 12 months.

The following will be applicable from 2nd February 2025:

(a) Articles 1 to 4, relating to the subject matter, scope, definitions (supply contracts may therefore use technical and legal definitions of the AI Act) and AI literacy obligations (obligation for suppliers and developers to have trained and competent personnel, who may find specific entry into contracts with suppliers).
(b) Article 5 on prohibited AI practices (particular attention will have to be paid – for example – to advanced profiling using biometrics, especially in the workplace, to check the applicability of the ban).

After 12 months (from 2nd August 2025) the following will apply:

(a) the rules on the penalty system (with penalties of up to €35 million or 7% of annual global turnover; the penalty for providers of AI models for general purposes – up to €15 million or up to 3% of turnover – will apply after 24 months);
(b) the rules on General Purposes AI models (GPAI) (from which relevant compliance and contractual issues arise, considering that companies already use on a daily basis solutions – such as Chat-GPT and generative AI – integrated into devices/services);
(c) the rules on notified bodies and on the related notification procedures;
(d) Article 78 *("Confidentiality*");
(e) the rules establishing the EU database on high-risk AI systems.

Finally, the applicability of the rules on "high-risk" AI systems, as well as the related obligations, is postponed to 2nd August 2027 .

To whom shall the Regulation 2024/1689 apply?

The Regulation 2024/1689 shall apply to public and private entities, inside and outside the EU, provided that an AI system is placed on the EU market or that its use affects persons located in the EU.

The rules will bind both providers/developers of AI systems (e.g. a developer of a CV screening tool) and professional end-users (called "*deployers*") of high-risk AI systems (e.g. a company that purchases the aforementioned screening tool).

The Regulation 2024/1689 will also apply to the entire commercial chain (importers, distributors, manufacturers of products who place an AI system on the market or put into service together with their product and with their name or brand, etc.): importers of AI systems in the EU will have to ensure, for example, that the non-EU supplier has already performed the appropriate conformity assessment procedure and that the AI system bears a European conformity (EC) and is accompanied by the required documentation and instructions for use.

There are also specific obligations for providers of general-purpose AI models (GPAIs) including large generative AI models (LLM systems – *Large Language Models,* such as Chat-GPT, Copilot, Gemini, etc.).

Providers of free and open-source models are exempt from most of these obligations. However, this exemption does not cover obligations applicable to providers of GPAI general purpose AI models that involve systemic risks.

Regulation 2024/1689 shall not apply to research, development and prototyping activities prior to placing on the market and to AI systems developed for military, defence or national security purposes, regardless of the type of entity carrying out such activities.

In what sense does Regulation 2024/1689 regulate Artificial Intelligence based on the type of risk (risk-based approach)?

The Regulation 2024/1689 employs a risk-based approach, according to four levels of risk for AI systems, and to the identification of specific risks for GPAI models:

1) Unacceptable: A set of particularly harmful uses of AI (so-called 'artificial intelligence practices') that contravene EU values since they breach fundamental rights shall be forbidden, such the following:

- attribution to people of a social score (*social credit scoring*) for public and private purposes;

- exploitation of people's vulnerabilities, use of subliminal techniques;
- real-time remote biometric identification in publicly accessible spaces by public authorities competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, subject to limited exceptions in the case of serious crimes;
- biometric categorisation of natural persons on the basis of biometric data to infer or infer their race, political opinions, trade union membership, religious or philosophical beliefs or sexual orientation; it will still be possible to filter datasets based on biometric data in the area of law enforcement;
- predictive police affecting individuals;
- recognition of emotions in the workplace and in educational institutions, except for medical or safety reasons (e.g. monitoring a pilot's fatigue levels);
- Non-targeted extraction of facial images from the Internet or CCTV cameras for the creation or expansion of databases (so-called online *scraping*).

2) High risk: a limited number of AI systems identified in Article 6 and listed in Annex III of Regulation 2024/1689 that have the potential to have a negative impact on people's safety or their fundamental rights are considered to be high risk. Such systems shall also include product safety components covered by sectoral Union legislation, which will always be considered to be high-risk if subject to a third-party conformity assessment under that sectoral legislation;

3) Limited Risk: These refer to AI systems that must meet specific transparency obligations. For instance, individuals interacting with a chatbot must be informed that they are engaging with a machine so they can decide whether to proceed (or request to speak with a human instead).

