Araki International IP&Law

Newsletter September 2024

The EU AI Act explained: the major effects produced by the new Regulation

This Newsletter represents the first part of a series of articles about the ruling of Artificial Intelligence (AI). As a starting point, we will provide an overview of the EU Artificial Intelligence Act, being the world's first comprehensive legal framework to address the use and the related issues posed by AI.

**** Last updated on 27, February 2025***

I. Introduction:

The European Union's Artificial Intelligence Act (the "AI Act") entered into force on August 1, 2024. It is the first legislation to provide comprehensive legal framework on artificial intelligence (AI) worldwide, aiming to foster trustworthy AI in Europe and beyond[1]. The AI Act has been adopted in the form of an EU Regulation rather than the EU Directive, and thus it is directly applicable in the EU Member States. To accomplish its objective, the AI Act adopts a "risk-based approach", providing AI developers and deployers with requirements and obligations in accordance with the different levels of identified risk. Considering the broad scope of application of the AI Act, it might have significant implications for Japanese companies that develop, create, use AI systems or provide such service in the EU.

II. Scope of the AI Act:

General scope:

The AI Act generally applies to "AI systems", which are defined as "a machine-based system designed to operate with varying levels of autonomy, 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"[2].

The AI Act broadly covers multiple operators across the AI ecosystem, including[3]:

- Providers, who develop AI systems or a general-purpose AI model and place them on the market or put them into service under their own name or trademark, whether for payment or free;
- Deployers, who use AI systems under their authority as part of their professional activities;
- Importers, who are located or established in the EU and place on the market AI systems bearing the name or trademark of a natural or legal person established outside the EU;
- Distributors, who make an AI system available on the Union market (but differ from the providers or the importers).

In addition to the AI systems, the AI Act also regulates "General Purpose AI models" (GPAI) as explained below.

Extraterritorial applicability:

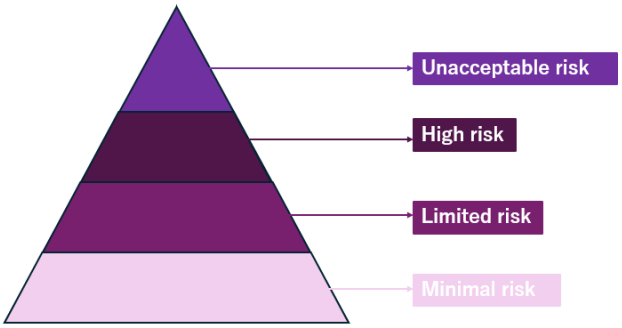
As above, the AI Act broadly covers AI operators throughout the AI ecosystem and could be applied beyond the geographical borders of the EU, thus potentially having an extra-territorial and a global reach (just like the GDPR). The AI Act also applies to providers and deployers of AI systems that are established in a third country if[4]:

- Providers put on the market or into service AI systems or place on the market general-purpose AI models in the EU, and
- Providers and deployers of AI systems if the output produced by the system is used in the EU.

III. Risk-based approach:

The AI Act introduces the risk-based approach to regulate the AI systems, which imposes requirements and obligations that differ depending on the level of risk to health, safety, and fundamental rights posed by the AI systems. AI systems are classified into four categories, depending on the degree of risk as follows:

(a) Prohibited AI systems
(b) High-risk AI systems
(c) Limited-risk AI systems
(d) Minimal-risk AI systems



Pyramid showing the criticality for AI Systems
Image created using the EU Commission's source (AI Act | Shaping Europe's digital future (europa.eu))

The majority portion of the AI Act sets the obligations imposed on the providers of high-risk AI system.

(a) **Prohibited AI systems:**

The AI Act bans the placing on the EU's market, put into service, or use of Prohibited AI systems in the EU. This category includes, with several exceptions, the AI applications that pose unacceptable level of risk of violation of Union values or fundamental rights, such as[5]:

- The exploitation of vulnerabilities of persons or use of subliminal, manipulative or deceptive techniques;
- Social scoring for public and private purposes;
- Individual predictive policing based solely on profiling people;
- Untargeted scraping of internet or CCTV for facial images to build-up or expand databases;
- Emotion recognition in the workplace and education institutions;
- Biometric categorization or identification of natural persons.
- Real-time remote biometric identification of natural persons in publicly accessible spaces for law enforcement purposes.

(b) High-risk AI systems:

The Regulation imposes strict requirements and obligations on "High-risk AI systems", including the obligations of pre-market conformity assessment.

