Akin®

EU Ratifies Pioneering Artificial Intelligence Legislation

May 31, 2024

Reading Time : **9 min**

By: Davina Garrod, Jenny Arlington, Jay Jamooji, Olivia Odubanjo, Natasha G. Kohne, Hans Christopher Rickhoff, Reggie Babin, Ryan Dowell

On May 21, 2024, the European Union finalized the adoption of the groundbreaking EU Artificial Intelligence Act, a comprehensive and sector-agnostic legislation that extends globally. This 420-page Act aims to regulate the deployment and development of AI systems, categorizing them into high-risk and low-risk, and even banning certain types of AI. The Act emphasizes trust, transparency, and accountability in AI usage, promoting the safe integration of AI technologies. This legislation sets a potential global benchmark for AI regulation, although its complexity may pose interpretative and implementation challenges for stakeholders. We set out the key provisions below.

Extra-territorial Scope Affecting a Wide Range of Participants in the AI Value / Supply Chain

The AI Act regulates "AI systems", defined broadly but generally along the lines of the definition in the Organization for Economic Cooperation and Development (OECD) Principles for Trustworthy AI,[2] as well as "general-purpose AI models" (GP AI models), which are defined as models that display significant generality, are capable of competently performing a wide range of distinct tasks and that can be integrated into a variety of downstream systems or applications (including where such an AI model is trained with a large amount of data using self-supervision at scale). GP AI models include the large language or foundation models currently being used by consumers and businesses around the world. AI models which are used for research, development or prototyping activities before they are placed on the market are excluded from the GP AI models definition.

Akin®

In terms of territorial scope, the AI Act applies to providers placing on the market AI systems or GP AI models in the EU, or putting into service (i.e., supplying an AI system for own use or for first use to deployers) AI systems in the EU, regardless of where such providers are located or established in the world. Deployers of AI systems that are located or established in the EU are caught by the Act too, as well as providers and deployers of AI systems outside the EU where the output by the AI system is used in the EU. Product manufacturers, importers and distributors are among the other stakeholders subject to the AI Act.

The Act sets out a few exemptions from its scope, such as AI systems exclusively used for military, defence or national security purposes, or AI systems and AI models specifically developed and put into service for the sole purpose of scientific research and development.

Obligations Depend on What Risk an AI System Poses (Other than for GP AI Models)

The AI Act adopts a risk-based approach to uses of AI systems, outlining four levels of risk; the higher the risk, the stricter the obligations. Businesses are to identify which level (or levels) of risk their AI systems fall into.

Unacceptable risk: prohibited AI practices

AI systems which are particularly harmful, abusive or dangerous, and contradict EU values of respect for human dignity, freedom, equality, democracy, the rule of law and fundamental rights (including the right to non-discrimination, to data protection and to privacy), are prohibited. At a high level, these include:

1. AI systems that deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective or effect of materially distorting that person's behaviour (by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken) in a manner that causes or is reasonably likely to cause significant harm;

2. AI systems that exploit any vulnerabilities due to individuals' age, disability or a specific social or economic situation, with the objective or effect of materially distorting that person's behaviour in a manner that causes or is reasonably likely to cause significant harm;

3. AI systems used to evaluate or classify people over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics (i.e. social scoring), resulting in certain detrimental or unfavourable treatment;

4. AI systems used to make a risk assessment in order to predict the risk of a person committing a criminal offence;

5. AI systems used to create or expand facial recognition databases by untargeted scraping of facial images on the internet and closed-circuit television (CCTV) footage;

6. emotion recognition systems in the workplace and education institutions (except for medical or safety reasons);

7. biometric categorisation systems that categorise persons based on their biometric data to deduce or infer sensitive personal data, unless limited exceptions apply; and

8. use of real time remote biometric identification in publicly accessible spaces for law enforcement, unless limited exceptions apply.

High-risk AI systems: data governance, risk management, safety and other obligations, including mandatory registration in a public database

AI systems considered high risk under the Act entail a raft of new obligations for developers, deployers and other stakeholders.

A wide range of AI systems are considered high-risk, including:

1. certain biometric identification, categorisation and emotion recognition systems;

2. AI systems used in the management and operation of critical infrastructure, including digital infrastructures;

3. AI systems used in the employment and workers management, including recruitment;

4. AI systems used to evaluate creditworthiness of people or access to other essential private or public services;

5. AI systems used for influencing the outcome of an election, referendum or the individuals' voting behaviour; and

6. an AI system which is used as a safety component of a product or is itself a product covered by specified EU laws, such as those concerning vehicles, aviation, lifts, medical devices and machinery.

Akin®

Derogations to the classification of high-risk AI systems have been introduced: for example, if an AI system is intended to perform a narrow procedural task, or does not otherwise pose a significant risk to harm to the health, safety or fundamental rights of natural persons, it can be considered not high-risk but the provider has to document an impact assessment and still register the AI system in the EU database.

Providers of high-risk AI systems must ensure they comply with the new requirements and demonstrate such compliance to the regulator, on request. They include obligations regarding quality of the training, validation and testing data sets; transparent operations; design that includes human oversight; achieving appropriate levels of accuracy, robustness and cybersecurity; implementing a risk management system; undergoing a pre-market conformity assessment affixing the "Conformité Européenne (CE) marking" of conformity; and registering the AI system in a public EU database.