4) Minimal risk: These applications are already widely deployed and make up most of the AI systems we interact with today. Examples include spam filters, AI-enabled video games and inventory-management systems. No obligations are specifically provided.

* * * * * * * *

In addition, Regulation 2024/1689 takes into account systemic risks that could arise from GPAI models, including LLM AI models that can be used for a wide range of tasks and are becoming the basis of many AI systems in the EU. Some of these models could pose systemic risks if they are particularly effective or widely used. Powerful models could, for example, cause major incidents or be misused for large-scale cyberattacks.

What criteria are employed by the Regulation 2024/1689 to classify an AI system as "high risk"?

Together with a clear definition of what is meant by "high-risk", the Regulation 2024/1689 establishes a robust methodology that helps to identify high-risk AI systems within the legal framework. The aim is to ensure legal certainty for businesses and other operators.

The first criterion is set out in Article 6 of the Regulation: an AI system shall be considered to be high-risk where both of the following conditions are fulfilled:

(a) the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonisation legislation listed in Annex I of the Regulation;

(b) the product whose safety component pursuant to point (a) 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 of the Regulation.

In addition to the high-risk AI systems referred to in above, AI systems referred to in Annex III of the Regulation shall be considered to be high-risk, specifically:

1) Biometrics, in so far as their use is permitted under relevant Union or national law:

2) Critical infrastructure: AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity.

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 (relevant for banks and insurance companies, amongst the others).

6) Law enforcement, in so far as their use is permitted under relevant Union or national law.

7) Migration, asylum and border control management, in so far as their use is permitted under relevant Union or national law.

8) Administration of justice and democratic processes.

AI systems intended to perform a narrow procedural task, or to improve the result of a previously completed human activity, which are not meant to replace or influence the previously completed human assessment or intended to perform a preparatory task <u>are not considered to be high-risk – even if they fall under the Annex III list just provided above</u>.

Furthermore, very large online platform recommendation systems are not included among high-risk AI systems as they are already regulated by other legislation, such as the two Regulations on digital services (EU Regulation 2022/2065) and on digital markets (EU Regulation 2022/1925).

Finally, it is worth reminding that an AI system is always considered to be at high risk if it performs the profiling of natural persons.

What are the obligations for providers of high-risk AI systems?

Before placing a high-risk AI system on the EU market, or putting it into service, providers must subject it to a conformity assessment**.** They will thus be able to demonstrate that their system complies with the mandatory requirements for trustworthy AI (e.g. data quality, documentation and traceability, transparency, human oversight, accuracy, cybersecurity and robustness). This assessment must be repeated in the event of a material change in the system or its purpose.

AI systems that constitute safety components of products covered by sector-specific Union legislation will always be considered high-risk if they are subject to a third-party conformity assessment under that sector-specific legislation. A third-party conformity assessment is also always required for biometric systems.

Providers of high-risk AI systems will also need to implement quality and risk management systems to ensure compliance with the new requirements and minimise risks to users and affected persons, even after a product has been placed on the market.

High-risk AI systems deployed by public authorities or entities acting on their behalf will have to be registered in a public EU database, unless such systems are used for law enforcement and immigration control activities. The latter systems will have to be registered in a non-public part of the database, which will be accessible only to the competent supervisory authorities.

Market surveillance authorities will contribute to post-market monitoring through audits and by providing suppliers with the possibility to report incidents or serious breaches of fundamental rights obligations of which they have become aware. Any market surveillance authority may authorise the placing on the market of a specific high-risk AI for exceptional reasons.

In the event of a breach, the requirements will allow national authorities to have access to the information necessary to investigate whether the use of the AI system complies with the law.

Are end-users of high-risk AI systems – such as, for example, a company purchasing said systems from a supplier – subject to obligations?

Yes. Article 26 of Regulation 2024/1689 introduces significant technical, organisational, documentary and managerial obligations for the "*deployer*" (i.e.: "*a natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a non-professional personal activity*").

