

Main new features of the EU's Regulation on artificial intelligence

After lengthy negotiations between the EU's institutions, on Wednesday 13 March 2024 the European Parliament adopted the AI Regulation, the final text of which was published in the Official Journal of the European Union on 12 July 2024.

As the most ambitious piece of legislation on this area in the world, this intention is that this regulation will become a global regulatory standard.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence ("[AI Regulation](#)"). The aim of the AI Regulation is to make the EU a global reference and standard-setting region for artificial intelligence ("AI") by ensuring that AI is human-centred, sustainable, safe, secure, inclusive and trustworthy, and guarantees respect for fundamental rights, democracy, the rule of law and environmental sustainability. At the same time, the AI Regulation aims to drive innovation and establish the EU as a leader in AI space, acting as a catalyst for industry.

The key points of the AI Regulation are summarised below:

1. DEFINITION OF AI

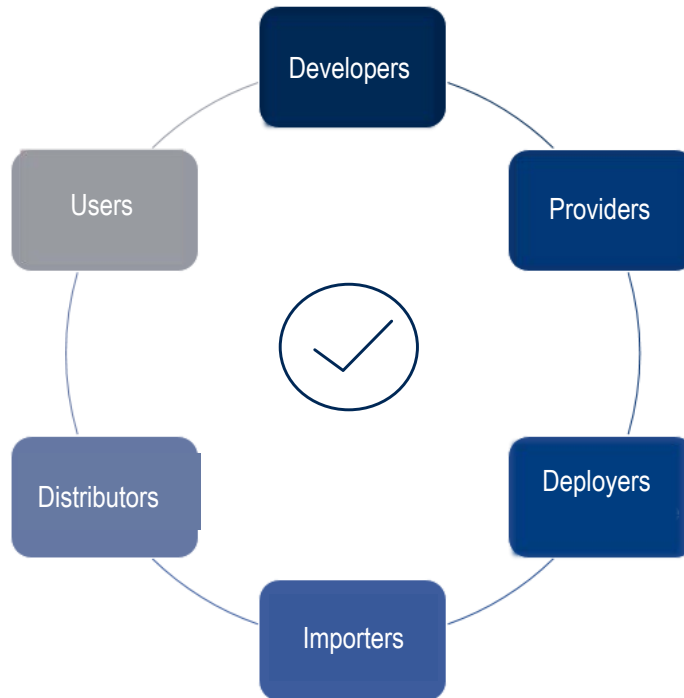
The main concepts defined in the AI Regulation are as follows:

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

General-purpose AI model: *an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market.*

2. SCOPE OF APPLICATION OF THE AI REGULATION

The objective of the AI Regulation in establishing its subjective scope has been to ensure that the rules it sets apply to the impact of AI systems in the EU, regardless of the location of the subjects involved



(extraterritorial application). The AI Regulation applies to the following subjects:

- (A) **providers** bringing AI systems to the market or putting them into service or placing on the market general-purpose AI models in the EU, irrespective of whether those providers are established or located within the EU or in a third country;
- (B) **deployers** of AI systems that have their place of establishment or are located within the EU;
- (C) **providers and deployers of AI** systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the EU;
- (D) **importers and distributors** of AI systems;
- (E) **product manufacturers** that place an AI system on the market or put it into service together with their product and under their own name or trademark;
- (F) authorised representatives of providers not established in the EU; and
- (G) affected persons that are located in the EU.



The EU intends to focus regulatory effort on those AI uses and systems that generate relevant risk in the EU market, in order not to hinder the development of AI or research activities and other low impact areas such as domestic use.

The AI Regulation shall **not** apply, however, to the following:

- (A) AI systems that are used exclusively for military, defence or national security purposes;
- (B) public authorities of third countries or international organisations using AI systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the EU or with one or more Member States, provided that the third country or international organisation provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals;
- (C) AI systems or AI models specifically developed and put into service for the sole purpose of scientific research and development;
- (D) research, testing or development activity regarding AAI systems or AI models prior to their being placed on the market or put into service (but it does apply to testing in real-world conditions);
- (E) deployers who are natural persons using AI systems in the course of a purely personal non-professional activity; and
- (F) AI systems released under free and open-source licences (e.g. they are placed on the market or put into service as high-risk or prohibited AI systems).

