Proskauer

EU's AI Act: Ten Facts for Organisations in the UK and US

November 13, 2024

The EU's AI Act (the "Act") is the world's first comprehensive AI law. The Act manages risks posed by certain AI systems and prohibits certain AI-related practices. UK and US organisations should not assume that the Act does not apply to them; it has a broad extra-territorial scope and imposes high fines for non-compliance.

This briefing summarises at a headline level the key aspects of the Act and the initial steps that UK and US organisations can take towards compliance.

01 / AI systems

02 / Exemptions

03 / In-scope operators

04 / Territorial scope

05 / Risk categorisations

06 / Sanctions

07 / Key dates

08 / EU guidance and delegated acts

09 / Steps towards compliance

10 / Proskauer support

Download Full Report

01 / AI systems

The Act regulates "AI systems". An AI system is defined 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."

AI systems are distinct from traditional software systems and do not include systems that simply follow rules pre-defined by individuals to automatically execute operations. A key part of the Act's definition is the capacity of an AI system to "infer". That is more than basic data processing; it enables learning, reasoning or modelling, typically after deployment of the AI system in its production environment.

An example of an AI system is a software platform that automatically adjusts prices based on demand, competition, and customer behaviour, where that system autonomously infers the best pricing strategies from datasets and adapts to market conditions. In comparison, a traditional CRM system that manages customer information and interactions based on static databases, and requires human direction for operation, would not be an AI system.

Evolving definition: The definition of "AI system" evolved during the drafting and negotiation of the Act. The very first definition referred to different AI techniques and approaches (e.g., reinforcement learning, inference engines, and Bayesian estimation), while the final definition aligns with the OECD's internationally-recognised definition of AI. It is clear from Proskauer's work on a number of Act compliance projects that the final definition of "AI system" captures certain products, features, applications and tools that engineers would not typically characterise as AI.

02 / Exemptions

The Act does not apply to users engaging with AI solely for personal use or to AI systems released under free and open-source licences (unless they deploy prohibited AI practices, constitute high-risk AI systems or trigger specific transparency obligations (**see section 5**). Specific exemptions exist for AI systems used exclusively for military, defence or national security purposes, for AI systems used solely for scientific R&D, and for third-country public authority use of AI systems. Exceptions also apply to research, testing (other than in real-world conditions) and development conducted before an AI system is placed on the market or put into service.

Note that most of the Act does not apply to high-risk AI systems placed on the market or put into service before 2 August 2026 (though this exemption will no longer apply if significant design changes are made to the relevant AI system after that date, e.g., a change of operating system or software architecture). It also does not apply to public sector use cases or AI systems used on certain large-scale union IT systems.

Tracking high-risk AI systems: The 2 August 2026 grace period should not exclude a high-risk AI system from any inventory of AI systems (see **section 9**). Changes to high-risk AI systems need to be tracked as part of ongoing compliance work as, at the tipping point where significant design changes are made, all compliance obligations relating to the high-risk AI systems will apply.

03 / In-scope operators

Subject to the limits of its territorial scope **(see section 4)**, the Act imposes obligations on various categories of organisation:

Providers: These are organisations that develop an AI system, or commission its development, and place it on the EU market or put it into service in the EU under the relevant organisation's name or trade mark (whether for payment or free of charge).

Deployers: These are organisations using an AI system under their authority (except in the course of personal or non-professional use).

Others: These are importers and distributors of AI systems, and manufacturers of products that incorporate AI systems.

Allocation of obligations: The majority of obligations under the Act apply to providers of AI systems. However, mere users can also have meaningful obligations - especially where they are using high-risk AI systems (see **section 5**).

04 / Territorial scope

The territorial scope of the Act captures:

- Providers that place AI systems on the EU market or put them into service within the EU.
- Deployers located in the EU.
- Providers and deployers outside the EU, where outputs of their AI systems are used in the EU.
- Importers in the EU that place on the EU market an AI system bearing the name or trade mark of a person outside the EU.
- Distributors who make an AI system available on the EU market.
- Product manufacturers who place on the EU market, or put into service in the EU, a product incorporating an AI system, under their own name or trade mark.

An organisation can fall into more than one of these categories; most AI developers are both providers and deployers of AI systems.

Non-EU providers of high-risk AI systems subject to the Act must appoint an Authorised Representative located within the EU, who will ensure compliance with the Act and serve as an EU point of contact.

