KIRKLAND & ELLIS

Kirkland Alert

AI Act Arrives: EU Equips AI With a New Rulebook

01 August 2024

Overview

The European Union's long-awaited Artificial Intelligence Act (the "**AI Act**") comes into force today, 1 August 2024. Whilst many of the AI Act's provisions apply starting on 2 August 2026, certain obligations will be phased in sooner. Providers, commercial deployers and intermediaries of AI systems should start to develop their compliance frameworks in short order to avoid the risk of heavy fines associated with non-compliance.

Who does the AI Act apply to?

The AI Act applies to "*providers*" and "*deployers*" of AI systems — broadly, those who develop and place AI systems on the EU market under their own name or trademark, and those who use AI systems in the EU market for professional or business purposes. The AI Act has "extra-territorial effect", and therefore applies to providers and deployers even if they are located outside of the EU, provided that the output of the AI system is used in the EU.

The AI Act also applies to other intermediaries in the AI supply chain, such as "*importers*" and "*distributors*" of AI systems, i.e., those who place AI systems on the EU market under the name or trademark of an entity based outside of the EU, and those who (whilst not providers or deployers) place AI systems on the EU market, respectively, as well as to product manufacturers, authorised representatives of providers and other affected persons located in the EU.

What is an AI System and how is it regulated?

The term "*AI system*" is broadly defined to mean "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".

Some may argue that this definition is only moderately elevated above traditional software, with the key differentiating elements including the concepts of "autonomy" and ability to "infer".

The AI Act categorizes AI systems based on the risks posed by their respective use cases, in order to take a tiered approach to regulation: most notably, unacceptable risk (prohibited) and high risk (subject to compliance obligations, which generally align with good practice AI standards, ethics and quality controls). In addition, the AI Act places transparency obligations on certain other AI systems, and further obligations on providers of "general purpose AI models".

The AI Act is not intended to (unduly) stifle AI development in the EU, and that philosophy can generally be seen in the AI Act's obligations:

Unacceptable Risk AI

AI systems that pose an unacceptable level of risk are prohibited and will be banned. Examples include AI systems that deploy subliminal, manipulative or deceptive techniques to impair an individual's ability to make an informed decision, AI systems that exploit vulnerable groups, and AI systems that predict the risk of an individual committing a criminal offence based solely on profiling. Article 5 of the AI Act provides a detailed list of prohibited AI practices.

High-Risk AI

The AI Act sets out specific classification criteria to establish whether an AI system is "high-risk", and expressly includes example use cases within: (i) biometrics; (ii) the management or operation of critical infrastructure; (iii) education and vocational training; (iv) employment, worker management and access to self-employment; (v) access to and enjoyment of essential private and public services and benefits; (vi) law enforcement; (vii) migration, asylum and border control management; and (viii) administration of justice and democratic processes. It is important to note that not all use cases within the above categories or sectors will be considered "high risk"; Annex III of the AI Act provides more specific details. For example, not all AI systems used by

an educational establishment would be “high risk”; but, Annex III specifies that AI systems used to determine access or admission to an institution would be (amongst other examples).

The AI Act also specifies that certain AI systems used in products falling under the EU’s product safety legislation, such as toys, aviation, cars, medical devices and lifts, will be considered "high risk".

AI systems that pose a high risk will not be banned, but are subject to compliance obligations. Those compliance obligations are broadly considered to align with good practice AI standards, ethics and quality controls; although in-scope entities should conduct a compliance audit ahead of the relevant obligations coming into effect to ensure that: (i) high risk AI systems are identified; (ii) any gaps between the entity’s current practice and the AI Act’s compliance obligations are identified; and (iii) a road-map is developed to ensure compliance gaps are addressed prior to the relevant obligations coming into effect.

- **Obligations on providers of high-risk AI systems**: Providers of high-risk AI systems are required, *inter alia*, to register the AI system in a publicly accessible EU database, conduct post-market quality assessments throughout the lifecycle of the AI system, apply human oversight, create technical documentation, maintain records, implement cybersecurity measures and make a declaration of conformity with the AI Act.

- **Obligations on deployers of high-risk AI systems**: Deployers of high-risk AI systems are subject to fewer obligations, including, *inter alia*, to monitor the AI system and maintain logs of its operation, and inform workers’ representatives when using high-risk AI systems in the workplace.

- **Obligations on importers and distributors**: Distinct obligations apply to intermediaries in the AI supply chain, namely, importers and distributors. For example, intermediaries must verify that the AI system bears the required CE conformity assessment marking indicating that the AI system conforms with the AI Act.

Crucially, if a deployer, importer or distributor puts their own name or trademark on an AI system, substantially modifies an AI system or deploys it for a high-risk use case otherwise than in accordance with the use case intended by the provider, the deployer, importer or distributor may be deemed to be a provider themselves.

Certain exceptions are made for AI systems used for testing and development or for scientific research. Individuals will have the right to file complaints about high-risk AI systems to regulators designated by each Member State.

Transparency Obligations

AI systems that are intended to directly interact with individuals, but that do not meet the legislative criteria for unacceptable or high-risk, may be subject to transparency obligations (e.g., chatbots and deepfakes), in particular where it would not be obvious from the user's point of view that they are interacting with an AI system.

Beyond such transparency obligations, AI systems that pose minimal or no risks (and which are not considered "general purpose AI") are generally not regulated by the AI Act. Notably, the European Commission's strategy paper states that: "*the vast majority of AI systems currently used in the EU fall into this category*." The European Commission used the examples of AI-enabled video games and spam filters.

