Risk & Governance Legal Newsletter（February 2025）

February 2025

In brief

On July 12, 2024, the EU officially published Regulation (EU) 2024/1689, known as the Artificial Intelligence Act (the "**AI Act**"[1]), in its official journal. This marks the world's first comprehensive legal framework governing AI.

Discussions on the AI Act had been ongoing since the European Commission initially proposed the legislation on April 21, 2021. The rapid advancement of generative AI and other technologies necessitated continuous updates to the proposal. Ultimately, The AI Act was formally adopted after receiving approval from the Council of the EU on May 21, 2024.

The AI Act entered into force on August 1, 2024, with most of its provisions set to take effect from August 2, 2026. Certain provisions, however, will be enforced at different times as appropriate.

The AI Act applies not only to companies within the EU but also broadly to businesses providing AI System and related services within the EU. As a result, Japanese companies cannot afford to overlook its implications.

The following section provides an overview of the AI Act and outlines key steps that companies should consider from a compliance perspective.

In detail

1. Step 1 Identification of AI System

The AI Act primarily regulates "AI System" ("**AI System**")[2] and "general-purpose AI models ("**general-purpose AI model**" or collectively with AI system as "**AI Systems**")[3]. Their respective definitions under the AI Act are as follows.

As a business operator[4], the first step is to identify the AI being developed or utilized and assess whether it falls within these definitions.

AI system（Article 3(1)）	a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after

[1] In this newsletter, the AI Act is presented in a simplified manner. For more detailed information, please refer to the original text at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689

[2] According to the AI Act, the concept of "AI system" should be clearly defined to ensure legal certainty and facilitate international convergence and wide acceptance, while maintaining the flexibility to accommodate rapid technological developments. It should also be closely aligned with the activities of international organizations engaged in AI research (Recital 12). In this context, the aforementioned definition is based on the OECD's definition of an "AI system."

[3] Initially, general-purpose AI model was not included in the scope of the AI Act. However, due to the recent rapid advancements in generative AI, they have been urgently incorporated into the regulatory framework.

[4] In this newsletter, the term "business operator" refers to any business entity involved with AI systems, whether as a provider or a user. This definition applies throughout the text.

	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
General-purpose AI model （Article 3(63)）	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[5] 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[6]. (However, this excludes AI model used for research, development, or prototype manufacturing conducted prior to market release.)

Furthermore, it is fully anticipated that general-purpose AI model may be deployed in the market as components of AI system. In such cases, the regulations applicable to AI system and those applicable to general-purpose AI model will be cumulatively enforced (Recital (97)).

2. Step2 Identification of Regulated Persons

The AI Act applies to various stakeholders involved with AI systems. However, the primary regulated parties are as follows (Article 2(1)(a)–(c)).

- "**providers**" placing on the market or putting into service AI System or placing on the market[7] general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country
- "**deployers**" of AI System that have their place of establishment or are located within the Union
- providers and deployers[8] of AI System 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

When categorized by providers and users, the table is structured as follows:

Provider		Location	
		Inside the EU	Outside the EU
Place of action	Inside the EU	Applicable in the following cases: ・placement on the market/putting into service of AI System ・placement on the market of general-purpose AI model	Applicable in the following cases: ・placement on the market/putting into service of AI System ・placement on the market of general-purpose AI model ・The use of AI system outputs
	Outside the EU	N/A	N/A

Deployer		Location	
		Inside the EU	Outside the EU
Place	Inside the	Applicable in the following	Applicable in the following cases:

[5] The generality of a model can sometimes be determined by the number of parameters. According to the AI Act, models with at least a billion parameters and trained with a large amount of data using self-supervision at scale should be considered to display generality (Recital 98).

[6] Large generative AI models are considered typical examples of general-purpose AI model (Recital 99).

[7] "Placing on the market" refers to the first making available of an AI system or a general-purpose AI model on the Union market (Article 3(9)). "Putting into service" means the supply of an AI system for first use directly to the deployer or for own use in the Union for its intended purpose (Article 3(11)).