> **Impact of extra-territoriality:** The combination of the worldwide nature of business operations and the Act's broad extra-territorial scope is expected to lead to the Act becoming a de facto global standard for AI regulation. We should also expect future AI-specific laws in the UK and US to be based in part on the principles of the Act.

05 / Risk categorisations

The specific obligations of an in-scope operator depend on: (a) the role of that operator in relation to the relevant AI system (e.g., provider or deployer); and (b) the Act's categorisation of the relevant AI system.

The Act categorises AI systems based on their potential risks and divides them into different categories depending on the data they capture, and the decisions or actions taken with that data.

Prohibited AI practices

AI systems that deploy certain practices are banned, and include AI systems that:

- use subliminal techniques or manipulative or deceptive methods to distort behaviour and impair informed decision-making, causing (or which are likely to cause) significant harm;
- exploit vulnerabilities due to age, disability, or social or economic situations, materially distorting behaviour and causing (or which are likely to cause) significant harm;
- evaluate or classify individuals or groups based on social behaviour or personal characteristics, leading to detrimental or disproportionate treatment in unrelated contexts or unjustified to their behaviour;
- assess the risk of individuals committing criminal offences based solely on profiling or personality traits (with limited exceptions);
- create or expand facial recognition databases through untargeted scraping from the internet or CCTV footage;
- infer emotions in workplaces or educational institutions (with limited exceptions);
- constitute biometric categorisation systems (with limited exceptions); or
- use “real-time” remote biometric identification in public spaces for law enforcement (with limited exceptions).

Manipulative or deceptive methods: An example of a manipulative or deceptive method is an AI system that employs imperceptible audio or visual stimuli to influence consumer choices without the consumer’s knowledge.

High-risk AI systems

Certain AI systems are categorised as high-risk and therefore are subject to requirements around, among other things, risk mitigation, human oversight, documentation, fundamental rights impact assessments, and conformity testing. High-risk AI systems are those AI systems that are intended:

- for use as safety components in products (or are themselves products) that fall under certain EU product safety legislation (listed in Annex I to the Act) and require a third-party conformity assessment before being placed on the EU market or put into service in the EU (e.g., toys, cars, medical devices and lifts); or
- to be used for the use cases listed in Annex III of the Act. This list includes:

permitted biometrics (e.g., remote biometric identification; biometric categorisation; emotion recognition);

critical infrastructure (e.g., supply of utilities; traffic management);

education or job training (e.g., determining access to or level of training; evaluating training outcomes; monitoring prohibited behaviour during testing);

worker engagement (e.g., placing of job advertisements; analysing job applications; evaluating candidates);

worker management (e.g., making decisions affecting worker terms; promotion or termination; monitoring and evaluating performance and behaviour at work);

essential public and private services and benefits (e.g., evaluating individual credit scores; pricing for life or health insurance; prioritising emergency responses);

law enforcement (e.g., use as polygraphs; evaluating reliability of evidence; determining risk of victimisation);

immigration (e.g., detection of persons; assessing security risks; evaluating applications for asylum, visa or residence permits); and

administration of justice and democracy (e.g., influencing election outcomes; assisting judiciary in interpreting facts or law).

However, **except where it involves profiling**, an AI system that is intended for a use listed in Annex III will not constitute a high-risk AI system if it is only intended to perform a narrow procedural task, improve the result of a human-completed task, detect decision-making patterns without influencing a human assessment, or carry out certain preparatory tasks.

Recategorisations: A deployer of a high- risk system can be recategorised as a provider of that AI system in certain circumstances, such as if they place their name on or substantially modify (e.g., materially fine-tune) a high-risk AI system already on the EU market or put into service in the EU. A deployer of an AI system already on the EU market or put into service in the EU that is not classified as high-risk can also be recategorised as the provider of that AI system if they modify the intended purpose of the AI system in such a way that it becomes high-risk.

If you are a UK- or US-based provider of a high-risk AI system that is placed on the market or put into service in the EU, or with outputs that are used in the EU, your obligations will include:

- **appointing an authorised representative** that is established in the EU;
- establishing, implementing, documenting, and maintaining a **risk management system**;
- using training **data sets that are relevant, representative and to the best extent possible free from errors and complete**, and implementing **data governance and management practices;**
- drawing up and maintaining **technical documentation** that demonstrates that the AI system complies with certain requirements, and keeping relevant documentation and automatically-generated logs;
- operating the AI system **transparently** and **providing information** to deployers;
- including measures to enable **human oversight** of the AI system;
- designing and developing the AI system to achieve an appropriate level of **accuracy, robustness, and cybersecurity**, and to **perform consistently**;
- undertaking **conformity assessment** procedures before placing the AI system on the market or putting it into service and drawing up a declaration of conformity;
- putting in place a **quality management system**;
- if your high-risk AI system is listed in Annex III of the Act, **registering** yourself and the AI system in an EU database before placing it on the market or putting it into service;
- affixing the **CE mark** to the AI system or its packaging/accompanying documentation to indicate conformity with the Act;

- establishing, documenting, and implementing a **post-market monitoring system** to monitor compliance with certain of the Act's requirements;
- **reporting serious incidents** to the market surveillance authority; and
- complying with certain **transparency obligations** (see below).

