

# Artificial Intelligence Act

2021/0106(COD) - 12/07/2024 - Final act

**PURPOSE:** to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter of Fundamental Rights, including democracy, the rule of law and environmental protection, against the harmful effects of artificial intelligence systems (AI systems) in the Union, and to support innovation.

**LEGISLATIVE ACT:** Regulation (EU) 2024/1689 of the European Parliament and of the Council 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).

**CONTENT:** the regulation on AI aims to foster the development and uptake of **safe and trustworthy AI systems** across the EU's single market by both private and public actors. At the same time, it aims to ensure **respect of fundamental rights** of EU citizens and stimulate **investment and innovation** on artificial intelligence in Europe. The AI act applies only to areas within EU law and provides exemptions such as for systems used exclusively for military and defence as well as for research purposes.

## *Prohibited AI Practices*

The legislation follows a **'risk-based' approach**, which means the higher the risk to cause harm to society, the stricter the rules. The new law categorises different types of artificial intelligence according to risk. AI systems presenting only limited risk would be subject to very light transparency obligations, while high-risk AI systems would be authorised, but subject to a set of requirements and obligations to gain access to the EU market.

The new rules prohibit the following AI practices:

- AI system that deploys **subliminal techniques** beyond a person's consciousness or purposefully manipulative or deceptive techniques;
- AI system that exploits any of the **vulnerabilities** of a person or a specific group of persons due to their age, disability or a specific social or economic situation;
- AI systems with **social scores**;
- AI system for making risk assessments of natural persons in order to assess or predict the likelihood 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;
- AI systems that create or expand **facial recognition** databases through the untargeted scraping of facial images from the internet or CCTV footage;
- **'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement**, unless and in so far as such use is strictly necessary for one of the following objectives: (i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as searching for missing persons; (ii) the prevention of a genuine threat of a terrorist attack; (iii) the identification of a person suspected of having committed a criminal offence, for

the purpose of conducting a criminal investigation, prosecution or executing a criminal penalty for offences punishable by a custodial sentence of a maximum duration of at least four years.

The following have been added to the list of high-risk systems, in particular, systems intended to be used:

- as safety components in the management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating and electricity;
- to determine the access, admission or assignment of individuals to educational and vocational training establishments, at all levels;
- for the recruitment or selection of natural persons, in particular for publishing targeted job offers, analysing and filtering applications and evaluating candidates;
- to assess the eligibility of individuals for essential social security benefits and services, including healthcare services;
- for risk assessment and pricing of life and health insurance for individuals;
- to influence the outcome of an election or referendum or the electoral behaviour of natural persons in the exercise of their vote.

### ***Transparency and protection of fundamental rights***

Before a high-risk AI system is deployed by some entities providing public services, the fundamental rights **impact** will need to be assessed. High-risk AI systems, as well as certain users of a high-risk AI system that are public entities will need to be registered in the **EU database** for high-risk AI systems, and users of an emotion recognition system will have to inform natural persons when they are being exposed to such a system.

### ***General-purpose AI (GPAI)***

General-purpose AI systems, and the GPAI models such as ChatGPT they are based on, must meet certain **transparency requirements** including compliance with EU copyright law and publishing detailed summaries of the content used for training. The more powerful GPAI models that could pose systemic risks will face additional requirements, including performing model evaluations, assessing and mitigating systemic risks, and reporting on incidents.

Additionally, artificial or manipulated images, audio or video content (“deepfakes”) need to be clearly labelled as such.

### ***Measures in support of innovation***

The new legislation foresees that AI **regulatory sandboxes**, enabling a controlled environment for the development, testing and validation of innovative AI systems, should also allow for testing of innovative AI systems in real world conditions.

### ***Governance***

To ensure proper enforcement, several governing bodies are set up: (i) an AI Office within the Commission to enforce the common rules across the EU; (ii) a scientific panel of independent experts to

support the enforcement activities; (iii) an AI Board with Member States' representatives to advise and assist the Commission and Member States on consistent and effective application of the AI Act; (iv) an advisory forum for stakeholders to provide technical expertise to the AI Board and the Commission.

### ***Penalties***

The fines for infringements to the AI act are set as a percentage of the offending company's global annual turnover in the previous financial year or a predetermined amount, whichever is higher. SMEs and start-ups are subject to proportional administrative fines.

ENTRY INTO FORCE : 1.8.2024.

APPLICATION: from 2.8.2026.