The AI Act describes the high-risk AI system as potentially causing significant harm to health, safety or fundamental rights of natural persons. High-risk AI systems are provided as, with certain exceptions:

- AI systems used as a safety component of a product covered by EU laws listed in Annex I of the AI Act[6], and required to undergo a third-party conformity assessment under such laws[7]; and
- AI systems deployed in eight specific areas provided under Annex III of the AI Act[8], which are:
  - Non-banned biometrics;
  - Critical infrastructure;
  - Education and vocational training;
  - Employment, workers management and access to self-employment;
  - Access to and enjoyment of essential public and private services;
  - Law enforcement;
  - Migration, asylum and border control management;
  - Administration of justice and democratic processes.

For the AI systems that fall under the second category (i.e. the eight areas under Annex III), certain narrowly defined exceptions are applied, but AI systems that profile individuals are always considered high-risk and subject to strict requirements.

Providers of the high-risk AI systems must fulfill strict obligations including (but not limited to)[9]:

- Ensure that the extensive requirements for high-risk AI systems are met throughout the lifecycle of the AI system. Such requirements include[10]:
  - Risk management system;
  - Data governance;
  - Recordkeeping;
  - Transparency and informing deployers;
  - Human surveillance; and
  - Accuracy, robustness and cybersecurity
- Ensure the establishment of a quality management system;
- Maintain all 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 EU as a contact person if the provider is outside the EU;
- Ensure that the high-risk AI system undergoes the conformity assessment procedure under Article 43 of the AI Act;
- Ensure the compliance with accessibility requirements;
- Cooperate with the competent authorities.

Also, other operators such as deployers, importers and distributors must fulfill obligations that are set out under the AI Act. For deployers, the obligations include (but not limited to)[11]:

- Implement appropriate technical and organizational measures;
- Implement human oversight by people with the appropriate training and competence;
- Ensure and monitor the operation of the high-risk AI system under the use instructions;
- Maintain logs of the high-risk AI system's operations for at least six months;
- Inform individuals that may be affected by results derived from high-risk AI system about the use of this AI system (*e.g.,* employees);
- Comply with the relevant registration requirements when the user is a public authority;
- Comply with GDPR obligations to perform a data protection impact assessment;
- Cooperate with the relevant authorities.

(c) <u>Limited-risk AI systems:</u>

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 "deepfake". Such use poses a limited risk and is subject to specific transparency and disclosure obligations[12].

The transparency requirements associated with limited-risk AI systems – and the applicable relevant exceptions – are described in Article 50 of the AI Act, especially:

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.

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.

(d) Minimal-risk AI systems:

Other AI systems that do not fall within the categories described above are "minimal-risk AI systems" and they are not regulated because they pose minimal or no risk (*e.g.*, spam filters). 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[13].

IV. GPAI Model:

The AI Act also regulates the use of general-purpose AI (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".[14]

The use of GPAI model is regulated in a tiered approach with more obligations for those GPAI model providers posing systemic risks.

All providers of GPAI models must fulfill the obligations to[15]:

- Create and regularly update the technical documentation of their model;
- Prepare and update documentation for AI system providers who plan to integrate the GPAI model into their systems;
- Establish a policy for complying with EU copyright law and related rights; and
- Elaborate and make available to the public summaries of the training data.

For free and open 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 additional obligations below[16]. Such systemic risks are found when the cumulative amount of compute used for its training is greater than 10^{25} floating point operations (FLOPs)[17]:

- Perform standardized model evaluations;
- Assess and mitigate potential systemic risks;
- Track and report serious incidents and possible corrective measures;
- Ensure adequate level of cybersecurity protection.

Providers of GPAI models with a systemic risk may rely on codes of practice to demonstrate compliance until a harmonized standard is published. Compliance with such harmonized standard will lead to a presumption of conformity. The AI Office may invite GPAI model providers, relevant national competent authorities to participate in drawing up codes of practice at Union level.

V. New governance structure:

The AI Act has established new governing bodies with the aim of properly implementing the regulation, including the EU AI Office, a scientific panel of independent experts, the AI Board, and an advisory forum for stakeholders[18].

VI. Penalties:

Non-complying 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, specifically[19]:

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 GPAI-related requirements or obligations imposed on providers of high-risk AI systems, authorized representatives, importers, distributors or notified bodies	Fines up to €15 million or 3% of total worldwide annual turnover, whichever is higher

Provision of incorrect or misleading information to the 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

As an exception to the application of the highest fine, the lowest amount applies in case of small and medium enterprises (SMEs) [20].

