CLIFFORD

CHANCE

EU AI ACT
EXEC BRIEFER

EU AI ACT

5 things you need to know

01 GLOBAL REACH

Can apply to businesses outside of the EU (e.g., where they place on the market or put into service AI in the EU or where the output is used in the EU).

02 BROAD APPLICABILITY

Applies across sectors and covers the whole AI value chain (e.g., providers, deployers, importers, distributors).

03 RISK-ADJUSTED

Rules and compliance requirements are defined following a tiered approach dependent on the AI risk (e.g., prohibitions, high-risk, GPAI, GenAI).

04 STRONG ENFORCEMENT

Enforced by national authorities and new EU-level bodies (incl. AI Office under the European Commission), with fines up to 7% of global annual turnover.

05 IMMINENT IMPACT

Enters into force on 1 August 2024, following its publication on 12 July 2024. Prohibitions and literacy requirements apply after 6 months, i.e. from February 2025. Other requirements apply 12 / 24 / 36 months after entry into force. Organisations need to be preparing now.

When do the new rules start to apply?

2 February 2025

Prohibitions, AI literacy, general provisions

2 August 2025

General-purpose AI (GPAI), Member States' rules on penalties

2 August 2026*

Standalone high-risk AI (e.g. HR, credit scoring, life/health insurance risk assessment and pricing), specific transparency requirements, regulatory sandboxes, etc.

*By-default transition period

2 August 2027

High-risk AI under specific sectoral legislation (e.g., re medical devices, radio equipment, toys, machinery), GPAI models already on the market.

EU AI ACT – A TIERED APPROACH

When we talk about AI – What do we mean?

Broad notion under the EU AI Act but still aims to distinguish from simpler traditional software or programming approaches.

Capability to infer > **Machine-based** > **Degree of autonomy**

Key AI classifications under the EU AI Act

CATEGORY	USE CASE*
Prohibited	• Subliminal / manipulative / deceptive techniques • Work / education emotion recognition • Social scoring • 'Real time' remote biometrics for law enforcement
High-risk	• Certain HR solutions • Credit scoring • Remote biometric identification, biometric categorisation, emotion recognition (non-banned) • Education / vocational training • Life / health insurance risk assessment and pricing or public assistance eligibility • Critical infrastructure safety components • Products / safety components under specific sectoral legislation (e.g., re medical devices, radio equipment, toys, machinery)
GPAI models	• AI model trained with large data sets using self-supervision at scale and capable of performing distinct tasks in different contexts - e.g. LLMs
Enhanced transparency	• AI Q&A and chatbots • GenAI including deep fakes • Emotion recognition / biometric categorisation

Limited* exceptions to some high-risk

… if intended to:

- perform narrow procedural task
- improve result of previously completed human activity
- detect decision-making patterns
- perform preparatory task to high-risk use cases

***exceptions do not apply if profiling carried out**

* This table is high-level only and it is non-exhaustive. The use cases have specific descriptions in the text which should be considered when assessing impact.

SPECIFIC REQUIREMENTS FOR HIGH-RISK AI

The main responsibilities lie with the provider but requirements flow down the entire value chain, to deployers and others (e.g., importers, distributors).

PROVIDER

- Ensure conformity assessments are carried out.
- Implement quality & risk management systems.
- Use high-quality data sets for training, validation and testing.
- Ensure appropriate measures to detect, prevent and mitigate possible biases.
- Enable effective human oversight.
- Provide instructions for use including clear information on system capabilities and limitations.
- Establish a post-market monitoring system, continuously assess performance and report on serious incidents / risks.

AND DEPLOYER* CAN BECOME PROVIDER

DEPLOYER

- Use the AI system in accordance with the instructions for use supplied by the provider.
- Ensure input data is relevant and representative.
- Assign human oversight to competent people.
- Inform workers where they are to be subject to a high-risk AI system.
- Perform a prior fundamental rights impact assessment (e.g., banking / health insurance).
- Monitor the system operation and report on serious incidents / risks.

* Like other operators in the value chain.

SPECIFIC REQUIREMENTS FOR GENERATIVE AI

Enhanced transparency on content

Ensuring that the outputs of a generative AI system are marked and detectable as artificially generated or manipulated (provider).

Ensuring awareness that the content has been artificially generated or manipulated re deep fakes (deployer).

Ensuring awareness that text has been artificially generated or manipulated re text published to inform the public on matters of public interest (deployer).

There are enhanced transparency requirements for other types of AI, e.g. chatbots, emotion recognition / biometric categorisation systems.

Generative AI can also be subject to rules for other types of AI systems and models

- Prohibited practices.
- High-risk AI systems.
- GPAI models, large generative AI models being a prime example.

… and also the EU AI Act's literacy requirements.

SPECIFIC REQUIREMENTS FOR GPAI MODELS

The EU AI Act regulates GPAI models following a tiered approach, with requirements for all GPAI models and additional requirements for those presenting systemic risk.

Obligations for providers of all GPAI models

- Provide technical documentation.
- Make available information to downstream providers.
- Put in place a policy to respect EU © law and protect IP rights including in connection with text and data mining.
- Publish a summary re the content used for training, including text and data protected by © law.
- Some exceptions re models made accessible under free and open-source licence (unless models with systemic risk).

Additional obligations re models with systemic risk

- Notify European Commission within max. 2 weeks.
- Perform model evaluation, including adversarial testing.
- Assess and mitigate systemic risks at Union level.
- Track, document and report on serious incidents and corrective measures.
- Ensure adequate cybersecurity protection for the model and its physical infrastructure.

Classification as GPAI model with systemic risk

- Based on high impact capabilities or equivalent capabilities / impacts.
- Presumption where compute used for training measured in FLOPs is > 10^{25}.
- Provider to notify European Commission where model qualifies.
- European Commission can designate model as GPAI with systemic risk.

For more information and insights, you can refer to our publication entitled "The EU AI Act – Overview of key rules and requirements".

CLIFFORD

CHANCE

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 1 rue d'Astorg, CS 60058, 75377 Paris Cedex 08, France

© Clifford Chance 2024

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

2405-011228