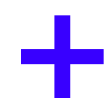




AI ACT QUICK GUIDE



Interactive PDF
optimised for desktop



WHAT IS THE EU AI ACT?

The EU AI Act is Europe’s flagship “risk based” AI regulation, having direct effect in all 27 EU Member States. It sets certain standards for AI regulation in other jurisdictions, much in the same way that the EU’s GDPR is used as a global benchmark for data privacy.

The AI Act takes a “**risk-based approach**” – the higher the risk, the stricter the rules. AI systems that pose an “unacceptable risk” are prohibited, while stringent regulatory requirements will be imposed on “high-risk” AI systems and General Purpose AI models when those provisions come into effect. Conversely, “limited risk” and “minimal risk” AI systems are subject to simpler transparency obligations.

The Commission has launched a [Single Information Platform](#) to help organisations understand and comply with the AI Act. The platform serves as an accessible, up-to-date information hub offering clear guidance on the AI Act’s application, FAQs, a compliance checker, and an [AI Act Service Desk](#).

WHEN WILL THE AI ACT APPLY?

The AI Act became law on **1 August 2024**, with its operative provisions due to come into effect after a 24-month lead in period on **2 August 2026**, except for the following provisions which entered into application over a progressive timeline:

- + The prohibitions on specified categories of AI (Unacceptable Risk AI Systems) came into force after six months on **2 February 2025**.
- + The provisions on General Purpose AI Models come into force after 12 months on 2 August 2025 (applicable to those not already on the market.)

The application of certain key provisions has been delayed pursuant to the Digital Omnibus on AI, with the following deferred deadlines now applying:

- + obligations on High-Risk AI Systems in Annex III apply from **2 December 2027**.
- + obligations on High-Risk AI Systems in Annex I apply from **2 August 2028**.