[8] A specific example is when a business entity based in the EU outsources certain services related to activities performed by a high-risk AI system to a business entity located in a third country outside the EU. In such cases, the AI system used in the third country processes data that was lawfully collected within the EU and transferred from the EU, and the resulting outputs are provided to the EU-based entity (Recital 22).

of action	EU	cases: ・Use of AI system	・Use of AI system outputs
	Outside the EU	Applicable in the following cases: ・Use of AI system	N/A

The definitions of "Provider" and "Deployer" are as follows.

Subject	Definition
Provider (Article 3(3))	a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge
Deployer (Article 3(4))	a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity

For these parties, the applicability of the AI Act is determined based on the place of activity, regardless of whether they are established within the EU. Therefore, businesses must identify which category of regulated parties they fall under and verify where the AI systems identified in Step 1 are being developed, placed on the market, or used.

3. Step 3 Exemption Eligibility

The AI Act provides exemption provisions for certain AI systems. Even if certain AI systems meet the regulatory requirements identified in Step 1 and Step 2, it will not be subject to regulation if it qualifies for an exemption. Therefore, before implementing regulatory compliance measures, businesses should first verify whether their AI system falls under any of these exemptions.

Article 2 of the AI Act outlines the AI system that are exempt from its scope, primarily including the following:

- AI System where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defense or national security purposes, regardless of the type of entity carrying out those activities or which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defense or national security purposes, regardless of the type of entity carrying out those activities (3)
- Public authorities in a third country or international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI System in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the Union or with one or more Member States, provided that such a third country or international organisation provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals (4)
- AI System or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development (6)
- Any research, testing or development activity regarding AI System or AI models prior to their being placed on the market or put into service. Testing in real world conditions shall not be covered by that exclusion (8)
- Deployers who are natural persons using AI System in the course of a purely personal non-professional activity (10)
- AI System released under free and open-source licenses, unless they are placed on the market or put into service as high-risk AI System (12)

In addition, AI system that does not fall under any of the categories of unacceptable risk, high risk, or limited risk in the system classification described in Step 4 will not be subject to the regulations.

4. Step 4 Categorization of AI system

The AI Act adopts a risk-based approach, categorizing AI System based on the magnitude of the risks they pose, with stricter regulations applied to those with higher risks. Since the measures that

business operators must take vary depending on the category, they need to verify which category their AI system falls into.

The contents of each category are as follows:

(1) Prohibited AI Practice

The category considered to pose the highest risk is referred to as "**Prohibited AI Practice**". This AI system is classified as such because they have the potential to cause significant harm to people's physical and mental health or economic interests and are either intended to substantially distort human behaviour or have such an effect. (Recital (29)). Specifically, the following AI System fall under this category (Article 5(a) to (h)).

① AI system that deploys subliminal techniques (Article 5(a))
② AI system that exploits any of the vulnerabilities of a natural person (e.g., age, disability) (Article 5(b))
③ AI System for the evaluation or classification of natural persons with the social score leading to detrimental or unfavorable treatment (Article 5(c))
④ AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics (Article 5(d))
⑤ AI system that creates or expands facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage (Article 5(e))
⑥ AI system to infer emotions of a natural person in the areas of workplace and education institutions (Article 5(f))[9]
⑦ biometric categorization systems that categorize individually natural persons 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 (Article 5(g)) [10]
⑧ real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforce (Article 5(h)) [11]

(2) High-risk AI System

The category considered to have the highest risk after prohibited AI practice is referred to as high-risk AI System ("**high-risk AI System**"). This high-risk AI System are broadly classified into two categories (Articles 6(1) to 6(3)):

(i) Products or safety components subject to applicable EU harmonization legislation listed in Annex I of the AI Act, which require third-party conformity assessment before being placed on the market under such legislation.

(ii) AI System used in eight specific sectors listed in Annex III of the AI Act. However, AI System that do not have a significant impact on individuals' decision-making[12] or do not pose serious risks to health, safety, or fundamental rights are excluded. Nevertheless, AI System that involve profiling individuals are always classified as high-risk.