If you are a UK- or US-based deployer of a high-risk AI system with outputs that are used in the EU, your obligations will include:

- using the AI system in accordance with its **instructions for use**;
- assigning **human oversight** of the AI system;
- ensuring that **input data** is relevant and sufficiently representative;
- **monitoring the operation** of the AI system;
- **informing** the provider or distributor and the market surveillance authority and suspending use of the AI system if there is reason to believe use may result in **risk to health, safety, or fundamental rights or if a serious incident is identified**;
- keeping **automatically-generated logs**;
- **performing a fundamental rights impact assessment** in certain circumstances;
- if your AI system is listed in Annex III of the Act, **informing natural persons** that they are subject to the use of a high-risk AI system, and workers of use of the AI system in the workplace;
- **cooperating with relevant competent authorities** in relation to the AI system; and
- complying with certain **transparency obligations** (see below).

Carefully consider which obligations apply: Whether an organisation is a provider or deployer in respect of a AI system depends on the facts and may be difficult to determine. It is essential to carefully analyse whether the obligations on providers, deployers, or neither apply. Misclassification of your role in relation to a high-risk AI system may result in non-compliance, customer challenges and material regulatory sanctions (see **section 6**).

AI systems subject to transparency requirements

The Act designates certain AI systems as presenting specific transparency risks, and so providers and deployers of these AI systems are subject to additional disclosure obligations. These obligations can apply to all types of AI systems (including high-risk AI systems).

The provider of an AI system that:

- is **intended to interact directly with individuals** (e.g., chatbots), must design the AI system so that its users are informed that they are interacting with an AI system (unless obvious from the context); or
- **produces synthetic content** (e.g., image, audio or text generators), must ensure outputs are marked and detectable as artificially generated/ manipulated content (unless the AI system is simply assisting standard editing or making non-substantive alterations to inputs).

The deployer of an AI system that:

- is an **emotion recognition or biometric categorisation AI system** must inform individuals who are subject to the AI system about its operation;
- **generates deepfakes** must disclose that the generated content has been artificially generated or manipulated; or
- **generates or manipulates text that informs the public on matters of public interest**, must disclose that the text is AI-generated or manipulated (unless it has undergone human review or editorial control, and a person holds editorial responsibility for its publication).

Flow-down of obligations: Providers of AI systems are already flowing down various obligations under the Act to deployers of those AI systems. For example, OpenAI's Usage Policies currently flow down OpenAI's transparency obligations under Article 50(1) of the Act by requiring users of OpenAI's API to "ensure that automated systems (e.g., chatbots) disclose to people that they are interacting with AI, unless it's obvious from the context".

General-purpose AI models

The Act includes rules for general-purpose AI models, which are defined (separately from AI systems) as AI models that *"display significant generality, capable of competently performing a wide range of tasks, and suitable for integration into various downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market."*

The Act imposes obligations on providers (rather than deployers) of generalpurpose AI models. If you are a UK- or US-based provider of a general-purpose AI model that is placed on the market in the EU, your obligations will include:

- **appointing an authorised representative** that is established in the EU before placing the generalpurpose AI model on the market;
- drawing up **technical documentation** of the model, including its training and testing process and the results of its evaluation;
- **making available information and documentation** to providers of AI systems who intend to integrate the general-purpose AI model into their AI systems;
- putting in place a **policy to comply with EU copyright law**; and
- making publicly available a summary about the **content used for training** the general-purpose AI model.

Systemic risk: Additional obligations apply if a general-purpose AI model has systemic risk. This is where it possesses high-impact capabilities, such as when the cumulative amount of computation used for its training is greater than 10^25 Floating Point Operations per Second. Systemic risks associated with general-purpose AI models include major accidents, disruptions of critical sectors and serious consequences to public health and safety; negative effects on democratic processes, public and economic security; and the dissemination of illegal, false, or discriminatory content.