Deployers of high-risk AI systems must monitor its operations, ensure the input data is relevant and sufficiently representative, and report certain risks to the developer and the regulator.

In certain circumstances deployers of high-risk AI systems are to be considered providers. As the Act allocates responsibilities along the AI value / supply chain, it requires that in such cases the initial provider cooperates closely with the new provider and assists with the fulfilment of the relevant obligations.

Limited risk AI systems, including certain general-purpose AI systems: transparency obligations

AI systems that interact with individuals (such as chatbots), emotion recognition and biometric categorisation systems, and other systems such as those generating synthetic content or creating 'deep fakes', are considered to pose limited risk and, as a result, are subject to certain transparency obligations. The providers and deployers of such AI systems will be required to provide further information and disclosures to individuals, unless limited exemptions apply.

Minimal risk: no mandatory requirements but voluntary codes of conduct

All other AI systems (apart from GP AI models, see below) fall within the category of AI presenting minimal risk and are not subject to mandatory requirements. These include, for example, AI-enabled video games and email spam filters. They are encouraged to adhere to

voluntary codes of conduct which would follow some of the high-risk AI systems requirements.

Obligations on Providers of GP AI Models, and Stricter Obligations Regarding GP AI Models with Systemic Risk

The Act regulates all GP AI models and some of them, considered GP AI models with systemic risk, are subject to further requirements.

GP AI models

Providers of all GP AI models are subject to new obligations, including:

> 1. to draw up and keep up-to-date technical documentation to be provided to the regulator on request, including details on the design specifications and data used for training, testing and validation;

> 2. to draw up and make available certain information and documentation to providers of AI systems who intend to integrate the GP AI model into their AI systems, including information to enable such providers to have a good understanding of the capabilities and limitations of the GP AI model and to comply with their obligations under the Act;

> 3. to implement a policy to comply with EU law on copyright and related rights;

> 4. to draw up and make publicly available a sufficiently detailed summary about the content used for training of the GP AI models.

By way of derogation, GP AI models that are released under a free and open licence are exempt from certain of these requirements, unless these models are GP AI models with systemic risk.

GP AI models with systemic risk

GP AI models with systemic risk are those models that have high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, or those that have been determined to have such capabilities by the European Commission (EC) having regard to certain criteria, such as number of parameters of the model, quality or size of the data set, input and output modalities and number of registered users. When the cumulative amount of computation used for the training of a GP AI model, measured in floating points operations,

is greater than 10^{25}, it is presumed that the GP AI model is with systemic risk. It is envisaged that providers of GP AI models can challenge the decision of the EC to classify the model as one with systemic risk.

Providers of GP AI models with systemic risk must comply with the obligations in respect of GP AI models mentioned above, as well as with additional obligations including performing model evaluation, assess and mitigate possible systemic risks, report serious incidents to the regulators and ensure an adequate level of cybersecurity.

New Regulators, Penalties and Enforcement

A newly created AI Office at EU level will oversee the implementation and enforcement of the AI Act. The EC has exclusive powers to enforce the provisions relating to GP AI models, and it has entrusted the implementation of that task to the AI Office, which for example may conduct evaluations of the GP AI models. The AI Office may also assist national authorities in relation to market surveillance of high-risk AI systems. In addition, it should facilitate the drawing up of codes of conduct to assist businesses with compliance.

Another institution created under the Act is the European Artificial Intelligence Board, composed of representatives of the EU member states, which will be responsible for advisory tasks such as issuing opinions and recommendations.

In respect of penalties:

> 1. non-compliance with the prohibition on AI systems carrying unacceptable risk is subject to fines of up to 7% of total worldwide annual turnover or EUR 35 million, whichever is higher;
>
> 2. breach of certain provisions in respect of high-risk AI systems will result in a fine of up to 3% of total worldwide annual turnover or EUR 15 million, whichever is higher;
>
> 3. the supply of incorrect, incomplete or misleading information to the relevant authorities may also be subject to a fine of up to 1% of total worldwide annual turnover or EUR 7.5 million, whichever is higher; and
>
> 4. providers of GP AI models will be subject to fines of up to 3% of total worldwide annual turnover or EUR 15 million, whichever is higher, when the EC finds that the provider intentionally or negligently infringed the AI Act or failed to comply with requests from the regulators.

Akin

Timing

There will now be a staggered entry into force, with the provisions relating to prohibited AI systems applying from around December 2024 (six months after the publication of the AI Act in the Official Journal, which is expected to occur shortly). The obligations relating to GP AI models will apply from around June/July 2025, and most of the remaining provisions, including as to high-risk AI systems, from June/July 2026.

The **Global Akin AI Group** is available to discuss the AI Act, and other AI developments at your convenience.

---

[1]https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/

[2]https://oecd.ai/en/ai-principles

Categories

| Cybersecurity, Privacy & Data Protection | European Union | United Kingdom |

| Artificial Intelligence | Consumer Data Protection |

other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.