The European Artificial Intelligence Act

Explainatory Brochure

12 May, 2025

Araki International IP&Law 荒木法律事務所

Table of Contents

1. Overview of the AI Act

What is the "AI Act"?

Regulation (EU) 2024/1689 (hereinafter referred to as "AI Act") is the first legislation to provide comprehensive legal framework on artificial intelligence (hereinafter referred to as "AI") worldwide.

What is the purpose of the "AI Act"?

The purpose of the AI Act is as follows:
- improve the functioning of the internal market;
- promote the uptake of human-centric and trustworthy AI;
- ensure a high level of protection of health, safety, fundamental rights enshrined in the Charter of Fundamental Rights of the European Union, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union;
- support innovation.

2. The scope of the AI Act

AI subject to the regulation

The AI Act applies to "AI systems", which are defined as: "a machine-based system that is 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".

The AI Act applies also to "general-purpose AI models" (hereinafter referred to as "GPAI models"), which are defined as: "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market".

Businesses subject to the regulation

The AI Act applies to various business operators in the AI value chain:

(a) **providers** placing on the market or putting into service AI systems or placing on the market GPAI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country;

(b) **deployers** of AI systems that have their place of establishment or are located within the Union;

(c) providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union;

(d) **importers** and **distributors** of AI systems;

(e) **product manufacturers** placing on the market or putting into service an AI system together with their product and under their own name or trademark;

(f) **authorised representatives of providers,** which are not established in the Union.

Exemptions:
The AI Act does not apply to certain cases, including but not limited to:

- AI systems placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes;
- Certain uses of AI systems by public authorities in a third country or international organisations with adequate safeguards;
- AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development;
- Research, testing or development activity regarding AI systems or AI models prior to their being placed on the market or put into service. Nevertheless, testing in real world conditions shall not be covered by this exclusion;
- Natural persons using AI systems in the course of a purely personal non-professional activity;
- AI systems released under free and open-source licences (except when placed on the market or put into service as an AI system that falls under the category of high-risk, prohibited AI practices or certain AI).

Extraterritorial applicability

The AI Act applies extraterritorially in the following cases:

- The Act applies to providers placing on the market or putting into service the AI systems or placing on the market the GPAI models in the Union, regardless of their establishment or location;
- The Act also applies to providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union.

A key mechanism for enforcing the extraterritorial reach of the AI Act is the concept of "authorized representative". The authorised representatives in the Union should be appointed by the providers of high-risk AI systems or GPAI models established in third countries prior to making the AI system or GPAI model available on the Union market through written mandate and shall perform the tasks specified in such mandate.

4

3. Risk-Based Approach

In order to introduce a proportionate and effective set of binding rules for AI systems, the AI Act introduces a risk-based approach. This approach should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate.

Prohibited AI practices

High-risk AI systems

Limited risk AI systems (Certain AI systems)