06 / Sanctions

Sanctions for non-compliance with the Act are sizeable. In the following circumstances, businesses may be subject to the following fines:

Fines

Violating prohibited AI practice rules: Fines of up to €35 million or 7% of worldwide annual turnover in the previous financial year (whichever is higher).

Violating most other obligations (including high-risk AI system compliance, fundamental rights impact assessments, and transparency obligations): Fines of up to €15 million or 3% of worldwide annual turnover in the previous financial year (whichever is higher).

Providing incorrect information to authorities under the Act: Fines of up to €7.5 million or 1.5% of worldwide annual turnover in the previous financial year (whichever is higher).

SMEs

Fines for SMEs (including start-ups) are capped at the lower of the percentages or amounts applicable to each violation category.

Enforcement

Most enforcement will occur at the national level, with each EU Member State to designate one notifying authority and at least one market surveillance authority. National market surveillance authorities will conduct compliance investigations and enforcement actions (with limited exceptions).

The Act will be enforced against the authorised representatives of UK and US organisations. The Act specifically recognises that authorised representatives are appointed to "enable [the Act's] enforcement" (see **section 4**).

07 / Key dates

1 August 2024: The Act came into force.

November 2024: The first draft of the Codes of Practice (the technical guidelines for general purpose AI model compliance with the Act) is expected to be published.

2 February 2025: Prohibited AI practices are banned, and general provisions (e.g., requirements relating to AI literacy) apply.

2 May 2025: Finalised Codes of Practice will be published.

2 August 2025: Obligations on providers of general-purpose AI models take effect, and Member States must have appointed their notifying authorities and bodies. Annual EU Commission review of, and possible legislative amendments to, the list of prohibited AI practices.

2 August 2026: Obligations go into effect for high-risk AI systems specifically listed in Annex III. Member states to have implemented rules on penalties and to have established at least one operational AI regulatory sandbox. Commission review of the list of highrisk AI systems.

2 August 2027: Obligations go into effect for high-risk AI systems that are intended to be used as a safety component of a product. Obligations go into effect for high-risk AI systems in which the AI itself is a product and the product is required to undergo a third-party conformity assessment under certain EU laws (e.g., toys, radio equipment, and civil aviation security).

By end of 2030: Obligations go into effect for certain AI systems that are components of the large-scale IT systems established by EU law in the areas of freedom, security and justice (e.g., the Schengen Information System).

Working towards compliance: While the Act has a staggered implementation over a prolonged period, it is important to start working towards compliance now. Proskauer's experience on Act compliance projects indicates that some organisations already satisfy certain compliance requirements. However, a full gap analysis to identify and address any holes in compliance is critical. See **sections 9** and **10** for more information.

08 / EU guidance and delegated acts

While the Act is detailed, further guidance will be provided throughout its staggered implementation. In particular, the Act provides that the EU Commission can issue the following guidance on the following matters:

By 2 August 2025

High-risk AI system incident reporting.

By 2 February 2026

Practical implementation of high-risk AI system requirements (with examples of high-risk and not high-risk use cases).

When deemed necessary

Prohibited AI practices; application of the definition of an AI system; requirements for high-risk AI systems; practical implementation of transparency obligations; relationship of the Act and its enforcement with other EU laws.

The EU Commission can also issue delegated acts on:

- ???the definition of AI systems;
- ???criteria and use cases for high-risk AI systems;
- ???thresholds for general-purpose AI models with systemic risk;
- ???technical documentation requirements for general-purpose AI systems;
- ???conformity assessments; and
- ???EU declaration of conformity.

The EU Commission's power to issue delegated acts lasts for a period ending on 2 August 2029 and is extendable for another 5 years.

Should the Commission adopt any delegated acts, it will do so after consulting expert groups. Citizens and other stakeholders will also be invited to provide feedback on the draft texts of the relevant delegated acts.

We recommend that organisations closely monitor the EU Commission's activity in relation to delegated acts, and consider participating in opportunities to provide feedback on draft texts.

Ongoing monitoring: The complexities of the Act, the issuing of additional guidance and the emergence of new AI systems means that compliance with the Act will be an ongoing, long-term process for many organisations. The monitoring of guidance and delegated acts will be important to ensure compliance steps are relevant and accurate.

