AI Act: Quick Guide

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

What is the AIA?

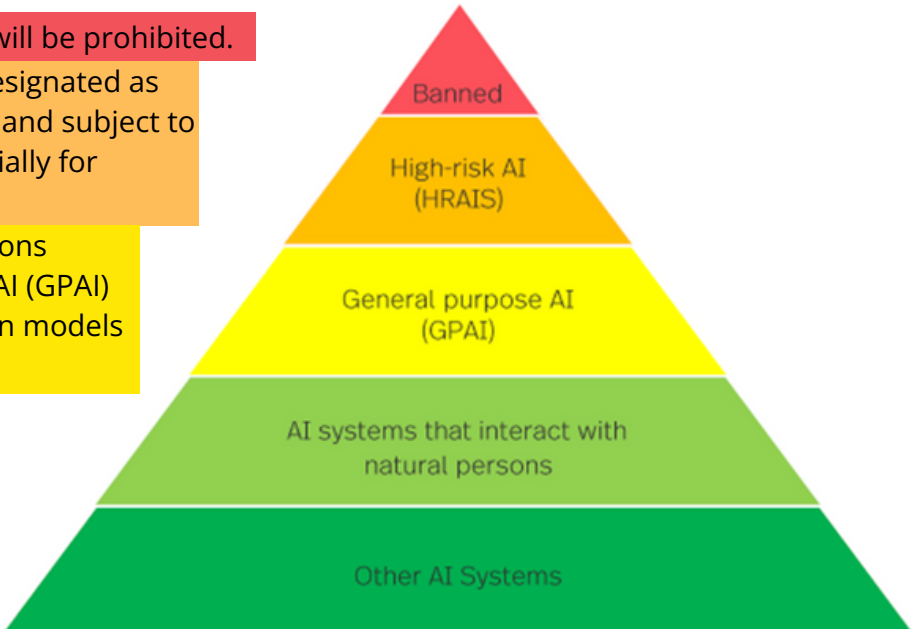
The EU AI Act (**AIA**) is the EU's flagship new artificial intelligence regulation. The most likely final text of the AI Act was adopted by the Committee of the Permanent Representatives of the Governments of the Member States to the European Union (COREPER) on 2 February 2024 and by the relevant committees of the European Parliament (IMCO, LIBE) on 13 February 2024. Once formally adopted by the European Parliament in plenary and entered 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 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 upon publication in the official journal.

Most provisions of the AIA will apply after a **2-year implementation period**. During this period, various supporting delegated legislation, guidance and standards will be published to assist with AIA compliance.

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

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.

Prohibited AI Systems

The AIA will prohibit the use of certain types of AI systems. 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 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 extensive 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 (ANNEX II), as well as those intended to be used for certain purposes, particularly in the following domains (ANNEX III):

- AI systems used as safety components in the management and operation of essential public infrastructure e.g. **water, gas and electricity** suppy (critical infrastructure).
- AI systems used to determine access to **educational** 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 that are used to assess the **creditworthiness** of natural persons or to classify the risk of natural persons in the area of life and health insurance.

The list of high-risk AI systems is not exhaustive and may be supplemented in the future as further high-risk uses of 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 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 to be overseen by humans, who should meet various requirements, such as the ability to understand the HRAIS ('AI literacy') and to terminate 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 have a comprehensive quality management system in place.
- **Post-market monitoring:** HRAIS providers must document a system for collecting and analysing data provided by users on the performance of the HRAIS throughout its lifetime.

HRAIS providers will be subject to various procedural obligations before can they supply a HRAIS:

- **CE marking:** Providers must ensure that 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 malfunctions involving their HRAIS to a relevant authority within 15 days.

Other operators of HRAIS will be subject to more limited obligations, such as completing a fundamental rights impact assessment, ensuring that they use the HRAIS in accordance with its instructions of use, monitoring the operation of the HRAIS and keeping a record of the logs generated by the HRAIS (if under their control).

General Purpose AI (GPAI)

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

The most extensive other requirements under the AIA relate to **general purpose AI (GPAI)**. The requirements for most GPAI models, which include foundation models and generative AI models, are primarily focused 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 datasets and exhibits superior performance (high impact capabilities). 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

Apart from the cases mentioned above and apart from the cases excluded from the scope of the AI Act (military/defence; scientific research and development), 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.

Sanctions

The sanctions to be applied under the AIA will depend on the type of infringement and the size of the company. Fines can range from EUR 7.5 million (or 1.5% of global annual turnover) to EUR 35 million (or 7% of global annual turnover) for the preceding financial year.

The content of this Quick Guide has been kindly **provided by Simmons & Simmons.** Simmons & Simmons is one of the leading international law firms in the field of AI, with, amongst others, offices in Germany, France, Italy, Spain and London. Simmons & Simmons advises on legal and regulatory issues relating to the scope and application of the AIA, including delivering an impact or risk assessment. Simmons & Simmons is a partner of the German AI Association.

In case of questions, do not hesitate to contact: **Christopher Götz, LL.M.** (christopher.goetz@simmons-simmons.com).

The European AI Forum (the umbrella organisation of nine European national AI associations and clusters) thanks Simmons & Simmons for providing the content.