Minimal risk AI systems
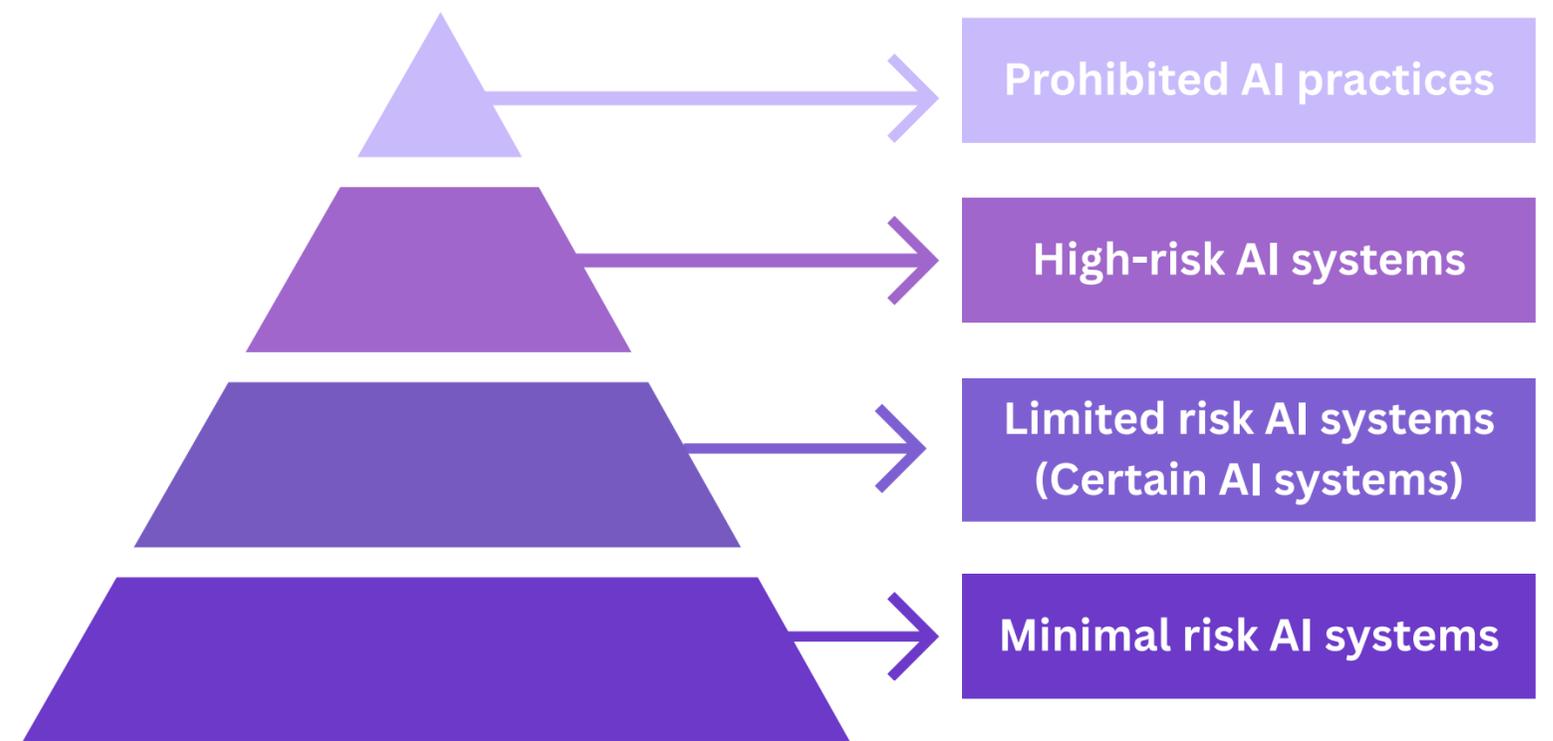
＊ Some AI systems may fall within both high-risk and limited risk categories, where target businesses shall fulfill all the relevant requirements. For this reason, such AI systems are sometimes referred to as "Certain AI systems" instead of "Limited risk AI systems".

Prohibited AI practices

What are prohibited AI practices?

The AI Act prohibits the placing on the Union market, put into service, or use of prohibited AI practices in the Union. This category includes, with several exceptions, the AI systems that pose unacceptable risks to Union values or fundamental rights, such as:

(a) AI systems that deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective or with the effect of distorting behaviour, causing or reasonably likely to cause significant harm;

(b) AI systems that exploit vulnerabilities due to age, disability or a specific social or economic situation, with the objective or with the effect of distorting behaviour, causing or reasonably likely to cause significant harm;

(c) AI systems that evaluate or classify natural persons or groups of persons based on social behaviour or personal or personality characteristics, with the social score leading to detrimental or unfavourable treatment when data comes from unrelated social contexts or such treatment is unjustified or disproportionate to the social behaviour;

(d) AI systems that assess or predict the risk of people committing a criminal offence based solely on profiling or personality traits and characteristics; except to support a human assessment based on objective and verifiable facts directly linked to a criminal activity;

(e) AI systems that create or expand facial recognition databases through untargeted scraping of facial images from the internet or closed-circuit television ('CCTV') footage;

(f) AI systems that infer emotions at the workplace or in education institutions; except for medical or safety reasons;

(g) AI systems that categorise people based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex-life or sexual orientation; except for labelling or filtering of lawfully acquired biometric datasets, including in the area of law enforcement;

(h) AI systems for real-time remote biometric identification in publicly accessible spaces for the purposes of law enforcement; except if necessary for the targeted search of specific victims, the prevention of specific threats including terrorist attacks, or the search of suspects of specific offences (further procedural requirements, including for authorisation, are outlined in the Act).