In any case, the AI Regulation does not affect and should be considered without prejudice to other EU legislation applicable to these systems or tools, such as on data protection, consumer protection, product safety or employment law. Likewise, the AI Regulation does not modify the liability of providers of intermediary services as set out in the Digital Services Regulation (EU) 2065/2022 (DSA).

3. APPROACH BASED ON THE RISK

The AI Regulation approaches artificial intelligence on the basis of the potential risks it may pose to individuals and seeks to tailor the type and content of the obligations in accordance with the scope and severity of the risks involved. Thus, the EU has followed a clearly defined risk-based approach in the AI Regulation so that the AI Regulation tailors the type and content of such rules to the intensity and scope of the risks posed by the AI systems to which it applies.



4. PROHIBITED AI PRACTICES

The AI Regulation considers certain AI practices to have an unacceptable risk. In particular, it prohibits the following practices:

PROHIBITED AI PRACTICES	
Using subliminal, manipulative or deceptive techniques	Use of subliminal techniques beyond a person's consciousness or deliberately manipulative or deceptive techniques that have the purpose or effect of substantially altering the behaviour of a person or a group of persons, impairing their ability to make informed decisions and causing them to take a decision that they would not otherwise have taken in a manner that causes or is reasonably likely to cause significant harm.

PROHIBITED AI PRACTICES	
Exploiting people's vulnerabilities	Exploitation of vulnerabilities of natural persons or groups of persons (due to age, disability, social or economic status) to alter their behaviour in a way that could reasonably be expected to cause significant harm
Classifying persons for the purposes of a citizen score	Evaluation or classification of natural persons or groups of persons based on their social behaviour or known, inferred or predicted personal or personality characteristics, such that the resulting citizen score results in detrimental or unfavourable treatment of particular persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity, or in detrimental or unfavourable treatment in social contexts unrelated to the context in which the data was originally generated or collected
Predicting potential criminality	Risk assessment of a natural person to assess or predict the likelihood of them committing a criminal offence based solely on profiling or assessment of personality traits and characteristics
Creating or expanding databases through mass facial recognition	Creation or expansion of facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage
Inferring emotions in educational or work settings	Inference of a person's emotions in workplaces or educational institutions, except where the AI system is intended to be used for medical or safety purposes
Biometric categorisation to infer special categories of data	Biometric categorisation to deduce or infer an individual's race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation, except for the mere filtering or labelling of lawfully acquired biometric data sets within the scope of law enforcement.

PROHIBITED AI PRACTICES

Real-time remote biometric identification in public places for law enforcement purposes

Real-time remote biometric identification in publicly accessible areas for law enforcement purposes, except where strictly necessary and pursuant to a mandatory judicial or administrative authorisation for:

- (i) searching for victims of abduction, trafficking in human beings or sexual exploitation, or searching for missing persons;
- (ii) preventing a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;
- (iii) locating or identifying a person suspected of having committed a particularly serious criminal offence (e.g. terrorism, drug trafficking, murder, child pornography) as identified in Annex II of the AI Regulation.

5. AI SYSTEMS OF HIGH RISK

In line with the risk-based approach, the AI Regulation lays down specific provisions on AI systems classified as “high-risk”, which are subject to enhanced obligations. The Regulation classifies the following as a high-risk AI system (with criteria that can be updated by the European Commission):

Regulated products	Those intended for use as a safety component in certain regulated products, or if the AI system itself is a regulated product (e.g. toys, automobiles, aircraft, watercraft, medical devices) covered by the legislation listed in Annex I of the AI Regulation.
Areas of particular significance or sensitivity	Those identified as particularly significant or sensitive in Annex III of the AI Regulation, which includes certain uses of AI in areas such as biometrics, education or workplaces, financial services, critical infrastructure, access to essential services (e.g. health, financial, emergency services), police, migration and asylum, administration of justice or electoral processes, unless they do not pose significant risks of harm to the fundamental rights of natural persons (e.g. if they are intended to perform a limited procedural task, to improve the outcome of a previously performed human activity or to detect patterns or deviations from decision-making patterns without the purpose of replacing or influencing human assessment, and provided they do not involve profiling).