End users must:

(1) take appropriate technical and organisational measures to ensure that high-risk AI systems are used in accordance with the instructions for use accompanying the systems;
(2) entrust human oversight of the operation of high-risk AI systems to natural persons who have the necessary expertise, training, authority and support;
(3) trace and keep logs automatically generated by the high-risk AI system, to the extent that those logs are under their control, for at least six months;
(4) inform the employees' representatives – in accordance with relevant trade union procedures – and interested employees that they will be subject to the use of the high-risk AI system, before putting into service or using a high-risk AI system in the workplace;
(5) to the extent that they exercise control over the input data, ensure that such input data is relevant and sufficiently representative in light of the intended purpose of the high-risk AI system;
(6) monitor the operation of high-risk AI systems, providing for technical procedures for suspension or interruption in the event of indices;
(7) notify the supplier, distributor and market surveillance authorities of major IT incidents;
(8) carry out the impact assessment of personal data pursuant to Article 35 of the EU General Data Protection Regulation – GDPR no. 679/2016 (also making use of the specific information on the high-risk AI system referred to in Article 13 of the Regulation 2024/1689);
(9) inform data subjects if high-risk AI systems listed in Annex III are used that take decisions or assist in the taking of decisions affecting natural persons;
(10) carry out the impact assessment on fundamental rights and freedoms referred to in Article 27 of Regulation 2024/1689, but only if the user is a public entity or a private individual using AI systems to assess the creditworthiness of natural persons or to establish their creditworthiness (with the exception of AI systems used for the purpose of detecting financial fraud) or to assess risks and determine prices in in relation to natural persons in the case of life insurance and health insurance.

How are General Purposes AI models regulated?

GPAI models, including LLM models (e.g., CHAT-GPT), can be used for various tasks. Individual models can be integrated into a large number of AI systems. It is important that a provider that intends to rely on a GPAI model has all the necessary information to ensure that its system is secure and compliant with the AI Act.

The Regulation 2024/1689 consequently forces providers of GPAI models to make available certain information to downstream system providers. Such transparency makes it possible to better understand these models.

It is also necessary for GPAI model providers to have policies in place to ensure copyright enforcement during the machine learning of their models.

Some of these models may also pose systemic risks as they are particularly effective or widely used.

For the time being, the EU legislator considers that GPAI models that have been trained using a total computing power of more than 10^25 FLOPS pose systemic risks, given that models trained with a higher computing power tend to be more powerful. The AI Office (established within the Commission and already operational) may update this threshold in light of technological developments and may also, in specific cases, designate other GPAI models as such on the basis of additional criteria (e.g. the number of users or the degree of autonomy of the model).

Providers of GPAI models posing systemic risks are therefore required to assess and mitigate risks, report major incidents, conduct state-of-the-art model testing and evaluation, ensure cybersecurity and provide information on the energy consumption of their models.

To this end, they are invited to work with the European AI Office to develop codes of conduct that are a central tool for specifying standards in cooperation with other experts. A Panel will play a central role in supervising AI models for general purposes.

How is biometric identification regulated by the Regulation 2024/1689?

The use of real-time remote biometric identification in publicly accessible spaces (i.e. facial recognition using CCTV cameras) for law enforcement purposes is prohibited, unless it is used in one of the following cases:

- law enforcement activities relating to 16 specific crimes;
- targeted search for specific victims, abduction, trafficking and sexual exploitation of human beings and missing persons;
- prevention of threats to the life or physical integrity of persons or response to a current or foreseeable threat of terrorist attack.

The list of 16 offences contains:

- terrorism;
- trafficking in human beings;
- sexual exploitation of children and child sexual abuse material,
- illicit trafficking in narcotic drugs and psychotropic substances,
- illicit trafficking in arms, ammunition and explosives,
- voluntary homicide;
- serious bodily injury;
- illicit trafficking in human organs and tissues;
- illicit trafficking in nuclear and radioactive materials,
- kidnapping, kidnapping and hostage-taking;
- offences falling within the jurisdiction of the International Criminal Court,
- hijacking of an aircraft/ship;
- rape;
- Environmental crimes:

- organized theft or armed robbery;
- Sabotage, participation in a criminal organization involved in one or more of the crimes listed above.

Real-time remote biometric identification by law enforcement authorities is subject to prior authorisation by an independent judicial or administrative authority, whose decision is binding. In case of urgency, the authorization can be issued within 24 hours; If permission is not granted, all data and outputs must be suppressed.

