The EU AI Act: Quick Guide

A quick summary of the final text of the EU's ground-breaking AI Act, its key provisions and the timeline for compliance.

What is the AIA?

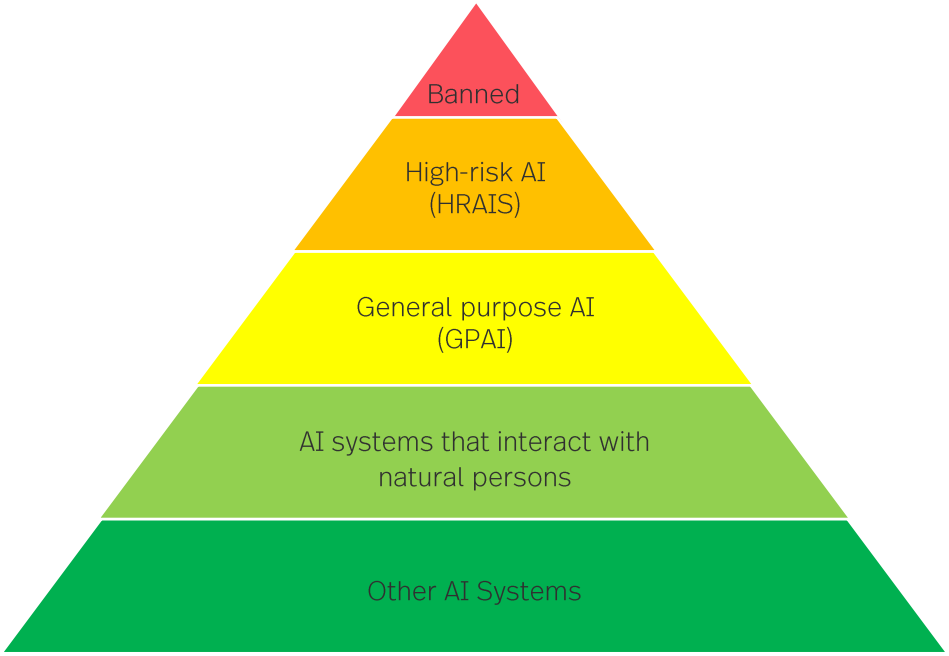
The EU AI Act (**AIA**) is the EU's flagship new artificial intelligence regulation. The final text of the AIA was approved on 2 February 2024. Following its formal adoption and entry into force, the AIA will have a significant impact on organisations developing or using AI, both in the EU and further afield.

The AIA will place risk- and technology-based obligations on organisations that develop, use, distribute or import AI systems in the EU, coupled with high fines for non-compliance (up to EUR 35 million or 7% of global annual turnover).

How will the AIA apply?

The application of the AIA depends on the AI technology involved, the use case and the role of the operator. The approach is broadly risk-based:

- AI systems for certain uses will be **prohibited**.
- Certain AI systems will be designated as **high-risk AI systems (HRAIS)** and subject to extensive obligations, especially for providers.
- There will be specific provisions governing **general purpose AI (GPAI)** models, including foundation models and generative AI.
- Other AI systems are considered low risk. These AI systems will be subject only to limited transparency where they interact with individuals.



When will the AIA apply?

The AIA is expected to be formally adopted following a vote in the European Parliament in Q2 2024. It will then enter into force on publication in the official journal.

Most provisions in the AIA will apply after a **two-year implementation period**. During this period, various supporting delegated legislation, guidance and standards will be published to assist with AIA compliance.

This 2-year timeline is subject to some important exceptions: The **prohibitions** on certain AI systems will come apply after **6 months**, while the requirements for **GPAI** will apply after **12 months**.

The EU AI Act: Quick Guide

Definition of AI systems, AI systems prohibited under the EU AI Act and AI systems designated as high-risk under the EU AI Act.

Definition of AI system

Most of the obligations under the AIA concern **AI systems**. The definition of AI system is: "*a machine-based system 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*".

The obligations for GPAI will also apply to certain general purpose AI models, which can underly a large range of different AI systems.