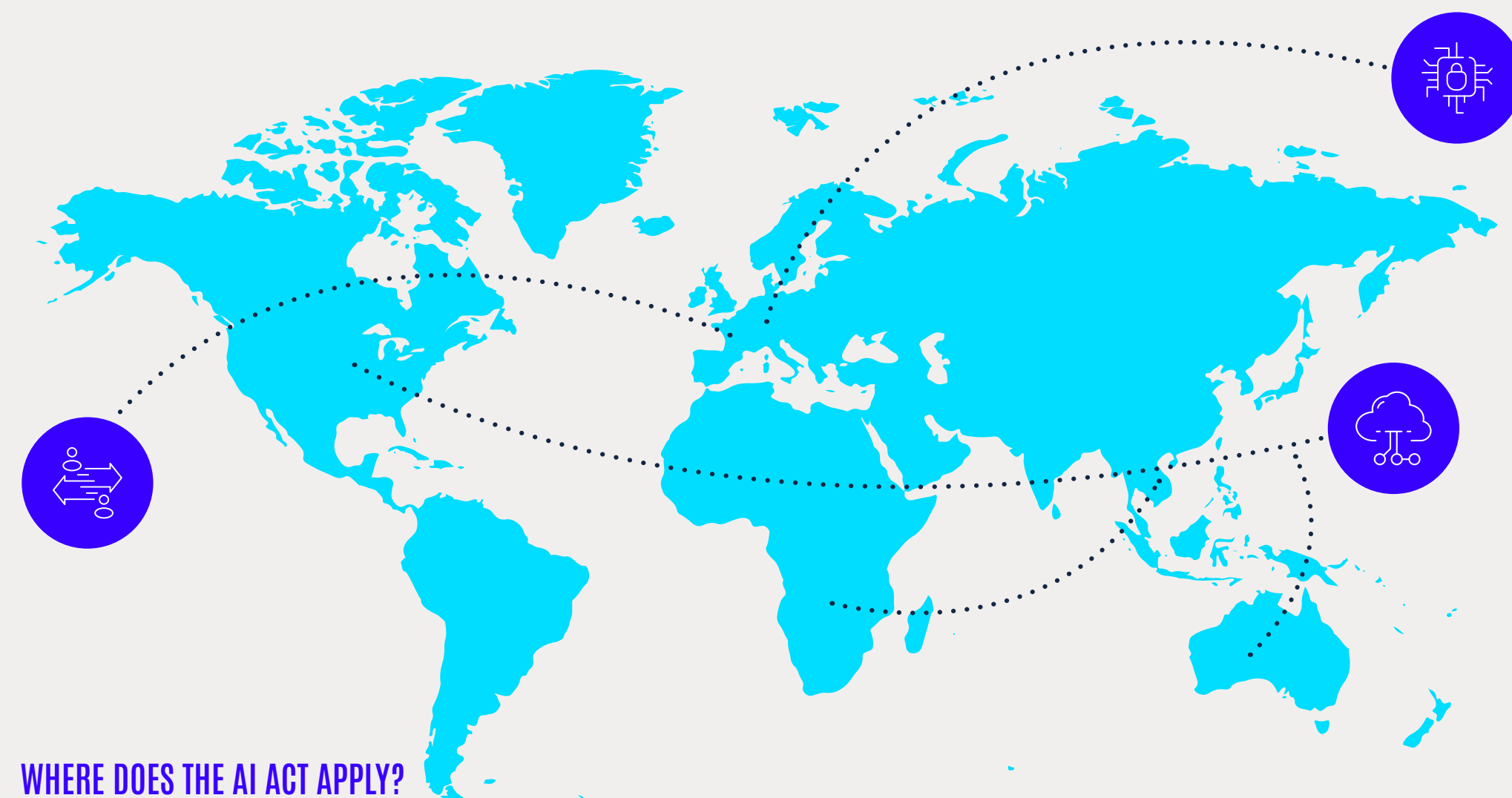
AI ACT APPLICATION

WHAT DOES THE AI ACT APPLY TO?

The AI Act applies to AI systems, being “a machine-based systems 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 received, how to generate output such as content, predictions, recommendations, or decisions, that can influence physical or virtual environments”. This tracks the OECD definition and excludes “simpler software systems”.

WHO DOES THE AI ACT APPLY TO?

The most onerous requirements under the AI Act apply to “providers” of AI systems, being organisations that develop AI systems or General Purpose AI models. However, other AI system operators (importers, distributors, deployers), and other third parties are also subject to strict compliance obligations. “Providers” include organisations that have AI systems developed for them and place them on the market (or otherwise put them into service) under their own name or trademark.



WHERE DOES THE AI ACT APPLY?

The AI Act has a wide extraterritorial scope, with a focus on where the impact of the AI system occurs within the EU, regardless of the location of the provider or user.

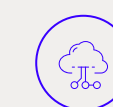
It applies to:



providers that place or put AI systems into service in the EU (irrespective of where they are established)



deployers, importers and distributors of AI systems established or located in the EU



providers and deployers outside of the EU where the output of the AI system is used in the EU (or intended to be used in the EU)

WHAT ARE THE KEY AI ACT OBLIGATIONS?

The AI Act takes a “risk-based approach”
– the higher the risk, the stricter the rules.



PROHIBITED AI

Certain particularly harmful AI systems are prohibited and cannot be placed on the market or put into service (Unacceptable Risk AI Systems). This category includes AI systems that use “subliminal techniques beyond a person’s consciousness”, exploit the vulnerabilities of a specific group of persons, or are used for social scoring (classifying people based on their social behaviour, socio-economic status, personal characteristics). Certain biometric categorisation, biometric identification and facial recognition uses will also be prohibited.



HIGH-RISK AI

The most onerous AI Act obligations apply to high – risk AI systems (High-Risk AI Systems), which include AI used in product safety, certain biometrics technologies, recruitment and employment, essential public infrastructure (utilities) or the insurance and banking sectors.

Key obligations include:

- + putting in place robust risk management systems to analyse and mitigate risk
- + ensuring they are accurate and resilient to errors and cyber threats
- + undertaking fundamental rights impact assessments
- + making available instructions for use and transparency information (including on capabilities and limitations)
- + ensuring a level of human oversight
- + monitoring its use over its lifetime
- + maintaining technical documentation, keeping detailed records, and demonstrating compliance via conformity assessments.



GENERAL PURPOSE AI

This covers AI that is not prohibited or high-risk (General Purpose AI Models) and includes foundation models and generative AI (with additional obligations applying to those that are trained on extensive data sets, and pose “systemic risks” due to their superior performance).

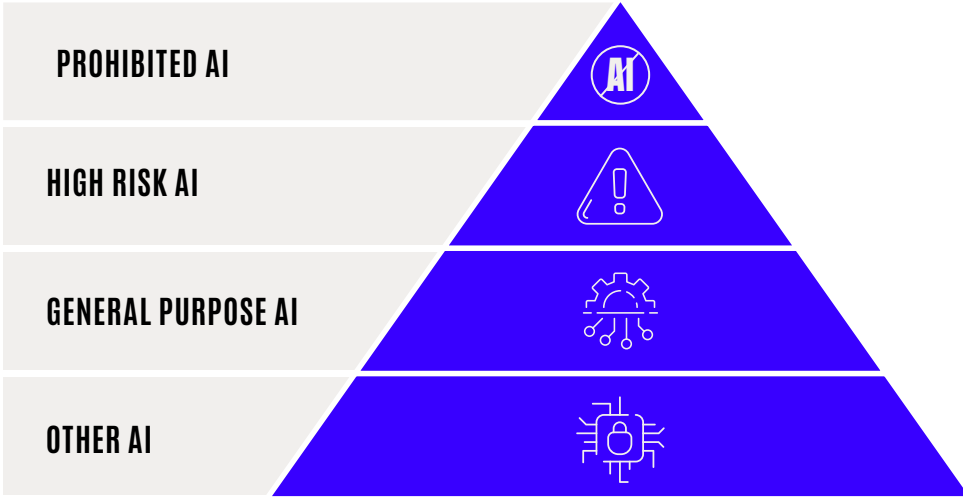
Key obligations include:

