EU Artificial Intelligence Act

TaylorWessing

Purpose
The EU AI Act sets out a legal framework for the development, marketing, and use of artificial intelligence in the EU to:

- Ensure AI systems in the EU market are safe and comply with fundamental rights.
- Ensure legal certainty for AI investment and innovation.
- Enhance governance and enforcement of laws on AI safety and fundamental rights.
- Foster a single market for trustworthy AI applications to prevent fragmentation.

Scope
The AI Act regulates EU market AI **providers** and **deployers**, excluding military and exclusive scientific research uses. The Regulation does not apply until the systems are put into service or placed on the EU market. Importers, distributors and product manufacturers also have obligations.

What is an AI system?
An '**AI system**' is a machine-based system, operating with autonomy levels and exhibiting adaptiveness, designed to generate outputs like predictions or decisions from inputs, influencing environments.

Exceptions
Exceptions apply for free and open source software, AI systems used for testing and development or for scientific use, national security, AI for personal use and minimal risk AI.

Application
The AI Act will come into force on **1 August 2024** with compliance phased in over a three year period. The compliance deadline for the bulk of obligations is **2 August 2026**. See timeline for more.

Key concepts of AI systems and models under the AI Act	**Prohibited AI:** AI systems that manipulate decisions, exploit vulnerabilities, evaluate social behaviour or personal traits, predict criminal behaviour, scrape facial images, infer emotions in workplaces or educational settings, and categorize people based on biometric data. Exceptions are made for law enforcement purposes, such as finding missing persons or preventing terrorist attacks. **High-risk AI systems:** systems that could significantly affect people's safety or fundamental rights. Examples include AI in critical infrastructure, education, employment, public services, law enforcement, and emergency call systems. Certain AI uses like biometric identification and recommender systems for large platforms (unless covered by other legislation) are also included. **General-purpose AI model (GPAI):** an AI model trained with extensive data using self-supervision, capable of performing diverse tasks and integrating into various applications, excluding models used solely for research, development, or prototyping before marketing.
Obligations for all AI systems	Providers must register themselves and their low-risk and/or high-risk AI systems in the EU database before use. Both providers and deployers must inform users when interacting with an AI system, unless obvious or the system is used to detect crimes. AI systems generating synthetic content must mark outputs as artificial. They must also disclose AI use in emotion recognition or biometric categorization, except when the system is used to detect crimes. The AI Office will provide guidelines for detecting and labelling such content.
Obligations on providers of high-risk AI	Providers must ensure compliance with safety, transparency, and human oversight standards, implement continuous risk management, and maintain high-quality data sets. They must prepare detailed technical documentation, keep event logs, provide clear user instructions, and mark products with CE markings. A quality management system is required, and documentation must be retained for ten years. In case of non-compliance, providers must take corrective actions and inform relevant authorities. Non-EU providers must appoint an EU representative, register high-risk AI systems in the EU database, and establish a post-market monitoring system. Non-EU providers must appoint an EU representative. Deployers must ensure transparency, assign human oversight, maintain data logs for six months, assess fundamental rights impacts, report risks, and ensure system registration. Public bodies and private entities must perform impact assessments and follow AI Office guidelines. Affected individuals have the right to an explanation of AI decisions.
Obligations for deployers of high-risk AI	Deployers have a range of safety duties relating to high-risk AI systems. They must operate the systems according to provided instructions and assign human oversight to monitor the AI's performance. The input data should be relevant and accurate and kept secure, and deployers must actively monitor the system's operation for any potential risks. If a risk is detected, it must be promptly reported to the provider and the appropriate authorities. Deployers are required to maintain logs generated by the AI system for a minimum of 6 months. Prior to system deployment, workers must be adequately informed. It is imperative that only AI systems registered in the EU database are used. Deployers must also conduct Data Protection Impact Assessments and Fundamental Rights Impact Assessments and fully cooperate with relevant authorities in addition to complying with a variety of other governance requirements.
General-purpose AI models (GPAI)	The EU AI Act imposes specific rules for general-purpose AI (GPAI) models, including those posing systemic risks. GPAI models must maintain up-to-date technical documentation, ensure transparency, respect Union copyright laws using advanced technologies, and provide a public summary of training content. Non-EU providers must appoint an EU representative, although open-source models are exempt from some obligations. Systemic-risk GPAI models, defined by high computational power and potential significant impacts, must notify the European Commission, assess and mitigate risks, ensure cybersecurity, and report serious incidents. Providers of GPAI models will be presumed to comply where they adhere to European harmonized standards or relevant codes of practice, but will need to demonstrate compliance by alternative means if they choose not to do so.
Penalties	The AI Act imposes penalties for non-compliance: up to €35 million or 7% of annual global turnover for prohibited AI practices; up to €15 million or 3% for high-risk system or GPAI-Provider violations; and fines of up to €7.5 million or 1% for providing incorrect or misleading information. Smaller fines apply to SMEs and Union institutions, bodies, offices and agencies.
Governance	The governance structure for the EU AI Act includes the AI Office, AI Board, Advisory Forum, Scientific Panel, Notifying Authorities, Notified Bodies, and Market Surveillance Authorities. The AI Office, centralized within the DG-CNECT, harmonizes implementation, supports regulatory sandboxes, monitors GPAIs, and cooperates with stakeholders. The AI Board, with representatives from each Member State and observers from the AI Office and European Data Protection Supervisor, ensures consistent application, coordinates national authorities, and issues recommendations. The Advisory Forum provides technical expertise and prepares opinions, while the Scientific Panel offers advice on systemic risks and develops evaluation tools. Notifying Authorities process applications and monitor conformity assessment bodies (CABs), ensuring no conflicts of interest. Notified Bodies verify high-risk AI systems' conformity and issue certifications. Market Surveillance Authorities investigate non-compliance, oversee real-world testing, manage incident reports, and support SMEs and start-ups.
Timeline	The EU AI Act will be enforced in stages: **6 months** for prohibited AI systems, **12 months** for GPAI, **24 months** for high-risk AI systems under Annex III, and **36 months** for high-risk AI systems covered by legislation in Annex I, with codes of practice due in 9 months. Key milestones include the first AI Board meeting in July 2024 and full compliance by August 2026 (subject to exceptions). National regulatory authorities (which must be set up by August 2025) and the Scientific Panel will oversee implementation and compliance.
Additional key definitions	**Provider:** develops or has an AI system developed and is responsible for ensuring its compliance with the AI Act before it is marketed or put into service. **Deployer:** uses an AI system under their authority (excluding personal, non-professional use) and ensures it operates in compliance with the AI Act. **Importer:** places AI systems from outside the EU on the market, ensuring these systems meet all AI Act requirements, including conformity assessments. **Distributor:** responsible for making AI systems available on the EU market, ensuring they comply with the AI Act before distribution. **Product Manufacturer:** integrates AI systems into products governed by specific EU legislation, ensuring compliance with both the AI Act and applicable sectoral laws. **Authorised Representative:** acts on behalf of a provider, managing compliance with the AI Act's obligations within the EU. **Operator:** any stakeholder (provider, manufacturer, deployer, representative, importer, or distributor) involved in the operation of AI systems, responsible for maintaining compliance during operational use. **General-purpose AI system:** an AI system based on a general-purpose AI model that has the capability to serve a variety of purposes both for direct use as well as integration in other AI systems.