The authorisation must be preceded by a prior fundamental rights impact assessment and must be notified to the market surveillance authority and the data protection authority concerned. In urgent situations, you can start using the system without registration.

The use of AI systems for remote biometric identification (identification of persons in previously collected video material) of persons under investigation requires prior authorisation from a judicial authority or an independent administrative authority and notification to the data protection authority and the market surveillance authority.

What is a fundamental rights impact assessment? Who must carry out this assessment? When should it be carried out?

The use of a high-risk AI system can have an impact on fundamental rights. Therefore:

1. deployers that are bodies governed by public law;
2. private entities providing public services;
3. deployers of high-risk AI system to assess the creditworthiness of natural persons or to establish their creditworthiness (with the exception of AI systems used for the purpose of detecting financial fraud) or to assess risks and determine prices in relation to natural persons in the case of life insurance and health insurance;

must carry out an assessment of the impact on fundamental rights and shall communicate the results to the national authority.

The assessment shall consist of:

a) a description of the deployer’s processes in which the high-risk AI system will be used in line with its intended purpose;
b) a description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used;
c) the categories of natural persons and groups likely to be affected by its use in the specific context;
d) the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information given by the provider pursuant to Article 13 of the Regulation;

e) a description of the implementation of human oversight measures, according to the instructions for use;
f) the measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.

If the entity required has already fulfilled the obligation through the personal data protection impact assessment under Article 35 of the GDPR, the fundamental rights impact assessment must be carried out in conjunction with this data protection impact assessment.

What governance system at European and national level is introduced by Regulation 2024/1689?

Member States play a key role in enforcing the Regulation and ensuring that it is enforced. In this regard, each Member State must designate one or more national competent authorities to supervise its application and implementation, as well as to carry out market surveillance activities.

To increase efficiency and establish an official point of contact with the public and other counterparts, each Member State must designate a national supervisory authority, which will also represent the country in the European Artificial Intelligence Board.

Additional technical expertise will be provided by an advisory forum where a balanced selection of stakeholders is represented, including industry, start-ups, SMEs, civil society and academia.

The Commission has also already set up and put into operation the new European AI Office, within the Commission, which oversees AI models for general purposes, cooperates with the European Board for Artificial Intelligence and will be supported by a panel of independent scientific experts.

What are the penalties in the event breach of the Regulation 2024/1689?

For AI systems that are placed on the market or put into service and that do not comply with the requirements of the Regulation 2024/1689, Member States will have to establish effective, proportionate and dissuasive penalties, including administrative fines, in relation to the infringements and shall communicate them to the EU Commission.

The Regulation establishes thresholds to be taken into account:

- 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, whichever is higher;
- Non-compliance with other relevant requirements set forth in the Regulation shall be subject to administrative fines of up to EUR 15 000 000 or, if the offender is an undertaking, up to 3 % of its total worldwide annual turnover for the preceding financial year, whichever is higher;

- The supply of incorrect, incomplete or misleading information to notified bodies or national competent 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, whichever is higher.

The EU Commission shall develop guidelines with a view to harmonising national rules and practices on the calculation of administrative fines.

EU institutions, agencies or bodies will not benefit from derogations: the European Data Protection Supervisor will have the power to impose financial penalties on them.

What are the regulatory sandboxes in the Artificial Intelligence sector?

The Regulation 2024/1689 introduces specific rules on the so called "AI regulatory sandboxes", meaning a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision.

Regulatory sandboxes, together with other measures such as networks of AI Centres of Excellence, public-private partnership on artificial intelligence, data and robotics, and access to digital innovation hubs and testing and experimentation facilities, will help create the right framework conditions for companies to develop and deploy AI.

Real-world testing of high-risk AI systems can be carried out for up to 6 months (extendable for a further 6 months). A plan shall be drawn up prior to the tests and submitted to the market surveillance authority, which shall approve the plan and the specific test conditions; If there is no response within 30 days, the plan is automatically considered tacitly approved. Evidence may be subject to inspection without prior notice by the authority.

Real-world testing can only be carried out if specific safeguards are in place, e.g. users of real-world test systems must provide informed consent, the tests must not have any adverse effect on users, test results must be reversible or can be ignored, and their data must be deleted after the tests have ended. Special protection must be granted to vulnerable groups, for example because of their age or physical or mental disability.