Enforcement deadline

The AI Act bans the placing on the Union market, put into service, or use of prohibited AI systems in the Union starting from **2 February 2025.**

High-Risk AI systems

What are high-risk AI systems?

The AI Act classifies the following AI systems as posing high-risks:

(a) AI systems inteded to be used as a safety component of a product or if the AI system is a product itself covered by Union harmonization legislations listed in Annex I and required to undergo a third-party conformity assessment pursuant to the Union harmonisation legislation listed in Annex I.

(b) AI systems deployed in eight specific areas provided under Annex III of the AI Act , which are:
- Biometrics;
- Critical infrastructure;
- Education and vocational training;
- Employment, workers management and access to self-employment;
- Access to and enjoyment of essential private and public services and benefits;
- Law enforcement;
- Migration, asylum and border control management;
- Administration of justice and democratic processes.

What are the legislations mentioned in Annex I?

Section A of Annex I
- Directive on machinery;
- Directive on safety of toys;
- Directive on recreational craft and personal watercraft;
- Directive on lifts and safety components for lifts;
- Directive on equipment and protective systems intended for use in potentially explosive atmospheres;
- Directive on the making available on the market of radio equipment;
- Directive on the making available on the market of pressure equipment;
- Regulation on cableway installations;
- Regulation on personal protective equipment;
- Regulation on appliances burning gaseous fuels;
- Regulation on medical devices;
- Regulation on in vitro diagnostic medical devices.

Section B of Annex I
- Regulation on common rules in the field of civil aviation security;
- Regulation on the approval and market surveillance of two- or three-wheel vehicles and quadricycles;
- Regulation on the approval and market surveillance of agricultural and forestry vehicles;
- Directive on marine equipment;
- Directive on the interoperability of the rail system within the EU;
- Regulation on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles;
- Regulation on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users;
- Regulation on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency.

The AI system used in one of the specific areas listed in Annex III of the AI Act will not be considered as high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights and where it meets any of these conditions:
- It is intended to perform a narrow procedural task;
- It is intended to improve the result of a previously completed human activity;
- It is intended to detect decision making patterns or deviations from prior decision-making patterns and which are not meant to replace or influence the previously completed human assessment, without proper human review; or
- It is intended to perform a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III.

Nevertheless, the same AI system used in one of the areas listed in Annex III is always considered to be high-risk where the AI system performs profiling of natural persons.
A provider who considers that an AI system referred to in Annex III is not high-risk shall document its assessment before that system is placed on the market or put into service. Such provider shall be subject to the registration obligation under the AI Act and shall provide the documentation of the assessment upon request of the national competent authorities.

Requirements for High-Risk AI systems

Requirements for high-risk AI systems include:

- Risk management system;
- Data and Data governance;
- Technical documentation;
- Recordkeeping;
- Transparency and informing deployers;
- Human oversight; and
- Accuracy, robustness and cybersecurity.

High-Risk AI systems

What are the obligations of target businesses?

(a) Provider

The providers of high-risk AI systems must fulfill certain obligations, including but not limited to:

- Ensure that the extensive requirements for high-risk AI systems are met;
- Ensure the establishment of a quality management system;
- Maintain all the relevant technical documentation;
- Keep the automatically generated logs by the high-risk AI system;
- Adopt corrective actions to ensure the continuous conformity of the AI system;
- Appoint an authorized representative established in the Union if the provider is established in a third country. Such appointment must be made prior to making the high-risk AI system available on the Union market through a written mandate;
- Ensure that the high-risk AI system undergoes the conformity assessment procedure before its placement on the market or put into service;
- Ensure the compliance with accessibility requirements;
- Upon a reasoned request, cooperate with the competent national authorities to demonstrate conformity of the high-risk AI system with the requirements;
- Comply with the registration obligations;
- Indicate the provider's name, registered trade name or trade mark and address for contact;
- Affix the CE marking to the high-risk AI system, its packaging or its accompanying documentation;
- Draw up an EU declaration of conformity.