VII. Timeline of the application of the AI Act:

The AI Act entered into force across all 27 EU Member States on August 1, 2024. Its provisions will become applicable according to the timetable below[21]:

1 August 2024	EU AI Act enters into force
2 February 2025	General provisions and prohibited AI practices
2 August 2025	Governance rules, obligations for General Purpose AI models and provisions concerning notifying authorities/notified bodies, penalties and confidentiality
2 August 2026	Application of the EU AI Act for AI systems, except Article 6(1) and the corresponding obligations
2 August 2027	Application of the EU AI Act for all risk categories

VIII. What is the impact of the AI Act on Japanese companies?

As explained above, the AI Act could reach beyond the border of the EU, and in such situation, Article 22 of the Act requires the providers of high-risk AI systems established outside the EU to appoint an authorized representative established in the EU by written mandate before making their systems available on the EU market. Japanese companies that develop, create, use AI systems or provide such service in the EU need to start the assessment of the potential impacts posed by the introduction of the AI Act.

Specifically, the following steps may be taken[22]:

- Identify and catalog the type of AI systems used in accordance with the categories listed in the AI Act;
- Assess if the AI Act covers the use of the AI systems made by the business considering the broad scope of application of the Act;
- Understand the specific risks posed by the AI systems both internally and externally and comprehend the requirements that must be met in relation to the role (*e.g.,* provider, deployer, etc.) and the AI systems used;
- Conduct a gap analysis to identify areas of non-compliance;
- Educate and train employees on the implications of AI applications;
- Communicate with the stakeholders to correctly address the AI Act requirements.

Finally, please note that although the AI Act is intended to specifically address the risks and the deployment of AI systems[23], there are many other regulatory frameworks such as GDPR, consumer protection, and intellectual property law that businesses need to consider. It is therefore crucial to understand that while concretely complying with the AI Act, businesses must not forget their other obligations under the existing legal framework[24].

---

[1] Article 1 of the AI Act

[2] Article 3 (1) of the AI Act

[3] The EU AI Act Is Here: 10 Key Takeaways for Business and Legal Leaders – Publications (morganlewis.com) (last visited on September 5, 2024)

[4] Article 2, para. 1, items a) and c) of the AI Act

[5] Article 5 of the AI Act

[6] Article 6, para. 1, item a) of the AI Act

[7] Article 6, para. 1, item b) and Recital 50 of the AI Act

[8] Article 6, para. 2 of the AI Act

[9] Articles 16-21 of the AI Act

[10] Articles 8-15 of the AI Act

[11] Article 26 of the AI Act.

[12] ey-eu-ai-act-political-agreement-overview-february-2024.pdf (last visited on September 5, 2024)

[13] https://www.trail-ml.com/blog/eu-ai-act-how-risk-is-classified (last visited on September 5, 2024)

[14] Article 3 (63) of the AI Act

[15] Article 53, para. 1 of the AI Act

[16] Article 55, para. 1 of the AI Act

[17] Article 51, para. 2 of the AI Act

[18] https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/?trk=public_post_comment-text (last visited on September 5, 2024)

[19] Article 99 of the AI Act

[20] Article 99, para. 6 of the AI Act

[21] Long awaited EU AI Act becomes law after publication in the EU's Official Journal | White & Case LLP (whitecase.com) (last visited on September 5, 2024)

[22] EU Artificial Intelligence Act - 10 essential EU AI Act questions businesses need to know (kpmg.com) (last visited on September 5, 2024)

[23] Article 3 of the AI Act

[24] https://www.linklaters.com/en/insights/blogs/digilinks/2024/may/eu---the-ai-act-reaches-the-finish-line---10-key-points (last visited on September 5, 2024)

Contact

Akiko Araki

Managing Partner of Araki International IP&Law
Attorney-at-law (Japan and California)
akiko.araki@arakiplaw.com
CV: https://arakiplaw.com/our-people/araki/

Laura Colombini

Paralegal of Araki International IP&Law
laura.colombini@arakiplaw.com
CV: https://arakiplaw.com/our-people/colombini/

About Araki International IP&Law

Araki International is a Japanese domestic law firm established by an attorney having experience with international law firms. The firm's mission is to make companies and people shining in the global market. To reach that goal, the firm is active in helping international clients running businesses in Japan in various legal areas. The firm's practice has been recognized in multiple rankings of international media, such as IAM and the Legal 500.
https://arakiplaw.com/en/
info@arakiplaw.com

Notice

This newsletter does not provide any legal advice, and thus it does not create any attorney-client relationship with the recipients. If you have any questions on any particular matters in relation to this subject matter, please contact AIL directly.
This newsletter has been distributed to those who have exchanged contacts with Araki International IP&Law (AIL) or registered for events hosted by AIL. If you no longer wish to receive emails from AIL, you may unsubscribe by sending a message here. AIL's privacy policy can be found here.