5.1 REQUIREMENTS FOR HIGH RISK SYSTEMS

The AI Regulation sets out the following requirements for AI systems considered to be high-risk:

- (A) **Establish a risk management system** to identify and analyse known and reasonably foreseeable risks and to adopt appropriate measures against such risks.
- (B) **Conduct data governance and management** practices that include appropriate practices in **relation to** training, validation and testing data sets (taking into account, among other things, potential biases or contexts of use).
- (C) **Draw up technical documentation** prior to the system being placed on the market or putt into service, which must be kept up to date and prepared in such a way as to demonstrate that the AI system complies with the requirements of the AI Regulation.
- (D) **Keep records** through measures that technically allow automatic recording of events (log files) throughout the life of the AI system.

- (E) **Communicate information to deployers in a transparent manner** such that they can correctly use and interpret the AI system's output (e.g. by means of instructions for use explaining the characteristics, capabilities and limitations of the performance of the AI system).
- (F) **Include human oversight** to prevent or minimise the risks that may arise in the use of the AI system, by equipping the AI system with appropriate human-machine interface tools.
- (G) Design and develop **with appropriate levels of accuracy, robustness and cybersecurity** so that they perform consistently in those respects throughout their lifecycle (e.g. by establishing technical and organisational measures against errors, faults, biases or security breaches).

5.2 MAIN OBLIGATIONS RELATING TO HIGH RISK SYSTEMS

SUBJECTS	OBLIGATIONS
Providers	Ensure that the high-risk AI system complies with the requirements set out in the AI Regulation
	Identify themselves by registered trade name and contact address and affix the CE marking to the high-risk AI system or, if not possible, to its accompanying documentation
	Ensure that the high-risk AI system has undergone a conformity assessment procedure in accordance with the AI Regulation before being placed on the market or put into service
	Register the high-risk AI system and register as a high-risk AI system provider in the database established in the AI Regulation
	Establish a quality management system to ensure compliance with the obligations in the AI Regulation (e.g. procedures, policies, assessments, controls) in such a manner that compliance is properly documented and can be demonstrated to the competent authorities
	Retain all documentation relating to compliance with the AI Regulation (including, among other things, the EU declaration of conformity) for a period of ten years from the placing on the market or putting into service of the high-risk AI system
	Retain the logs automatically generated by the AI system for a period of time appropriate to their purpose (as a general rule, no less than six months)

SUBJECTS	OBLIGATIONS
	<p>Immediately take the necessary corrective actions when they consider that a high-risk AI system that they have placed on the market or put into service does not comply with the AI Regulation and inform distributors, deployers and other affected parties (e.g. importers)</p> <p>Cooperate with the competent authorities by providing information and documentation and demonstrating compliance with the AI Regulation</p> <p>Appoint an authorised representative in the EU, if the provider is established outside the EU, who shall have the above obligations where applicable</p>

Providers that understand that their AI system is not high-risk before placing it on the market must conduct and document an assessment. This assessment may be required by the competent authorities.

SUBJECTS	OBLIGATIONS
Importers	<p>Verify that the provider has complied with its obligations under the AI Regulation, before placing it on the market.</p> <p>Not to place a high-risk AI system on the market if they consider it to be non-compliant with the AI Regulation and to inform the provider, authorised representatives and market surveillance authorities thereof.</p> <p>Identify themselves by registered trade name and contact address in the high-risk AI system or, if not possible, in the accompanying documentation and ensure that it bears the CE marking.</p> <p>Ensure that the storage or transport conditions of the high-risk AI system do not compromise compliance with the AI Regulation.</p> <p>Retain documentation of compliance with the AI Regulation for a period of ten years from the placing on the market or putting into service of the high-risk AI system.</p> <p>Cooperate with the competent authorities by providing information and documentation and demonstrating compliance with the AI Regulation.</p>