General Purpose AI

A 'general purpose AI model' is defined under the AI Act as "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", and will include models such as ChatGPT.

General purpose AI models are not automatically classified as high risk under the AI Act, but providers of such AI models will have to comply with specific transparency requirements and EU copyright law, including disclosing that the content was generated by AI, designing the model to prevent it from generating illegal content, and publishing "sufficiently detailed" summaries of the content used as training data (according to a template to be published by the newly formed AI Office).

In addition, general purpose AI models with "*high impact capabilities*" (that is, those general-purpose AI models trained with more than 10^25 floating point operations per second (FLOPs)) are deemed to pose "*systemic risks*". Providers of systemic-risk AI models are subject to additional compliance obligations, including self-assessments and mitigation of systemic risks, reporting of serious incidents, conducting test and model evaluations, as well as cybersecurity obligations. The AI Act also provides for the

development of EU-level "*codes of practice*" for providers of general purpose AI models to facilitate compliance.

Importantly, while the AI Act distinguishes between general-purpose AI models (that may pose systemic risks) and AI systems (that may pose high risk), the regimes are not mutually exclusive. As a result, a general purpose AI model may also qualify as a high-risk AI system if a relevant use-case applies.

The Recitals to the AI Act also clarify that, in relation to the Directive on Copyright in the Digital Single Market (DSM), rights holders may choose to reserve their rights over their copyright works to prevent text and data mining (TDM), unless this is done for the purposes of scientific research. Where the rights to opt out has been expressly reserved in an appropriate manner, providers of general purpose AI models need to obtain an authorisation from right holders if they want to carry out TDM over such works. In other words, the AI Act restates the position under the DSM in the context of generative AI and provides that in the absence of an express opt-out, copyright works that are otherwise freely available on the internet can be extracted for TDM purposes (including, for example, to train foundation models). Therefore, if rights holders wish to protect their copyright from exploitation in generative AI datasets, an express opt-out is essential. On the other side, providers of generative AI models relying on the TDM exception in the training process, will need to ensure that they are not later prevented from deploying the model in other markets without broad TDM exceptions.

Oversight and Enforcement

The AI Act provides for a two-tiered oversight framework, with enforcement at both the EU and Member State level:

- **EU**: The European Commission has overall responsibility for oversight and implementation of the AI Act. The European Commission will be supported by the newly established AI Office, tasked with monitoring, supervising and enforcing the AI Act rules on general purpose AI models across Member States. In addition, the EU AI Board, comprised of representatives from each Member State, will support the European Commission's advisory function by preparing standardized protocols and best practices, in consultation with the AI Office and other EU-level stakeholders.

- **Member States**: Substantive enforcement will be carried out by competent authorities designated by each Member State. Member States are required to establish or designate at least one market surveillance authority (to supervise the

application and implementation of the AI Act) and at least one notifying authority (responsible for assessing and monitoring AI conformity assessment bodies).

Penalties

The AI Act imposes significant penalties for non-compliance:

- up to €35 million or 7% of annual global turnover for prohibited AI practices;
- up to €15 million or 3% of annual global turnover for high-risk system violations, and violations of most other obligations;
- up to €7.5 million or 1.5% of annual global turnover for providing incorrect or misleading information.

Smaller fines apply to SMEs, and (in line with the principles under the GDPR) any penalties shall be effective, proportionate and dissuasive.

Key Implementation Dates

- **2 February 2025**. Prohibition on AI systems posing unacceptable risks.
- **2 May 2025**. Codes of practice to be ready.
- **2 August 2025**. General purpose AI obligations apply.
- **2 August 2026**. General application date; most other obligations (including in respect of high-risk AI systems) apply, with limited exceptions.
- **2 August 2027**. The rules on high-risk AI systems used as a safety component for a product falling under the EU's product safety legislation will apply.

Key Takeaways

- The AI Act comes into force on 1 August 2024, but with phased implementation as set out above.
- All in-scope organizations should conduct an AI audit under which they:

    - assess their role in the AI supply-chain (e.g., “provider”, “deployer”, “importer”, “distributor”, etc.)

    - assess the risk category of their AI systems in accordance with the definitions laid out in the AI Act (e.g., “unacceptable risk”, “high risk”, “general purpose AI without systemic risk”, “general purpose AI with systemic risk” or AI that is subject to transparency obligations)

    - assess their obligations under the AI Act based on the analysis above.

- Having defined its role and risk profile under the AI Act, an organization should conduct an analysis to identify any gaps between its current practice and the AI Act’s applicable compliance obligations.

- Develop a road map to ensure compliance gaps are addressed prior to the relevant obligations coming into effect.

- European and multinational organizations that develop or use AI systems, or that are otherwise caught by the scope of the AI Act, will need to monitor ongoing developments, including codes of practice and best practice guidance published by the European Commission.

Authors

Emma L. Flett

Partner / London

Max Harris

Partner / London

Calum Parfitt

Associate / London

Related Services

Practices

- Technology & IP Transactions

Suggested Reading

- 31 July 2024 Award Kirkland's Intellectual Property Practice Ranked in Managing Intellectual Property's IP Stars 2024
- 26 July 2024 Press Release Kirkland Advises Advent International on Sale of Evri to Apollo
- 25 July 2024 Press Release Kirkland Advises Instructure on Acquisition by KKR for $4.8 Billion