CUATRECASAS

Key aspects of the Artificial Intelligence Act

On May 21, 2024, the Council of the European Union approved the much awaited Artificial Intelligence Act. We analyze the main points below.

European Union - Legal flash
May 22, 2024

Key aspects

- The Artificial Intelligence Act ("**AI Act**") aims to foster the adoption of **trustworthy** and **human-centric AI**, while ensuring a high level of protection of health and safety, and fundamental rights against potential AI-related risks.
- **It prohibits certain AI practices** posing unacceptable risks.
- It qualifies certain AI systems as **high-risk** and it imposes stringent requirements for these systems, and obligations on operators involved in the value chain, including companies that use AI systems.
- It regulates the placing of **general-purpose AI models** on the market.
- It lays down **transparency obligations** for certain AI systems, particularly those intended to interact with natural persons or to generate content.
- It establishes an **institutional supervision and governance system** and imposes heavy **penalties** for infringement of the Act

Introduction

The **AI Act** regulates the **placing on the market**, the **putting into service** and the **use of artificial intelligence (AI) systems** in the EU. Its main goal is to foster the **development and use of AI** in the EU, while **ensuring a high level of protection of health, safety, and fundamental rights**.

It follows a **risk-based approach** considering the risks that may arise from the use of AI systems and it imposes requirements and obligations on the actors in the value chain. The obligations are not restricted to AI systems providers, but also affect, among others, **those who use AI systems for professional purposes**, who are referred to as "**deployers**."

The text of the AI Act is long and complex, and the European Commission will need to develop and clarify certain aspects through delegated acts and guidelines. Below we summarize the **main features** of the Act.

The EU's move to regulate AI by means of this Regulation is complemented by **other legislative initiatives**, particularly two proposals for Directives, that are currently being processed. First, the Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence, which establishes procedural rules on the burden of proof related to non-contractual civil liability claims for damage caused by AI systems. Second, the Proposal for a Directive on liability for defective products, which repeals the previous directive adopted in 1985 and addresses liability for AI systems that are defective and cause damage or data loss, allowing the possibility to seek compensation from the AI-system provider or from any manufacturer that integrates an AI system into another product.

The AI Act is without prejudice to EU law on other matters, some of which are closely related, such as data protection, consumer protection, fundamental rights, employment, worker protection and product safety. Specifically, the AI Act does not affect the obligations imposed under the **General Data Protection Regulation** on providers and deployers acting as data controllers or processors when the development or use of AI systems entails personal data processing.

Scope

The AI Act applies to:

- **providers** placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the EU, irrespective of whether they are established or located within the EU or in a third country;
- **deployers** of AI systems that have their place of establishment or are located within the EU;

- providers and deployers of AI systems that have their place of establishment or are located **outside the EU**, where the output produced by the AI system is used in the EU;
- **importers and distributors** of AI systems;
- **product manufacturers** placing on the market or putting into service an AI system together with their product and under their own name or trademark;
- authorized representatives of providers, which are not established in the EU; and
- affected persons that are located in the EU.

The AI Act **does not encompass** certain systems, such as systems used exclusively for military, defense or national security purposes, and those used solely for scientific research and development activity. Likewise, it does not apply to any research, testing or development activity regarding AI systems or AI models prior to their being placed on the market or put into service. Moreover, individuals using AI systems solely **for personal non-professional activity** are not subject to the AI Act.

AI system

The AI Act defines "**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."*

This is essentially the definition provided by the OECD[1], that the AI Act adopts to ensure a common, worldwide understanding of key terms. This definition, and thus the AI Act, exclude software systems with capacities lower than those specified above.

[1] See *Recommendation of the Council on Artificial Intelligence*, OECD, 2019 (amended in November 2023).

Actors subject to the AI Act

This Regulation mainly applies to the following:

Term	Description
Provider	A natural or legal person, or public authority that develops an AI system or a general-purpose AI model (or has one developed) and places it on the market or puts the AI system into service under its own name or trademark
Importer	A natural or legal person located or established in the EU that places on the market an AI system of a provider established outside the EU
Distributor	A natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the EU market
Deployer	A natural or legal person, or public authority **using an AI system** under its authority except where the AI system is used in the course of a personal non-professional activity

Prohibited practices

Consistent with its perspective based on the level of risk, the AI Act **imposes a total ban** on several AI practices that pose unacceptable risks. In brief, and without prejudice to the different nuances and exceptions it sets out, the AI Act prohibits the following practices:

- The use of **subliminal, manipulative or deceptive techniques** to distort the behavior of a person or a group of persons, causing them to take a decision they would not have otherwise taken in a manner that is likely to cause them significant harm.
- The exploitation of the **vulnerabilities** of a natural person or a specific group of persons due to their age, disability or a social or economic situation, with the aim or effect of distorting their behavior in a manner that is likely to cause them significant harm.
- AI systems for the evaluation or classification of natural persons or groups of persons over a certain time based on their social behavior or characteristics (social scoring), leading to detrimental or unfavorable treatment in social contexts unrelated to the contexts in which the data was collected, or treatment that is unjustified or disproportionate.
- AI systems for assessing or **predicting** the risk of a natural person committing a criminal offense, based solely on that person's profile or personality traits.