In category (ii), the eight sectors listed in **Annex III** are as follows:

① Biometric identification
② Critical infrastructure

[9] except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons

[10] Except for any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement

[11] Except for (i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons, (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine andforeseeable threat of a terrorist attack or (iii) the localization or identification of a person suspected of having committed a criminal offence

[12] For example, AI System designed to perform limited tasks, such as detecting duplicates among a large volume of information, or AI System intended to enhance human-created outputs (e.g., standardizing notation), are considered to fall under this category (Recital 53).

③ Education and vocational training ④ Employment and workforce management ⑤ Access to private and public services ⑥ Law enforcement ⑦ Migration, asylum, and border control ⑧ Judiciary and democratic processes

(3) AI System with Limited Risk
The AI Act subjects certain types of AI System with limited risk ("**AI System with limited risk**"[13]) to transparency obligations (Article 50).

Specifically, the following AI System fall under this category:

① AI System designed for interaction with natural persons ② AI System that generates audio, images, video, or text ③ AI System used for emotion recognition or biometric categorization

(4) Other AI System
AI System other than those mentioned in (1) to (3) are not subject to regulation under the AI Act.

5. Step 5 Identification of applicable regulations

Operators need to take different approaches based on the categories classified in Step 4.

(1) Prohibited AI Practice
Prohibited AI Practice is banned from being placed on the market, put into service, or used. Violations are subject to penalties of up to 35 million euros or 7% of the business operator's total worldwide annual turnover, whichever is higher (Article 99(3)). If a business operator determines that an AI practice falls under this prohibited category, they must cease its actions or modify it to comply with a different category.

(2) High-risk AI System
The AI Act imposes requirements on high-risk AI System by (i) establishing compliance obligations for the systems themselves (Article 8) and (ii) imposing certain obligations on both providers and (iii) users. If a business operator is found to be involved with an AI system that falls into this category, they are required to take appropriate measures based on its specific attributes.

(i) The key requirements that high-risk AI System must comply with are as follows.

System requirements	Relevant provisions	Overview
① Establishment and implementation of a risk management system	Article 9	A risk management system consisting of the following steps will be established and implemented. This risk management system will be subject to periodic review. ・ Identification and analysis of risks to health, safety and basic human rights when used as intended ・ Identification and analysis of reasonably foreseeable misuse risks ・ Risk assessment through post-marketing monitoring ・ Appropriate risk management measures
② Data Governance	Article 10	When using data-based model learning technology, learning, verification and testing are carried out using data sets that meet certain quality standards.
③ Technology documents	Article 11	Technical documents that meet certain requirements are created before being placed on the market or put into service and are kept up to

[13] Under the AI Act, it is not a specifically defined term.

		date at all times.
④ Record preservation	Article 12	The system will be equipped with a function that automatically records logs over the period of system operation.
⑤ Ensuring transparency and providing information	Article 13	The system will be designed and developed in a way that ensures transparency, so that users can interpret the system's output and use it appropriately. In addition, a user manual that meets certain requirements for accessibility will be provided.
⑥ Human monitoring	Article 14	When using it, it will be designed and developed in a way that allows natural persons to monitor it effectively.
⑦ Cyber-security	Article 15	We will design and develop cyber security with appropriate levels of robustness and ensure that it performs as designed throughout its operational life.

(ii) The following is an overview of the obligations of providers of high-risk AI System. Violations are subject to penalties of up to EUR15m or 3% of the business operator's total worldwide annual turnover, whichever is higher(Article 99(4)).

①	Provision of AI System that meet compliance requirements	Article 16(a)
②	Display of name, contact details	Article 16(b)
③	Establishment of a quality control system	Article 16(c), 17
④	Preparation of technical documents	Article 16(d), 18
⑤	Storing automatically generated logs (when under control)	Article 16(e), 19
⑥	Implementation of conformity assessment procedures prior to market launch or commercialization	Article 16(f), 43
⑦	Preparing an EU Declaration of Conformity	Article 16(g), 47
⑧	CE Marking	Article 16(h), 48
⑨	Registration in the EU database	Article 16(i), 49
⑩	Implementation of corrective measures and provision of information	Article 16(j), 20
⑪	(if applicable) Providing access to logs, proof of compliance with requirements	Article 16(k)
⑫	Compliance with accessibility requirements	Article 16(l)
⑬	Establishment of an agent within the EU (limited to providers outside the EU)	Article 22

(iii) The obligations of users of high-risk AI System are outlined as follows. Violations are subject to penalties of up to EUR15m or 3% of the business operator's total worldwide annual turnover, whichever is higher (Article 99(4)).