- + transparency and risk management
- + undertaking fundamental rights impact assessments
- + providing summaries of training data
- + ensuring compliance with copyright laws and making publicly available a sufficiently detailed summary of the content used for training
- + labelling AI generated content
- + producing various technical documentation.



OTHER AI

For all other AI systems, there are limited compliance obligations, other than ensuring transparency (i.e. that individuals are made aware when they are interacting with AI systems).



KEY TAKEAWAYS

WHO WILL ENFORCE THE AI ACT?

The AI Act will be enforced by AI authorities designated within Member States. Member States may implement new independent AI authorities or may empower existing authorities (such as Data Protection Authorities), to enforce the AI Act.

At an EU level, a new European AI Office was established within the Commission to coordinate and supervise governance and enforcement across the EU (which will be supported by scientific experts). An AI Board was also established with representatives from Member States, acting as an advisory board to the Commission, and tasked with designing codes of practice. The General-Purpose AI (GPAI) Code of Practice was published on 10 July 2025.

OTHER KEY TAKEAWAYS UNDER THE AI ACT

- + Providers and public bodies using High-Risk AI Systems will need to register the AI system in an EU database.
- + The AI Act encourages national authorities to set up “regulatory sandboxes” and facilitate “real-world testing”, to develop and train AI systems before they are placed on the market.
- + The category of High-Risk AI Systems can be supplemented in the future, as new AI technology and use cases evolve.
- + The EU’s “AI Pact” gives AI providers the opportunity to implement the obligations of the AI Act on a voluntary basis, before they come into force.
- + Non-binding European Commission guidelines aim to support consistent interpretation across EU member states.
- + Draft guidelines on the classification of High-Risk AI Systems were published on 19 May 2026.

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

7% or **€35 MILLION**
of annual global turnover for infringements on prohibited practices or non-compliance related to requirements on data

3% or **€15 MILLION**
of annual global turnover for other violations (including those relating to High – Risk AI Systems and General Purpose AI Models)

1% or **€7 MILLION**
of annual global turnover for the supply of incorrect, incomplete or misleading information

WHAT ACTION SHOULD WE TAKE NOW?

Whilst the AI Act (and other regulatory frameworks in the UK, and around the world) is yet to apply in full force, and implementation timelines have been further delayed under the Digital Omnibus on AI, there is sufficient information and common themes for organisations to implement steps to prepare for new requirements that lay ahead. In fact, making headway on these now will almost certainly ease the compliance burden down the line.

ACTIONS TO CONSIDER INCLUDE:

- + develop an AI asset register – knowing where and how AI is used in your organisation will enable you to assess risks, and implement policies and compliance requirements
- + assess the applicability of the AI Act to your business– taking into account the information in your AI asset register, make a determination of whether and how the AI Act will apply to your organisation’s AI systems and what actions you need to take in order to be ‘AI ready’
- + establish an AI governance strategy – if AI is, or will, form a key part of your product portfolio, or internal operations, establish a governance structure to guide the business through compliant adoption
- + implement policies that govern how AI should be developed or implemented. These should address how to manage risks such as bias, dataset integrity, infringement of third parties’ intellectual property rights and transparency
- + carry out and document risk assessments, in particular where the AI could present higher risks. Start building these into standard operating procedures (in the same way data protection impact assessments are implemented)
- + approach third party vendors of AI systems to request further information to allow your organisation to assess the likely risk category of the AI system being provided and determine the vendor’s level of compliance
- + review terms and conditions of use before starting any internal use of an AI system to manage confidentiality of data and liability related to the use of the system
- + track global progress so you keep up to date with legislative developments in jurisdictions in which you operate. When AI is becoming deeply embedded in your organisation, you need to plan well ahead.

OUR TEAM

Please contact one of our AI experts should you have any queries, or to discuss your AI compliance strategy.

STEPHENSON HARWOOD

© Stephenson Harwood LLP 2026. Any reference to Stephenson Harwood in this document means Stephenson Harwood LLP and/or its affiliated undertakings. Any reference to a partner is used to refer to a member of Stephenson Harwood LLP.