EU AI Act

All you need to know

DENTONS GLOBAL ADVISORS

Prohibited AI systems

DENTONS GLOBAL ADVISORS

Subliminal, manipulative, or deceptive techniques

Social scoring or evaluating and classifying people based on behaviour and personality

Emotion recognition systems in workplaces or educational institutions, except for medical or safety reasons

Compiling facial recognition databases through untargeted scraping of internet and CCTV

Biometric categorisation systems classifying people based on their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation, excluding police uses, and labelling or filtering of lawfully acquired biometric datasets

Exploiting vulnerabilities related to age, disability, or socio-economic circumstances

Profiling for criminal risk assessments unless it supports human assessments.

Only police can deploy **real-time biometric identification systems** in public places, with authorisation from judicial or administrative authorities within 24 hours, when:

- *Searching for missing persons and trafficking victims.*
- *Preventing imminent security threats and terrorist attacks.*
- *Identifying suspects of serious crimes.*

Professional deployers, including police, can use **post-remote biometric identification systems**, with authorisation sought within 48 hours. Police cannot use it for surveillance unrelated to crimes.

High risk AI systems

DENTONS GLOBAL ADVISORS

Classification of systems as high risk

AI-enabled safety components or products that undergo third-party conformity assessments under certain EU laws (Annex II).

AI systems in **biometrics**, **critical infrastructure**, **education**, **employment**, **essential public and private services**, **law enforcement**, **border control**, and **judicial and democratic processes** (Annex III), unless they perform a narrow procedural or preparatory task, improve results of previously completed human activity, or detect decision-making patterns without human review – though profiling systems are always high risk (Art. 6).

Provider requirements

- Maintain a **risk management system**.
- Practice **data governance.**
- Produce **technical documentation** to demonstrate compliance.
- Embed the system with **automated incident recording capabilities**.
- Provide **instructions for use** to downstream deployers.
- Enable **human oversight** of the system.
- Design with appropriate **accuracy**, **robustness,** and **cybersecurity**.
- Establish a **quality management system** to support compliance.

Deployer requirements*

- Follow the **instructions**.
- Ensure **human oversight**.
- Ensure **input data** is relevant and representative.
- Conduct a **fundamental rights impact assessment**.
- Alert providers and authorities of any **discovered serious national level risks**.

** In a professional capacity, anyone becomes the legal provider by placing their name/trademark on the system, making substantial modifications to an existing system, or altering the intended purpose of an AI, rendering it high-risk. The original provider is only required to cooperate and provide information to support the new provider's compliance.*

General purpose AI (GPAI)

DENTONS GLOBAL ADVISORS

Closed source GPAI model provider requirements

Produce **technical documentation** to demonstrate compliance and provide **usage documentation** to downstream GPAI system developers and deployers.

Codes of conduct

All GPAI providers can demonstrate compliance through adherence to voluntary codes of practice that will be developed by circa mid-2025 until harmonised standards are published.

Closed and open source GPAI model provider requirements

Respect rightsholders' wishes to opt-out of their copyrighted works being used to train the model and publish a detailed **summary on training data content** to allow rightsholders to exercise their rights.

Providers of both closed and open source foundation models that are trained using compute that exceeds 10^25 floating point operations per second (FLOPS)* are considered systemic, and must additionally:

- Perform **model evaluations**, including adversarial testing (e.g. red teaming).
- **Assess and mitigate possible systemic risks** arising from their model.
- Track and report **serious incidents**.
- Ensure adequate model **cybersecurity**.

** The Commission will be obliged to adapt the threshold in light of evolving technological developments through secondary legislation (delegated act).*

Transparency disclosures to end-users

DENTONS GLOBAL ADVISORS

End-users should know they are interacting with AI at **first exposure**.

Providers should design their systems to ensure that people are aware they are interacting with AI when it is deployed.

Generative AI developers must ensure their system's outputs are easily recognisable as artificial, except for basic editing assistance.

Professional deployers of **emotion recognition** and **biometric categorisation systems** must inform people when they are exposed to these systems.

Professional deployers creating **deepfakes** must disclose that the content is AI-generated. If it is for artistic, satirical, or fictional works, the disclosure does not need to hamper the content's presentation.

AI Office will facilitate the creation of codes of practice to enable effective implementation of detection and labelling of AI-generated content, including supporting arrangements for checking provenance and ensuring watermarking mechanisms are accessible.