- AI systems that create or expand **facial recognition databases** through the untargeted scraping of facial images from the internet or CCTV footage.

- AI systems to **infer emotions** of a natural person in **workplace** and **education institutions**, except if their use is intended for medical or safety reasons.

- AI systems that categorize individually natural persons based on their **biometric data** to deduce or infer certain **sensitive data**.

- **Real-time remote biometric identification systems in publicly accessible spaces** for the purposes of law enforcement, barring certain exceptions, subject to several conditions and guarantees.

High-risk AI systems

The AI Act classifies as **high-risk** certain systems that pose a significant risk of harm to health, safety or fundamental rights. It differentiates between two groups:

- **Systems linked to the Union harmonization legislation on product safety** listed in **Annex I** to the AI Act: the AI system will be high-risk where it is a product included in this **harmonization legislation**, or where it is a safety component of these products; and provided that, under this **harmonization legislation**, the product or component must undergo a third-party conformity assessment.

- **Systems listed in Annex III** of the AI Act: those are systems that, owing to the area they are used in and the specific use they are given, in principle pose a high risk.

Annex III establishes **eight areas**, each of which identifies **specific cases of use** that are considered high-risk (insofar as their use is not prohibited). These areas are summarized below, along with some of the uses identified in each one, without going into great detail:

- **Biometrics**: this includes systems used for remote biometric verification; biometric categorization based on the inference of sensitive or protected characteristics; and emotion recognition, except in cases where it is forbidden.

- **Critical infrastructure**: systems 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.

- **Education and vocational training**: systems used to determine admission to educational and vocational training institutions; to evaluate learning results; to assess the level of education an individual will be able to access; and to monitor and detect prohibited behavior of students during tests.

- **Employment, workers management and access to self-employment**: AI systems used for (i) the recruitment or selection of natural persons, to place targeted job advertisements, to analyze and filter job applications, and to evaluate candidates; and (ii) making decisions affecting working conditions and the promotion or termination of work-related contractual relationships; allocating tasks based on individual behavior or personal traits or characteristics; and monitoring and evaluating workers' performance and behavior.

- **Essential private services and essential public services and benefits**: systems used to determine access to essential public assistance benefits and services; to evaluate the creditworthiness of natural persons (except those systems used to detect financial fraud); for risk assessment and pricing in the case of life and health insurance; and to establish priority in the dispatching of emergency first response services, e.g., by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems.

- **Law enforcement**: different systems used to prevent and investigate crimes, including certain predictive systems, and some systems used to profile natural persons or to evaluate the reliability of evidence.

- **Migration, asylum and border control management**: different systems used to assess security risks, risks of irregular migration, and health risks; to examine applications for asylum; and to recognize natural persons in the context of migration, asylum or border control.

- **Administration of justice and democratic processes**: systems used to assist a judicial authority in researching and interpreting facts and the law, and to influence the outcome of an election or referendum or the voting behavior of natural persons.

Within these eight areas, and following the criteria set out in the AI Act, the European Commission may add, amend or remove uses considered to be high-risk.

Even if a system is referred to in Annex III, it will **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. To reach a determination, the AI Act lays down some specific conditions, which the Commission may amend at a later date. The Commission is also requested to provide guidelines including "a comprehensive list of practical examples of use cases of AI systems that are high-risk and not high-risk." In any case, AI systems referred to in Annex III that perform **profiling of natural persons** will always be considered high-risk.

Requirements for AI systems and providers' obligations

The AI Act imposes very stringent **requirements** on high-risk systems, and subjects certain actors to a series of **obligations**.

In brief, high-risk AI systems **must**, among other requirements:

- implement and maintain a **risk management system** throughout the system's entire lifecycle;
- ensure **the quality of training, validation and testing data** through appropriate data governance and management practices;
- draft **technical documentation** on the system and keep it up to date;
- allow for the **automatic recording of events**;
- provide **instructions for use that are comprehensible for deployers**;
- allow effective **human oversight** while they are being used; and
- meet an appropriate level of **accuracy, robustness and cybersecurity**;

Fulfillment of these requirements can be proven through certain presumptions, particularly the presumption that they are fulfilled when the system meets the corresponding standards provided by European standardization organizations, the references of which are published in the Official Journal of the European Union, or when they adapt to the common specifications established by the European Commission.

