The EU AI Act: What you need to know

WHAT IT DOES?

- Legal framework for AI systems in the EU to achieve human centric and trustworthy AI
- Harmonised rules designed to protect health, safety and fundamental rights against the harmful effects of AI
- Risk based approach determined by intended purpose and the potential impact
- Facilitates innovation including via regulatory sandboxes and support for SMEs and start-ups

WHO IT APPLIES TO?

- Applies to AI providers, users, importers, distributors, manufacturers, and authorised representatives
- Will not apply to AI systems developed or used for scientific research, military, defence or international cooperation where there are sufficient fundamental rights safeguards in place

EXTRA-TERRITORIAL SCOPE

- It applies to entities established outside the EU putting AI on, or into service on, the EU market and/or using AI outputs in the EU
- Non-EU High Risk & GPAI providers must appoint Authorised Representatives

RISK CATEGORIES

- Prohibited: e.g. social scoring, cognitive behavioural manipulation, biometric categorisation
- High: e.g. use in employment, credit decisions, health/life insurance risk assessment
- General purpose models adaptable for multiple uses or integration into systems (GPAI)
- Limited: e.g. chatbots
- Minimal: e.g. spam filters or video games not falling within the above

HIGH RISK PROVIDERS

- Must have risk management system, data governance, technical documentation, record-keeping, transparency and provision of information to deployers, human oversight, accuracy, robustness and cybersecurity, quality management system, documentation keeping, automatically generated logs, cooperation with competent authorities
- Display CE Mark & register with EU database

GPAI PROVIDERS

- Voluntary codes of conduct will be published
- Mandatory obligations including technical documentation, copyright policy, and publishing data on content used for training
- Systemic risk GPAI require model evaluation, ongoing assessment & mitigation of risks, notification to the Commission, incident reporting and cybersecurity

USERS' OBLIGATIONS

- All: Ensure staff AI literacy
- High Risk: Technical and organisational measures, human oversight, monitoring, ensure relevant & representative input data, keep logs, conduct data protection impact assessments. If used in employment, inform employees
- Transparency re use of deep fakes, emotion recognition, biometric categorisation systems or public interest publications using GenAI (i.e. AI which generates or manipulates text)

ENFORCEMENT

- EU AI Office, AI Board & Commission delegated powers
- National supervisory authorities competent to enforce
- Prohibited AI: Fines of up to the greater of €35 million or 7% annual global turnover. Other AI: Fines of up to the greater of €15 million or 3% of annual global turnover
- Special provision for SMEs in relation to fines
- Standards, which will create a presumption of compliance, are in development

TIMING

The provisions of the AI Act are expected to apply from 1 August 2026 with exceptions:

- 1 November 2024 - National public authority protecting fundamental rights to be notified to the Commission
- 1 February 2025 - Scope,definitions and prohibited AI systems
- 1 August 2025 - GPAI, penalties and EU governance
- 1 August 2027 - Safety components/specific products of Annex I considered high risk

WHAT TO DO NOW?

- Identify AI used by your business and which risk category applies
- Put in place an AI governance framework appropriate to your use and the relevant risk category including an AI policy, staff AI training and vendor AI due diligence
- Communicate with stakeholders

FOR FURTHER INFORMATION PLEASE CONTACT:

Claire Morrissey
Partner
+353 1 619 2113
claire.morrissey@maples.com

Stefan Nolan
Associate
+353 1 619 2102
stefan.nolan@maples.com

Sarah Lydon
Associate
+353 1 619 2070
sarah.lydon@maples.com

maples.com