(b) Deployer

The deployers of high-risk AI systems must fulfill certain obligations, including but not limited to:

- Implement appropriate technical and organizational measures to ensure they use the systems in accordance with the instructions for use;
- Assign human oversight to people with the necessary authority, training and competence, as well as the necessary support;
- Ensure and monitor the operation of the high-risk AI system under the use instructions and inform the providers on the collection, documentation and analysis of relevant data;
- Inform the provider or distributor and the relevant market surveillance authority if the use of high-risk AI system under the use instructions may present a risk to health, safety or to fundamental rights of people and suspend the use of that system;
- Inform the provider, the importer or distributor and the relevant market surveillance authorities in case of serious incident;
- Maintain logs automatically generated by the high-risk AI system about its operations for at least six months;
- Inform affected individuals (e.g., employees) that they will be subject to the use of high-risk AI system;
- Comply with the relevant registration requirements when the deployer is a public authority, Union institution, body office or agency;
- Comply with the General Data Protection Regulation (hereinafter referred to as "GDPR") obligations and perform a data protection impact using the instructions for use provided by the providers of the high-risk AI systems;
- Inform the natural persons that they will be subject to the use of one of the high-risk AI system referred to in Annex III that makes decisions or assist in making decisions related to natural persons;
- Cooperate with the relevant competent authorities.

(c) Importer:

The importers of high-risk AI systems must fulfill certain obligations, including but not limited to:

- Verify the compliance with certain obligations posed on the provider prior to placing the AI system on the market;
- Inform relevant AI operators in case of risk;
- Indicate importer's name, registered trade name or trademark and address on the AI system and on its packaging or accompanying documentation;
- Ensure that they will not jeopardise the AI system's compliance with its requirements while it is under their responsibility;
- Keep relevant documentation for 10 years after the placing on the market or put into service of the AI system;
- Provide information and documentation upon request of the relevant competent authority;
- Cooperate with the relevant competent authority.

(d) Distributor

The distributors of high-risk AI systems must fulfill certain obligations, including but not limited to:

- Verify the compliance with certain obligations posed on the providers and importers prior to making the AI system available on the market;
- Ensure that they will not jeopardise the AI system's compliance with its obligations while it is under their responsibility;
- Inform relevant AI operators and implement corrective actions in case of non-conformity / risk or ensure that the provider, importer or any relevant operator take those corrective actions;
- Provide information and documentation upon request of the relevant competent authority;
- Cooperate with the relevant competent authority.
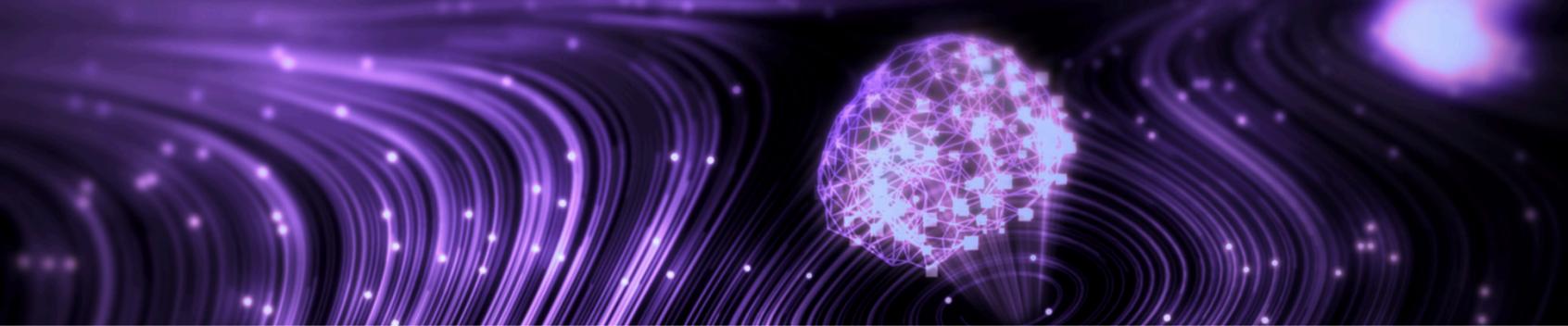
(e) Authorized Representative:

The authorized representative of providers of high-risk AI systems must fulfill certain obligations, including but not limited to:

- Provide a copy of the written mandate to the market surveillance authorities upon request;
- Perform the tasks specified in the mandate received by the provider, which shall enable the authorized representative to carry out the following:
1. Verify the compliance with the obligation posed on the provider concerning the EU declaration of conformity and technical documentation;
2. Keep relevant documentation for 10 years after the high-risk AI system has been placed on the market or put into service;
3. Provide the competent authority, upon reasoned request, with all the information and documentation necessary to demonstrate the conformity of a high-risk AI system with the requirements of high-risk AI systems (including the access to the logs automatically generated by the high-risk AI system, to the extent such logs are under the control of the provider);
4. Cooperate with the competent authorities, upon a reasoned request, in any action the latter take in relation to the high-risk AI system, in particular to reduce and mitigate the risks posed by the high-risk AI system;
5. Comply with the registration obligations, or, if the registration is carried out by the provider itself, ensure that the information provided is correct;
- Terminate mandate if it considers or has reasons to consider that the provider acts contrary to its obligations under the AI Act. The termination of the mandate and the reasons therefor shall be communicated to the relevant market surveillance authority and the relevant notified body (where applicable).

(f) Responsibility along the AI value chain:

Distributor, importer, deployer or other third-party shall be considered to be a provider of a high-risk AI system if:

1. they put their name or trademark on a high-risk AI system already placed on the market or put into service;
2. they make a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service;
3. they modify the intended purpose of an AI system that has already been placed on the market or put into service making it an high-risk AI system.

If any of the above events occur, the provider that initially placed the AI system on the market or put it into service is no longer considered the AI system's provider. The initial provider shall make available the necessary information and provide the technical access and assistance required to enable the new provider to comply with the obligation under the regulation, especially for the conformity assessment of high-risk AI systems. This does not apply if the initial provider has clearly specified that its AI system is not to be changed into a high-risk AI system. This is without prejudice to the need to observe and protect intellectual property rights, confidential business information and trade secrets. The provider of a high-risk AI system and the third party that supplies an AI system, tools, services, components or processes that are used or integrated in high-risk AI system must fulfill each of the following obligations:

- Shall specify by written agreement the necessary information, capabilities, technical access and other assistance in order to enable the provider of the high-risk AI system to fully comply with the obligations under the AI Act. This shall not apply to third parties making accessible to the public tools, services, processes, or components, other than GPAI models, under a free and open-source licence.
- The AI Office may develop and recommend voluntary model terms for contracts between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used for or integrated into high-risk AI systems.

10

High-Risk AI systems

Conformity Assessment: How to conduct it?

Harmonized Standards and Common Specifications

Standards and specifications play a fundamental role in providing technical solutions to ensure compliance with the AI Act:

- High-risk AI systems complying with harmonized standards or common specifications will be presumed to be in conformity with the requirements for high-risk AI systems, to the extent that the standards or specifications cover those requirements or obligations;
- On May 22, 2023, the European Commission issued a standardization request to the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC). Based on the request, CEN and CENELEC are in course of developing harmonized standards.

However, if harmonized standard that fulfills the requirement under the AI Act is not available, the Commission may instead adopt implementing acts establishing common specifications for the requirements for high-risk AI systems.

The conformity assessment is defined as the process of demonstrating whether the requirements for high-risk AI systems have been fulfilled.

Providers must ensure that high-risk AI systems undergo a conformity assessment procedure before placing them on the market or putting them into service, unless certain applicable derogations apply.

There are two types of assessment that are (a) the internal control, which is an assessment conducted by providers, and (b) third-party assessment with the involvement of a notified body. In the conformity assessment procedure based on internal control, the provider, without the involvement of a third-party notified body, verifies the compliance of the established quality management system with the regulation and examines the information contained in the technical documentation to assess the compliance of the AI system to the requirements for high-risk AI systems, and conducts an assessment of the design and development process of the AI system and its post-market monitoring to ensure consistency with the technical documentation.