The AI Act also imposes obligations on providers, deployers and other affected actors.

Below we summarize the main **obligations** that high-risk AI system **providers** must fulfill:

- They must ensure that their systems meet the above **requirements** and demonstrate their conformity on a reasoned request of a competent authority.
- Providers should establish a sound **quality management system**.
- They must keep the **documentation** on the system and make it available to the authorities, as well as any **logs** under their control.
- They must ensure that the system undergoes **the conformity assessment**; draw up an **EU declaration of conformity;** and affix a **CE marking** to the system.
- They must register the system in the EU **database** of high-risk systems.
- They must take the necessary **corrective actions**, including withdrawing the system or disabling it if it is not in conformity with the AI Act.

In certain cases, a distributor, importer, deployer or other third-party **will be considered to be a provider** and will be subject to the above obligations. This occurs in cases where the party in question **puts its name or trademark** on a high-risk AI system already placed on the market, or makes a **substantial modification** to the system.

Obligations imposed on enterprises that use high-risk AI systems

Any natural or legal persons that use AI systems for professional purposes, referred to as "deployers," are subject to several obligations among which we highlight the duty to:

- take appropriate **technical and organizational measures** to ensure they use the systems in accordance with the instructions of use;
- ensure that **human oversight** tasks are performed by persons with the necessary competence;
- ensure that **input data** is **relevant and representative** in view of the intended purpose of the system to the extent the deployer exercises control over that data;
- **monitor the functioning** of the system and **report any risks and incidents** to the provider, importer or distributor, and to the market surveillance authorities;
- keep any **logs** generated when under their control;
- **inform their workers and legal representatives** before implementing a high-risk AI system in the workplace;
- **inform** any individuals that may be affected by the use of systems that make decisions or assist in making decisions;
- **cooperate** with the competent authorities; and
- ensure that the staff and other persons assigned on their behalf to deal with the operation and use of AI systems have an adequate level of **AI literacy**.

In certain cases, deployers must carry out a fundamental rights **impact assessment**.

Transparency obligations for certain AI systems

The AI Act imposes transparency obligations for certain AI systems, regardless of whether they qualify as high-risk, as follows:

- Systems intended to **interact directly with natural persons**: the **provider** must design the system in such a way that the natural persons concerned are informed that they are interacting with an AI system.

- Systems that generate **synthetic audio, image, video or text content**: the **provider** must ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated.

- **Emotion recognition systems** and **biometric categorization systems**: the **deployer** must inform the natural persons exposed to them of the operation of the system.

- Systems that generate or manipulate image, audio or video content constituting a **deep fake** and texts informing on matters of public interest: the **deployer** must disclose that the content has been artificially created or manipulated.

General-purpose AI models

As well as focusing on AI systems, the AI Act also addresses certain AI **models**. General-purpose AI models are integrated into AI systems, but are not systems per se. The AI Act defines **general-purpose AI models** as those that have a considerable degree of generality, are capable of performing a wide range of tasks, and can be integrated into several AI systems or applications.

The **providers** of these models are subject to certain obligations, including the obligation to:

- document the training process and the results of its evaluation;

- inform providers of AI systems who intend to integrate the general-purpose AI model into their systems of their characteristics and legal requirements;

- put in place a policy to comply with EU law on copyright and related rights, particularly as regards text and data mining; and

- make publicly available a detailed summary of the content used for training the general-purpose AI model.

Due to their high-impact capabilities, certain general-purpose AI models are considered to present a **systemic risk**, and providers are subject to stricter requirements to mitigate these risks.

Penalty regime

Member States will lay down the rules on penalties applicable to infringements.

- Non-compliance with the **prohibition of the AI practices** referred to in the AI Act will be subject to administrative fines of up to **€35 million or up to 7% of the offender's total worldwide annual turnover**, whichever is higher.

- Non-compliance with the main provisions imposed on providers, authorized representatives, importers, distributors and deployers will be subject to administrative fines of **up to €15 million or 3% of the offender's total worldwide annual turnover**, whichever is higher.

- The **supply of incorrect, incomplete or misleading information** to notified bodies or national competent authorities in reply to a request will be subject to fines of up to **€7 million or up to 1% of the offender's total worldwide annual turnover**, whichever is higher.

In the case of SMEs, including start-ups, the fine will be whichever is lower of the indicated maximum amounts and percentages.

Next steps

The AI Act will enter into force 20 days after it is officially published. In general terms, it will be applicable 24 months later. However, different terms are established for some articles, ranging between 6 months in the case of prohibited practices, 12 months in the case of some governance rules, and 36 months in the case of provisions on high-risk systems linked to EU harmonization legislation on product safety.

For additional information, please contact our *Knowledge and Innovation Group* lawyers or your regular contact person at Cuatrecasas.