EU 2024 ai regulation balances safety and innovation

In recent years, one common word we frequently hear in conversations – whether with professionals, students, or even teenagers – is Artificial Intelligence ("AI"). In reality, AI is a fast-evolving family of technologies that contributes to a wide array of economic, environmental, and societal benefits across the entire spectrum of industries and social activities.

What does Artificial Intelligence really mean? What does this term entail? Defining AI is not easy; in fact, there is no generally accepted definition of the concept. It is tricky though because while organizations and experts have tried to define artificial intelligence, there is no consensus on a single definition. Its definition can vary depending on the context, which may have helped AI to be adapted and advance in different scenarios.

Definition

In the UK, the House of Lords' Select Committee on AI recently released a report that used this definition:

'Technologies capable of performing tasks that would otherwise require human intelligence, such as visual perception, speech recognition, and language translation.'

As AI has a major impact on society and as part of its digital strategy, the European Union (EU) wants to regulate artificial intelligence to ensure consistency and protection of public interests regarding health, safety, and other fundamental rights, while supporting innovation. The EU wishes for AI systems to be overseen by people, rather than by automation, to prevent harmful outcomes.

For this purpose, the Parliament adopted the Artificial Intelligence Act, Regulation (EU) 2024/1689 ("AI Act") in March 2024, which was published in the Official Journal of the European Union in July 2024, making it the first comprehensive legal framework for the regulation of AI systems across the EU.

The AI Act is a legal framework regulating the development, placing on the market, putting into service, and use of artificial intelligence systems (AI systems) in the Union to ensure protection of public interests regarding health, safety, the environment, and fundamental rights. It sets specific requirements for high-risk systems, obligations for operators of such systems, and transparency rules for certain AI systems.

Application

This AI Act applies to Union institutions, bodies, offices, and agencies when acting as a provider or deployer of an AI system. Specifically, it applies to:

a) Providers placing on the market or putting into service AI systems or general-purpose AI models in the Union, irrespective of whether they are established within the Union or in a third country, and authorised representatives not established in the Union;

b) Deployers of AI systems established or located within the Union;

c) Importers and distributors of AI systems;

d) Manufacturers placing on the market an AI system.

The EU AI Act also enumerates certain exceptions to its material scope. For example, the EU AI Act

does not apply to AI systems released under free and open-source licenses unless they are prohibited or classified as high-risk AI systems, or AI systems used for the sole purpose of scientific research and development, and to deployers who are natural persons using AI systems in the course of a purely personal, non-professional activity.

To distinguish AI from simpler software systems, the AI Act defines an AI system as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments." The definition is broad enough to cover a wide range of data analysis techniques.

Assessment of Risk

The AI Act is a legal framework laying down rules on the development and use of AI in the internet market. The new rules establish obligations for providers and users depending on the level of risk from artificial intelligence. While AI systems pose minimal risks, according to the AI Act, this risk needs to be assessed.

The AI Act lays down a solid risk methodology to define “high-risk” AI systems that create significant risk to health, safety, or fundamental rights. It prohibits certain AI practices, lays specific requirements for high-risk AI systems, and establishes obligations for the operators concerned, along with transparency rules for lower-risk AI systems.

The framework identifies four categories of risk:

Unacceptable Risk: The EU AI Act prohibits certain uses of artificial intelligence (AI). These include AI systems that manipulate people's decisions or exploit their vulnerabilities, systems that evaluate or classify people based on their social behavior or personal traits, and systems that predict a person's risk of committing a crime.

High Risk:

AI systems identified as high-risk include AI technology used in:

- Critical infrastructures (e.g., transport), that could put the life and health of citizens at risk
- Educational or vocational training, that may determine access to education and professional course of someone’s life (e.g., scoring of exams)
- Safety components of products (e.g., AI application in robot-assisted surgery)
- Employment, management of workers, and access to self-employment (e.g., CV-sorting software for recruitment procedures)
- Essential private and public services (e.g., credit scoring denying citizens the opportunity to obtain a loan)

EU wants to regulate AI to ensure consistency and protection of public interest

High-risk AI systems are subject to strict obligations before they can be put on the market:

- Adequate risk assessment and mitigation systems
- High quality of the datasets feeding the system to minimize risks and discriminatory outcomes
- Logging of activity to ensure traceability of results
- Detailed documentation providing all information necessary on the system and its purpose for authorities to assess its compliance
- Clear and adequate information to the deployer
- Appropriate human oversight measures to minimize risk
- High level of robustness, security, and accuracy

Limited Risk: A classification for AI systems or uses that do not fall within the High-Risk category but do pose certain transparency risks and requirements not associated with Minimal Risk systems (such as chatbots).

Minimal Risk: A classification for AI systems or uses with minimal impact on individuals and their rights (e.g., spam filters or games), and are largely unregulated by the AI Act directly (and are instead regulated by other EU-wide and national legislation).

Governance

Member States hold a key role in the application and enforcement of this AI Act. Each Member State should designate at least one notifying authority and at least one market surveillance authority as national competent authorities for the purpose of supervising the application and implementation of this Act. Member States can appoint any kind of public entity (i.e., competition authority, data protection authority, cybersecurity agency) to perform the tasks of the national competent authorities, in accordance with their specific national organizational characteristics and needs.

According to Article 77, by 2 November 2024, each Member State shall identify the public authorities or bodies and make a list of them publicly available. Member States shall notify the list to the Commission.

On 6 November 2024, in Cyprus, the Deputy Ministry of Research, Innovation, and Digital Policy notified the European Commission of a list of three national public authorities that will supervise or enforce compliance with the obligations under EU law to protect fundamental rights, in accordance with Article 77 of Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act). This action completes the first obligation of Cyprus for the national implementation of the AI Regulation.

The list of public authorities of the Republic of Cyprus is as follows:

1) Commissioner for Personal Data Protection
2) Commissioner for Administration and the Protection of Human Rights (Ombudsman)
3) Attorney-General of the Republic

It is noted that the authorities included in the list will be granted additional powers under the Regulation to facilitate the exercise of their existing responsibilities in protecting fundamental rights in cases where the use of artificial intelligence (AI) poses high risks to these rights. These powers will take effect from 2 August 2026.

Enforcement

The regulation will fully apply from 2 August 2026, while prohibitions on high-risk AI practices and other general provisions will take effect earlier, on 2 February 2025. This phased approach reflects the urgency of mitigating risks while allowing stakeholders time to adapt.

Totalserve group has succeeded throughout its 54 years of operations to be an award-winning professional services provider. Headquartered in Limassol, Cyprus, the group maintains 2 more offices - in Athens, London. Totalserve specialises in the fields of corporate, trusts, fiduciary services and tax. Further, there is a specialised Intellectual Property department, assisting with all IP related aspects. Legal and audit services are offered through other group affiliated companies.

TOTALSERVE MANAGEMENT LIMITED

Virginia Adamidou, LL.B., MBA
Partner
virginia.adamidou@totalserve.eu