Prohibited AI Systems

The AIA will prohibit the use of certain types of AI system. The prohibitions will include (among other things):

- Certain AI systems for **biometric categorisation and identification**, including those for untargeted scraping of facial data from the internet.
- AI systems that deploy **subliminal techniques**, **exploit vulnerabilities** or **manipulate human behaviour** to circumvent fundamental rights or cause physical or psychological harm.
- AI systems for **emotion recognition** in law enforcement, border management, the workplace and education.
- AI systems for the **social scoring** evaluation or classification of natural persons or groups thereof over a period of time based on their social behaviour.

High-risk AI Systems (HRAIS)

The most onerous regulatory obligations under the AIA attach to high-risk AI systems or 'HRAIS'. These are AI systems in areas covered by existing EU product safety legislation, as well as those intended to be used for certain purposes, particularly in the following domains:

- AI systems used as safety components in the management and operation of essential public infrastructure e.g. **water, gas and electricity** supplies.
- AI systems used to determinate access to **education** institutions or in assessing students e.g. AI systems used to grade exams.
- AI systems used in **recruitment and employment** e.g. for placing job advertisements, scoring candidates or reviewing job applications, promotion or termination decisions or in reviewing work.
- AI systems used in migration, asylum and border control management or in various other **law enforcement** and judicial contexts.
- AI systems used for influencing the outcome of **democratic processes** or the voting behaviour of voters.
- AI systems used in the **insurance and banking** sectors.

The EU AI Act: Quick Guide

Substantive and procedural regulatory obligations for AI systems designated as high-risk under the EU AI Act.

- The list of high-risk AI systems is not closed and may be supplemented in future as further high-risk uses for AI emerge.
- The HRAIS obligations summarised below apply principally to **providers** of AI systems, rather than other operators. Providers are likely to be those who develop or procure an AI system with a view to placing it on the market or putting it into service under their own name or trademark.
- Other operators (including **deployers**, **distributors** and **importers**) are also subject to lesser obligations. Other operators may also be deemed to be providers in certain circumstances e.g. if they substantially modify a HRAIS or put it into service in their own name.
- HRAIS providers will be subject to extensive substantive obligations in relation to their HRAIS, including:
  - **Risk management system:** implementing process(es) for the entire lifecycle of the HRAIS to identify, analyse and mitigate risks.
  - **Data and data governance measures:** training and testing of HRAIS must be undertaken in accordance with strict data governance measures.
  - **Technical documentation:** drafting a comprehensive "manual" for HRAIS which contains specific minimum information.
  - **Record-keeping:** HRAIS must be designed to ensure automatic logging of events including e.g. period of use, input data, and these must be kept by the providers for defined periods.
  - **Transparency:** HRAIS must be accompanied by instructions for use which include detailed information regarding their characteristics, capabilities and limitations.
  - **Human oversight:** HRAIS must be designed so they can be overseen by humans, who should meet various requirements e.g. being able to understand the HRAIS ('AI literacy') and to stop its use.
  - **Accuracy, robustness and cybersecurity:** HRAIS must be accurate (with accuracy metrics included in instructions for use), resilient to errors or inconsistencies (e.g. through fail-safe plans) and resilient to cyber-attacks.
  - **Quality management system:** HRAIS providers must put in place a comprehensive quality management system.
  - **Post-market monitoring:** HRAIS providers must document a system to collect and analyse data provided by users on the performance of the HRAIS throughout its lifetime.
- HRAIS providers will also be subject to various procedural obligations before they supply any HRAIS:
  - **CE marking:** Providers must ensure their HRAIS undergoes a conformity assessment procedure before the HRAIS is supplied and affix a CE mark to its documentation.
  - **Registration in EU database:** Providers and public bodies using HRAIS must register the HRAIS in an EU-wide database of AI systems.
  - **Reporting obligations:** HRAIS providers must report serious incidents or malfunctioning involving their HRAIS to a relevant authority within 15 days.

The EU AI Act: Quick Guide

Regulation of general purpose AI, regulation of lower-risk AI systems and penalties for non-compliance.

Other operators of HRAIS will be subject to more limited obligations, such as to complete fundamental rights impact assessments, ensure they use the HRAIS in accordance with its instructions of use, to monitor the operation of the HRAIS and to keep a record of the logs generated by the HRAIS (if under their control).

General Purpose AI

AI technologies which are not prohibited or high-risk will be subject to much less onerous regulatory requirements.

The most onerous other requirements under the AIA attach to **general purpose AI (GPAI)**. The requirements for most GPAI models, which includes foundation models and generative AI models, are chiefly focussed on transparency.