- High-risk AI systems listed in point 1 of Annex III:
  - In general, the provider of the AI system may conduct conformity assessment based on either (a) the internal control or (b) third-party assessment, when it applies harmonized standards or common specifications;
  - However, if the harmonized standards do not exist or have been published with a restriction or the provider has not applied them; or if common specifications are not available or the provider has not applied them, the provider must conduct the conformity assessment based on third-party assessment.
- High-risk AI systems referred to in points 2 to 8 of Annex III:
  - The provider of AI systems shall follow the conformity assessment procedure based on internal control.
- High-risk AI systems covered by the Union harmonisation legislation listed in Section A of Annex I:
  - The provider shall follow the relevant conformity assessment procedure as required under those legal acts.

It must be additionally highlighted that high-risk AI systems that have already been subject to a conformity assessment procedure shall undergo a new conformity assessment procedure in the event of a substantial modification. However, high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment and are part of the relevant information related to the technical solutions adopted to ensure continuous compliance with the requirements for high-risk AI systems, shall not constitute a substantial modification.

11

High-Risk AI systems

Enforcement deadline

What does a provider need to do after completing the conformity assessment?

The deadlines concerning the high-risk AI systems are as follows:

(a)**February 2026**: practical guidelines on high-risk AI systems will be provided;

(b)**August 2026**: application of the AI Act for AI systems begins except for AI systems to be used as a safety component of a product or if the AI system is a product itself covered by Union harmonisation legislations listed in Annex I, and required to undergo a third-party conformity assessment pursuant to the Union harmonisation legislation listed in Annex I;

(c) **August 2027**: application of the AI Act for all risk categories begins.

1. Certificates or EU declaration of conformity:
Upon positive assessment of the conformity with the requirements for high-risk AI systems and upon completion of the conformity assessment procedure, the provider of the high-risk AI system shall draw up an EU declaration of conformity. The provider shall keep the EU declaration of conformity up-to-date as appropriate;

2. CE marking:
General principles set out in Article 30 of Regulation (EC) No 765/2008 shall apply: high-risk AI systems should bear the CE marking to indicate their conformity with the AI Act.

3. Registration:
In addition, registration in the EU database may be required.
- Before placing on the market or putting into service a high-risk AI system listed in Annex III (expect for the high-risk AI system listed in point 2 of Annex III), the provider or the authorized representative shall register themselves and their system in the EU database.

12

Limited risk systems

Minimal risk systems

What are limited risk AI systems?

The AI system may interact directly with users (e.g., chatbots) and perform certain activities involving the creation or manipulation of visual or audio content that constitute "deep fake". Such use poses a limited risk and is subject to specific transparency and disclosure obligations.

Enforcement deadline

The transparency obligations will come into effect on **2 August 2026.**

What are the obligations?

The transparency obligations associated with limited risk AI systems are as follows:

(a) **Providers** must:

- Ensure that AI systems intended to directly interact with natural persons are designed and developed in such a way that individuals are informed that they are interacting with an AI system; and
- Ensure that their systems' outputs when generating synthetic audio, image, video or text content are marked in a machine-readable format and detectable as artificially generated or manipulated. Such technical solutions must be effective, interoperable, robust and reliable.

(b) **Deployers** must:

- Disclose that the system's output has been artificially generated or manipulated when creating or otherwise editing images, audio or video content constituting a deep fake;
- Disclose that the system's output has been artificially generated or manipulated when creating or otherwise modifying a text published for the purpose of informing the public on matters of public interest, and;
- Inform individuals exposed to emotion recognition or biometric categorization systems, which can qualify as high-risk AI systems. Personal data should be processed under the provisions of the GDPR, Regulation (EU) 2018/1725 and Directive (EU) 2016/680.

What are minimal risk AI systems?

This is a residual category, systems classified as minimal risk are those that do not belong to the three previously mentioned categories.

What are the obligations?

Minimal risk AI systems may be deployed without further restrictions or mandatory obligations, however the AI Act calls for voluntary compliance to all or some of the requirements for high-risk AI systems under the regulation, which include transparency, human oversight and accuracy.