SUBJECTS	OBLIGATIONS
Distributors	<p>Verify that the importer and provider have complied with their obligations under the AI Regulation and ensure that the high-risk AI system bears the CE marking.</p>
	<p>Not to place a high-risk system on the market if they consider it to be non-compliant with the AI Regulation and to inform the provider or importer accordingly.</p>
	<p>Ensure that corrective action is taken when they consider that a high-risk AI system does not comply with the AI Regulation and inform the provider, importer or other relevant operators (e.g. competent authority) and, where appropriate, inform them of the corrective action taken in this respect.</p>
	<p>Ensure that storage or transport conditions of the high-risk AI system do not compromise compliance with the AI Regulation.</p>
	<p>Cooperate with the competent authorities by providing information and documentation and demonstrating compliance with the AI Regulation.</p>
Deployers	<p>Establish appropriate technical and organisational measures to ensure the proper development of AI systems in accordance with the instructions of providers and the applicable regulations.</p>
	<p>Entrust human oversight of AI systems to qualified persons who can intervene and monitor their operation and ensure respect for fundamental rights and the safety of individuals.</p>
	<p>Ensure that the input used for the intended purpose of the AI system is relevant and sufficiently representative and that it is regularly updated, monitored and reviewed.</p>
	<p>Monitor the operation of the high-risk AI system based on its instructions for use and, where appropriate, inform providers in accordance with post-market surveillance obligations and the post-marketing plan, and report to the provider and the competent market surveillance authority any serious risks or incidents identified, and suspending the use of the system if necessary to prevent or mitigate damage.</p>
	<p>Retain the log automatically generated by the AI system for a period of time adequate for the intended purpose of the system (at least six months or as required by applicable legislation) and make them accessible to the provider, the market surveillance authority and notified bodies upon request.</p>

SUBJECTS	OBLIGATIONS
	Inform workers' representatives and the affected workers whether they will be exposed to the use of a high-risk AI system.
	Conduct a fundamental-rights impact assessment in relation to the specific use of the AI system, potential risks, human oversight mechanisms and other appropriate measures to prevent risks in the implementation of such high-risk AI systems. ¹
	Inform persons exposed to the use of the AI system that they are interacting with an AI tool, its purpose and the implications for their rights and obligations, unless it is obvious or unreasonable to do so.
	Cooperate with the competent authorities in the implementation of the AI Regulation, providing the necessary documentation and information and complying with any corrective or sanctioning measures adopted.

6. TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS

In addition to the obligations indicated in the previous section, the AI Regulation establishes additional transparency obligations for **providers** and **deployers** of certain AI systems, which have to be fulfilled at the first interaction or exposure:

AI SYSTEMS	SUBJECT	OBLIGATIONS
AI systems intended to interact with people (e.g. chatbots or virtual assistants)	Providers and deployers	Ensure that persons exposed to the use of the AI system are informed that they are interacting with an AI system, unless this is obvious given the circumstances and context of use.
AI systems that generate synthetic audio, video or text content.	Providers	Ensure that outputs are marked in a machine-readable format and that it is possible to detect that they have been artificially generated or manipulated.

¹ Where the AI system involves the processing of personal data, it may also be necessary to conduct a data protection impact assessment in accordance with Regulation (EU) 679/2016 (the General Data Protection Regulation). The two impact assessments are compatible, but not mutually exclusive, and may be complementary to each other.

AI SYSTEMS	SUBJECT	OBLIGATIONS
AI systems that generate synthetic audio, video or text content.	Deployers	Make public that content constituting a deep fake content has been artificially generated or manipulated.

7. GENERAL PURPOSE AI MODELS

A general-purpose AI model shall be classified as a general purpose AI model **with systemic risk** if it has high-impact capabilities or if it has certain capabilities. An AI system shall be presumed to have high-impact capabilities when it uses a specific cumulative amount of computation for its training (currently set as when the cumulative amount of computation measured in floating point operations exceeds 10^{25}).

A number of obligations on providers of general-purpose AI models are established:

- (A) prepare and keep up to date the technical documentation of the general-purpose AI model required by the AI Regulation;
- (B) make information of AI systems to providers of AI systems who intend to integrate it into their general-purpose AI model;
- (C) evaluate compliance of general-purpose AI models with protocols and tools that reflect the state of the art and assess and mitigate potential systemic risks that may result from their development;
- (D) monitor, document and report information on serious incidents to the AI Office or competent national authorities and ensure that an adequate level of cybersecurity protection is in place.