The obligations for all GPAI will include issuing technical documentation, compliance with EU copyright law and providing summaries of the training data.

The final text includes additional requirements for GPAI that is trained on extensive data sets and exhibits superior performance; this is based on the potential systemic risks that these AI models may pose across the value chain (**GPAI with systemic risk**).

Any GPAI model with systemic risk will be subject to additional requirements that are expected to include:

- Stringent **model evaluations**, including adversarial testing/red-teaming.
- Assessing and **mitigating possible systemic risks** from use of the GPAI.
- Greater **reporting** obligations to regulators, particularly where serious incidents occur.
- Ensuring adequate **cybersecurity** for the GPAI with systemic risk.
- Reporting on the **energy efficiency** of the GPAI.

Other AI systems

Save for the above, and where two specific exemptions apply (military or defence; research and innovation), the only binding requirement for other AI systems is a limited obligation of **transparency**: providers must ensure that AI systems that are intended to interact with individuals are designed and developed in such a way that individual users are aware that they are interacting with an AI system.

The final text of the AIA does *not* include the European Parliament's proposed **general principles** for AI that appeared in an earlier draft of the AIA. However, these high-level principles still sit behind many of the AIA's provisions.

Financial penalties

The penalties that will apply under the AIA are expected to be very significant, ranging from €7.5m (or 1.5% global annual turnover) to €35m (or 7% global annual turnover) for the preceding financial year, depending on (i) the type of infringement and (ii) the size of the company.

How we can help

How can we help?

We can help you comply with the AIA in the following ways:

- Providing legal and regulatory advice on the scope and application of the AIA, including delivering an impact or risk assessment.
- Helping you to achieve compliance with the requirements of the AIA to future-proof your AI systems for this important regulation.
- We also deliver regular training sessions on the AIA which we would be happy to tailor for your organisation.

We have developed an AI Toolkit, setting out the ways in which we can help your organisation deal with AI-related legal issues.

We are one of the leading AI law firms

Simmons has a thriving AI law practice. Our AI Group comprises around 100 lawyers and non-lawyers in different practices and jurisdictions.

- Our Global AI Lead, Minesh, is Chair of the Society for Computers and Law (SCL) AI Group and Chair of the City of London Law Society (CLLS) AI Committee.
- Members of our AI Group have contributed to the leading AI law textbooks: *Artificial Intelligence Law and Regulation* (Elgar, 2022), *Artificial Intelligence in Finance* (Elgar, 2023) and the next edition of *The Law of Artificial Intelligence* (Sweet & Maxwell) (forthcoming)).
- Members of our AI Group are regularly invited to speak at AI conferences, including on behalf of the United Nations and at the prestigious CogX AI conference.
- Our ground-breaking work on the world's first AI Explainability Statement to receive input from a regulator (the UK's Information Commissioner's Office) was shortlisted at the *Legal Innovation Awards 2022* and the *Financial Times Innovative Lawyers Awards Europe 2022*.
- Through our Wavelength offering, we have a team of data scientists who can offer practical insight on AI.

We have advised:

- a **global bank** on AI regulation, including the AIA.
- one of **the world's largest developers of biometric technology** on a response to the European Commission's draft AIA proposal.
- a **'big tech' company** on the interpretation and application of the AIA, including drafting proposed changes.
- a **large financial institution** on contentious contractual issues arising out of a collaboration agreement for the joint development of AI technology.
- a **global chip manufacturer** on its AI regulatory compliance framework, including for the AIA.
- a **'big tech' company** on regulatory investigations relating to its AI products.
- a **leading global alternative investment management platform** on the disposal of its stake in an AI company.
- a **leading software developer / provider to financial institutions** on a digital sandbox tool to assist data synthesis in machine learning.
- an **AI app developer** on data privacy issues, including undertaking a data privacy impact assessment and liaising with the data protection regulator.
- one of **the world's largest biopharmaceutical companies** on collaboration and licensing agreements to develop and use AI models.
- one of **the world's largest online supermarkets** in its development of AI-powered smart platforms and robotics systems.
- an **Israeli unicorn** involved in biometric and medical AI products on its expansion and potential IPO.
- a **global telecoms provider** on an AI system used to predict healthcare issues for its customers.
- a **global technology company** on a cooperation agreement with Mercedes Benz on autonomous vehicles.