09 / Steps towards compliance

Businesses should work towards compliance with the Act now. This will limit the need for future compliance-driven re-engineering of products, services and internal systems; recrafting of internal processes; and re-education of staff. It will also allow businesses to avoid taking on unnecessary risk in a rush to achieve compliance by applicable deadlines. The promotion of fair and safe use of AI can have a positive effect on relationships with customer bases and stakeholders, too.Businesses should consider the following 5 steps towards compliance:

1 / Inventory

Prepare an inventory of the AI systems that the business uses and the AI systems that the business has developed. Document the Act's categorisation of the AI systems (including whether they are high-risk or trigger any transparency requirements) and the role of the business in relation to them (e.g., provider or deployer).

2 / Gap analysis

Conduct a gap analysis of the Act's requirements against the current practices of the business (including documentation and operational and technical controls). Be sure to monitor guidance, delegated acts, and codes of practice so that this gap analysis is up-to-date. Such monitoring could be facilitated by membership of the "AI Pact" network, which encourages early compliance with the Act's requirements and the exchange of best practices and compliance information.

3 / Proprietary AI systems—Ongoing compliance

In relation to any changes to how the business uses its existing proprietary AI systems—or in relation to any new proprietary AI systems that it is developing—build relevant Act categorisation exercises, compliance assessments and requirements into use-case determination and development processes (including, if appropriate, guidelines to help avoid application of the Act).

4 / Third party AI systems—Ongoing compliance

In relation to changes to the use of existing third-party AI systems—or in relation to new third-party AI systems to be procured—build relevant Act categorisations and compliance assessments into use-case determination, intake and procurement processes (including, if appropriate, guidelines to help avoid application of the Act or any provider re-categorisation).

5 / Training and trustworthy AI

Train personnel on applicable requirements under the Act, including relevant categorisations, assessments and requirements, so they understand the importance of new business processes and controls. Consider implementing "trustworthy AI" principles in the development and use of AI systems to reflect emerging market standards on transparent and ethical use of AI.

Taking a proactive approach: Familiarity with, and understanding of, the Act among most of the public (and even some lawyers) is low. Therefore, even for organisations that do not expect to have any obligations under the Act, completion of these five steps can provide value by demonstrating to investors, regulators, and customers that the organisation is taking a proactive, safety- first approach to the Act.

10 / Proskauer support

Proskauer's lawyers are experts in AI law, policy and practice. We regularly advise new entrants and established players in the AI market on their formulation and execution of key strategies, and their management and mitigation of AI-specific risks. Our clients range from well-known model developers and corporate end-users, to training data rightsholders and businesses whose vendors are integrating AI into existing services. We offer technical excellence in the law, as well as practical advice based on a wealth of real experience.

Recent examples of our team's work include advising a:

- Series of Private Equity Businesses on their assessment, procurement and use of generative AI tools, include Anthropic's Claude, Amazon's Q Developer and

Microsoft’s Copilot and Azure OpenAI Service

- Series of Venture Capital Businesses on their minority investments in AI startups and associated commercial partnerships, including AI-specific diligence; and their assessment, procurement and use of generative AI tools
- Global Delivery Organisation on its automation strategy, including its development of discriminative AI models and deployment of generative AI systems, including OpenAI’s API and elements of Slack
- Leading Tech Organisation on its generative AI deployment, including its enterprise licensing deal with OpenAI, and its use of ChatGPT, Google Gemini and Github Copilot
- Global Media Business on strategies related to its use of generative AI, including in connection with talent NIL, and the protection of its brand assets from unauthorised use in generative AI
- Leading E-billing Platform on its AI strategy, including customer communications relating to its training of categorisation models using customer data and its deployment of generative AI tools
- Global Leader in Market Research on its development of multiple generative AI software products for internal and customer use, and its compliance with the EU’s AI Act
- Listed Tech Unicorn on its lobbying efforts in relation to the EU’s AI Act, and subsequent compliance project (including relating to high-risk AI systems)
- Leading Trading Software Providers on the incorporation of third party AI systems into their customer product stacks, including to create combined discriminative and generative AI products
- Global AI Research House on the establishment and support of a joint venture for the commercialisation of therapeutic AI tech
- Transatlantic AI Business on the IP and tech aspects of its relationship with its parent, including licensing relating to the ethical use of AI

AI Summary

For a convenient summary of the key issues discussed in the briefing, listen to the short podcast below. Please note that this podcast was generated by AI and may contain errors or omissions. For a complete and detailed analysis, please refer to the full briefing.

Related Professionals

Oliver R. Howley

Partner

Kelly M. McMullon

Special International Labor, Employment & Data Protection Counsel

Peter J. Cramer

Associate