8. OTHER PROVISIONS OF THE REGULATION

- (A) **Regulatory sandboxes:** the AI Regulation allows personal data lawfully collected for other purposes to be processed in a controlled AI regulatory sandbox solely for the purpose of developing, training and testing certain AI systems in the sandbox when certain conditions are met.
- (B) **National competent authorities:** the AI Regulation requires Member States to designate a notifying authority and a market surveillance authority in the field of AI. In addition, it provides national authorities with investigative and sanctioning powers, as well as an obligation to establish an official single point of contact in each EU Member State.



In Spain, the competent market surveillance authority is the Spanish AI Supervisory Authority (AESIA), which is part of the Ministry for Digital Transformation and Public Administration and is based in A Coruña.

- (C) **Standardised templates for evidencing compliance:** the European Commission or the European standardisation authorities may establish standardised templates regarding the compliance requirements in the AI Regulation in order to facilitate AI systems evidencing compliance.
- (D) **European Artificial Intelligence Board:** a revised governance system of governance has been established at the EU level, with the introduction of the European Artificial Intelligence Board, an independent unit of the European Commission, composed of one representative from each Member State, with implementing powers at the EU level. The Board's task is to oversee foundational models and high-risk systems and will be advised by a permanent group representing interest groups such as providers, users or civil organisations.
- (E) **Surveillance, monitoring and controls:** market surveillance authorities must report annually to the European Commission and national competition authorities on any information gathered in the course of market surveillance activities that may be of potential interest for the application of EU competition law, as well as on the use of prohibited practices that have occurred during the year. In addition, the market surveillance authorities and the European Commission may propose joint investigation activities.

- (F) **Confidentiality:** the European Commission, market surveillance authorities, notified bodies and any other natural or legal person involved in the application of the AI Regulation must respect the confidentiality of information and data obtained in the exercise of their functions and activities.
- (G) **Codes of Conduct:** the AI Office will encourage and facilitate the development of Codes of Practice at the EU level, as an element to contribute to the correct implementation of the AI Regulation. The European Commission and Member States will also support the drafting of Codes of Conduct with the objective of encouraging the voluntary implementation of some of the requirements of the AI Regulation in certain types of AI systems.
- (H) **Penalties:** Member States shall lay down the rules on penalties, including warning measures or other non-monetary enforcement measures, as well as the applicability of the rules on penalties to public authorities and bodies. The AI Regulation also provides that the rules on penalties shall take into account the interests of SMEs, including start-ups, and their economic viability.

Fines are set for infringements of the AI Regulation.

Infringement	Fine
Non-compliance with the prohibition on certain AI practices	Fines of up to EUR 35 million , or if the offender is a company up to 7% of the total worldwide turnover for the preceding financial year, whichever is higher.
Failure to comply with the obligations imposed by the AI Regulation	EUR 15 million or, if the offender is a company, up to 3% of the total worldwide turnover for the preceding financial year, whichever is higher.
Submission of incorrect, incomplete or misleading information to the competent authorities in response to an application	EUR 7.5 million or, if the offender is a company, up to 1% of the total worldwide turnover for the preceding financial year, whichever is higher.

9. ENTRY INTO FORCE

The AI Regulation will have direct effect and application in all EU countries and will enter into force twenty days after its publication in the *Official Journal of the European Union*, i.e. from 2 August 2024.

Notwithstanding that entry into force, the AI Regulation will not apply until two years after its publication (i.e. from 2 August 2026), with the exception of certain provisions:

- the general provisions of the AI Regulation and those regarding prohibited AI practices shall apply from **six months** after entry into force, i.e. from 2 February 2025.
- the provisions concerning notifying authorities and notified bodies, general-purpose AI models, governance structure (AI Office, establishment and structure of the European AI Board, functions of the Board, consultative forum, etc.) and penalties will apply from **twelve months** after entry into force, i.e. from 2 August 2025.
- the provisions relating to AI systems classified as high-risk systems and the corresponding obligations shall apply **three years** after entry into force, i.e. from 2 August 2027.

10. CONTACT LAWYERS



Leticia López-Lapuente
+34 91 586 0131
leticia.lopez-lapuente
@uria.com



Ignacio Esteban Avendaño
+34 91 586 0644
ignacio.esteban@uria.com



Mirian Goitia
+34 91 587 0887
mirian.gotia@uria.com