General Purpose AI Model

What is "General Purpose AI Model"?

The AI Act also regulates the use of GPAI models that are defined as "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market".

In addition, a GPAI model shall be classified as posing system risks if it meets any the following conditions:
(a) it has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks. A GPAI model is presumed to have high impact capabilities if the cumulative amount of computation used for its training measured in floating point operations is greater than 10^{25}; or
(b) it has capabilities or an impact equivalent to (a) concerning the criteria mentioned in Annex XIIII of the AI Act, based on a decision of the Commission, ex officio or following a qualified alert from the scientific panel.

What are the obligations?

The use of GPAI models is regulated in a tiered approach with more obligations for those providers of GPAI models posing systemic risks.
All providers of GPAI models must fulfill the obligations to:

- Create and regularly update the technical documentation of their model;
- Prepare, keep up-to-date and make available information and documentation, which enable providers of AI system planning to integrate the GPAI model into their systems to understand the capabilities and limitations of the GPAI model and to comply with the obligations under the AI Act;
- Establish a policy for complying with Union copyright law and related rights and comply with a reservation of rights by the rights holders of the copyrighted material; and
- Elaborate and make available to the public sufficiently detailed summaries of the training data used for the GPAI model.

For free and open-source license GPAI models, only the latter two obligations apply to providers of GPAI models that are made accessible to the public under a free and open-source license, and whose parameters are made publicly available, unless the GPAI models present systemic risks.
In addition to the obligations above, providers of GPAI models with systemic risks must fulfill the following obligations:

- Perform standardized model evaluations;
- Assess and mitigate possible systemic risks;
- Track documents and report to the AI Office serious incidents and possible corrective measures;
- Ensure adequate level of cybersecurity protection and the physical infrastructure of the model.

What is "Code of Practice"?

Both providers of GPAI models and providers of GPAI models with a systemic risk may rely on codes of practice until harmonised standards or common specifications are published. Compliance with such codes of practice will lead to a presumption of conformity with certain obligations. The AI Office may invite GPAI model providers and relevant national competent authorities to participate in drawing up codes of practice at Union level.

Enforcement deadline

Provisions on GPAI models will become applicable from 2 August 2025.

4. Measures in support of innovation

AI Regulatory Sandboxes

"AI regulatory sandbox" means a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision.

There shall be at least one AI regulatory sandbox operational in each member state by 2 August 2026.

Testing of high-risk AI systems in real world conditions outside sandboxes

'Testing in real world conditions' means the "temporary testing of an AI system for its intended purpose in real-world conditions outside a laboratory or otherwise simulated environment, with a view to gathering reliable and robust data and to assessing and verifying the conformity of the AI system with the requirements of this Regulation and it does not qualify as placing the AI system on the market or putting it into service within the meaning of this Regulation".

Testing of high-risk AI systems in real world conditions outside AI regulatory sandboxes may be conducted by providers or prospective providers of high-risk AI systems listed in Annex III, in accordance with the regulation and the real-world testing plan, without prejudice to the prohibitions on the prohibited AI practices.

Measures for providers and deployers, in particular SMEs, including start-ups

- Small and medium enterprises (hereinafter referred to as "SMEs") will have priority access to AI regulatory sandboxes;
- Member States will utilize or establish dedicated channels for SMEs and organize specific awareness raising and training activities on the application of the regulation, and overall facilitate the participation of SMEs in the standardization development process;
- The specific interests and needs of the SME providers, including start-ups, shall be taken into account when setting the fees for conformity assessment.

5. New Governance structure

Union level

- **AI Office**:
It is the Commission's function of contributing to the implementation, monitoring and supervision of AI systems and GPAI models, and AI governance;
- **European Artificial Intelligence Board**:
It shall advise and assist the Commission and the Member States in order to facilitate the consistent and effective application of this regulation;
- **Advisory forum**:
It shall be an established to provide technical expertise that advises both the European Commission and the AI Board, and to contribute to their tasks under this regulation;
- **Scientific panel of independent experts**:
The panel shall support member states' enforcement activities under the regulation.