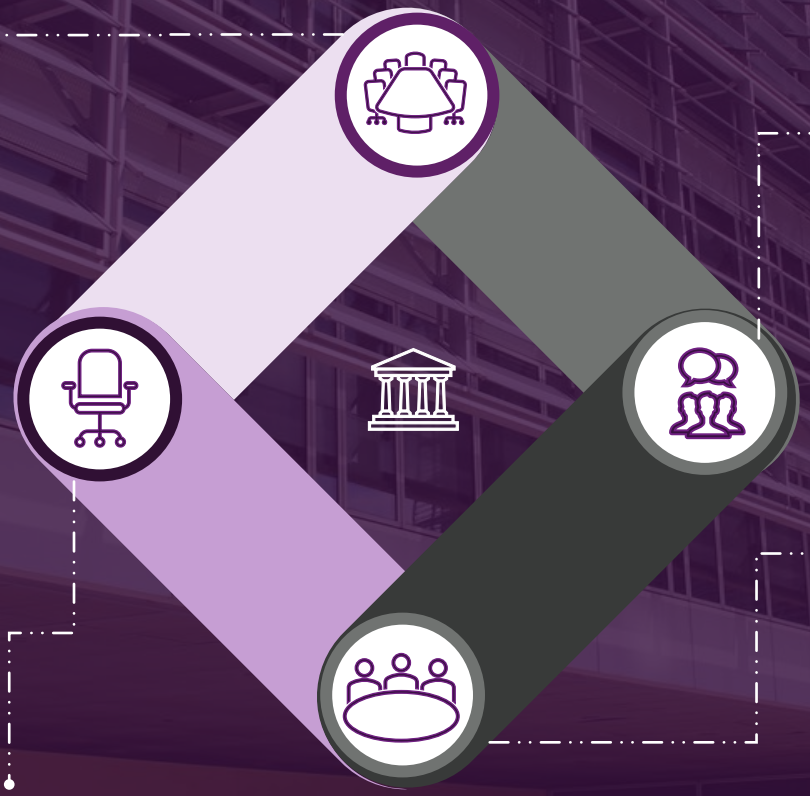
Governance

DENTONS GLOBAL ADVISORS

New AI Office within the Commission to monitor GPAI:

- *Can request documents, and gather information through structured dialogues, from GPAI providers.*
- *Can require GPAI providers to restrict, recall, or withdraw their models.*

New AI Board with a representative from each Member State to facilitate consistent implementation.



New scientific panel of independent experts who cannot be linked to AI developers:

- *Will advise the AI Office on GPAI implementation and enforcement, the methods for evaluating GPAI capabilities, and classifying models as systemic.*
- *Can provide a qualified alert to the AI Office, notifying them that a non-designated GPAI model has met the systemic threshold or should be treated as presenting a systemic risk due to other concrete factors.*

New Advisory Forum to advise and offer technical expertise to the Board and the Commission to aid in their tasks under the Regulation. Its membership will represent diverse stakeholders, ensuring a balance between commercial and non-commercial interests, including SMEs.

Implementation milestones

DENTONS GLOBAL ADVISORS

April 2024

Final text approved

May – June 2024

Publication in the EU Official Journal

Entry into force

20 days following publication in the Official Journal

Early 2025

Rules on prohibited practices shall apply from 6 months after entry into force

Mid-2025

By 9 months after entry into force, the AI Office should facilitate codes of practice on GPAI and

Mid-2025

Rules on GPAI and penalties shall apply 12 months after entry into force

Mid-2026

Obligations for high-risk systems under Annex III start applying (mid-2027 for systems falling under Annex II)

Secondary legislation & guidelines

DENTONS GLOBAL ADVISORS

Delegated acts

- Criteria that exempt AI systems from high risk rules.
- High risk AI use cases.
- Thresholds classifying General Purpose AI models as systemic.
- Technical documentation requirements for high risk AI systems and GPAI.
- Conformity assessments.
- EU declaration of conformity.

Implementing acts

- Approving codes of practice for GPAI and generative AI watermarking.
- Establishing the scientific panel of independent experts.
- Conditions for AI Office evaluations of GPAI compliance.
- Operational rules for AI regulatory sandboxes.
- Information in real-world testing plans.
- Common specifications (where standards do not cover rules).

Guidelines

- By 12 months after entry into force: High risk AI serious incident reporting.
- By 18 months after entry into force: Practical guidance on determining if an AI system is high risk, with list of practical examples of high-risk and non-high risk use cases.
- “when deemed necessary”: The application of the definition of an AI system; High risk AI provider requirements; Prohibitions; Substantial modifications; Transparency disclosures to end-users; Detailed information on the relationship between the AI Act and other EU laws.

Standards

- JTC21 in CEN-CENELEC, in consultation with ETSI, have already begun developing standards, compliance with which will lead to a presumption of conformity, where standards sufficiently cover the obligations.