National level

Each Member State shall establish or designate at least **one notifying authority** and at least **one market surveillance authority**, which shall exercise their powers independently, impartially and without bias so as to safeguard the objectivity of their activities and tasks, and to ensure the application and implementation of this regulation. The information on how competent authorities and single points of contact can be contacted shall be made publicly available by **2 August 2025.**

6. Penalties

Non-compliance with the rules set forth in the regulation will result in the application of penalties, the amount of which will differ depending on the type of obligation being violated.

✳ As an exception to the application of the fine, the lower amount in the table on the right (rather than the higher amount) applies in case of SMEs.
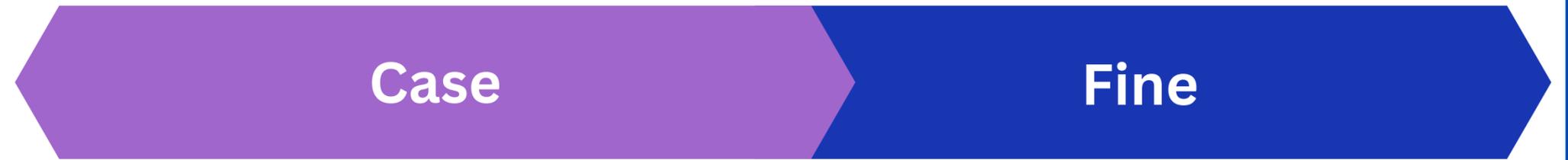
Case	Fine
Non-compliance with rules on prohibited AI practices.	Fines up to €35 million or 7% of total worldwide annual turnover, whichever is higher.
Violation of: • Transparency obligations for providers and deployers; • Obligations imposed on providers, authorized representatives, importers, distributors, deployers of high-risk AI systems; • Requirements and obligations of notified bodies.	Fines up to €15 million or 3% of total worldwide annual turnover, whichever is higher.
The supply of incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply to a request.	Fines up to €7.5 million or 1% of total worldwide annual turnover, whichever is higher.

✳ If providers of GPAI models intentionally or negligently infringe relevant provisions of the AI Act, the Commission may impose fines up to €15 million or 3 % of total worldwide annual turnover, whichever is higher.

7. Timeline of application

1

1 August 2024

AI Act enters into force.

2

2 February 2025

Chapters on General provisions and Prohibited AI practices apply.

3

2 May 2025

Codes of Practice by the Commission for GPAI models shall be ready.

4

2 August 2025

- AI Act applies to notifying authorities and notified bodies, governance, GPAI models, penalties and confidentiality
- If a code of practice cannot be finalized, or if the AI Office deems it is not adequate, the Commission may provide common rules.

6

2 August 2026

- Application of the AI Act to AI systems, excluding the obligation to take action regarding AI systems used as a safety component of a product and high-risk AI systems listed in Annex I
- This regulation shall apply to operators of high-risk AI systems placed on the market /put into service before this date (excluding AI systems that are components of the large-scale IT systems established by the legal acts listed in Annex X that are placed on the market or put into service before 2 August 2027). However, this only applies to systems which are subject to significant changes in their designs from this date onwards.

5

2 February 2026

The Commission provides guidelines on practical implementation of the requirements for high-risk AI systems.

7

2 August 2027

- Application of the AI Act for all risk categories
- Providers of GPAI models placed on the market before 2 August 2025 must have taken the necessary steps to comply with the obligations laid down in the AI Act by this date.

8

31 December 2030

AI systems which are components of the large-scale IT systems listed in Annex X and that were placed on the market / put into service before 2 August 2027 shall be brought into compliance with the AI Act by this date.

Araki International IP&Law 荒木法律事務所

Akiko Araki
Managing Partner
Attorney-at-law (Japan and California)

Tamami Takashima
Associate
Attorney-at-law (Japan)

Giacomo Tarsia
Law clerk

Laura Colombini
Paralegal

🌐 www.arakiplaw.com   ✉ info@arakiplaw.com   📞 +81.3.6810.2102

📍 254, Shin-Tokyo Building, 3-3-1, Marunouchi, Chiyoda-ku, Tokyo 100-0005, Japan