①	Implementation of technical and organizational measures for use in accordance with the instructions for use	Article 26(1)
②	Appointment of supervisors with the necessary skills	Article 26(2)
③	Data governance assurance (when managing input data)	Article 26(4)
④	Implementation of monitoring and notification to relevant parties	Article 26(5)
⑤	Storing automatically generated logs	Article 26(6
⑥	(When using the system at work) Notification to employee representatives, etc.	Article 26(7)
⑦	Implementation of data protection impact assessments as stipulated by EU law	Article 26(9)
⑧	Obtaining prior approval[14]	Article 26(10)
⑨	Notification to the target of the AI system[15]	Article 26(11)
⑩	Cooperation with the regulatory authorities	Article 26(12)
⑪	Implementation of Basic Rights Impact Assessment	Article 27

[14] When using post-remote biometrics for criminal investigations, etc.
[15] When using an AI system for natural persons to make decisions

(3) AI System with limited risk

The AI Act imposes transparency obligations on both providers and users of AI System with limited risks. Therefore, businesses are required to fulfil these transparency obligations clearly and in an identifiable manner, based on the content of the AI system, no later than at the time of the first interaction with a natural person, but only when they are involved as either a provider or user of such AI System (Article 50(5)). Furthermore, for AI System that qualify as both high-risk and limited risk, these transparency obligations will apply cumulatively (Article 50(6)).

Content of the system	Relevant provisions	Measures to Ensure Transparency
AI System designed for interaction with natural persons	Article 50(1)	Notify that the interaction is taking place with an AI system (except in cases where it is obvious to a natural person, considering the context and circumstances in which it is used).
AI System for generating audio, images, videos, or text	Article 50(2)	Indicate on the generated output that it is artificially created.
	Article 50(4)	Disclose that the content is artificially generated when deepfake[16] technology is used.
		Disclose that the text is artificially generated when it is created for the purpose of communicating matters of public interest to the public.
AI System used for emotion recognition or biometric classification	Article 50(3)	Notify the applicable individuals that an AI system is being used.

(4) General-purpose AI model

The AI Act classifies general-purpose AI models into two categories based on their risk levels: (i) standard general-purpose AI models, and (ii) general-purpose AI models with systemic risk. The latter category is subject to more stringent obligations. Therefore, providers of general-purpose AI models must first determine whether their models fall under the category of general-purpose AI models with systemic risk, and then comply with the corresponding obligations.

"Systemic risk" refers to risks specific to cutting-edge, high-performance general-purpose AI models that, due to their scope or their actual or reasonably foreseeable negative impact on public health, safety, security, fundamental rights, or society at large, could significantly affect the EU market and spread widely across the entire value chain (Articles 3(64), 3(65)). Specifically, this includes those evaluated as having significant impact through appropriate technical tools, including indicators and benchmarks[17], or those officially recognized by the European Commission based on certain criteria (Article 51(1)).

(i) The obligations imposed on providers of standard general-purpose AI models are outlined below (Article 53).

① Creation of technical documents that meet certain standards
② Provision of information to providers who are trying to integrate general-purpose AI model into their own AI System
③ Formulation of guidelines for complying with copyright laws in the EU
④ Creation and publication of an overview of the content used for data learning

(ii) The following is an overview of the obligations imposed on providers of AI model with systemic risk (Article 55(1)). These obligations are applied in addition to the obligations imposed on providers of ordinary general-purpose AI model (i) above.

[16] It refers to image, audio, or video content generated or manipulated by AI that resembles real persons, objects, or places and is likely to mislead individuals into believing it is real (Article 3(60)).
[17] If the cumulative number of calculations for data learning exceeds 25 decimal places in floating-point arithmetic, it is presumed to involve systemic risk (Article 51(2)).

① Notification to the European Commission within two weeks of recognizing that it falls under the category of systemic risk ② Implementation of model evaluation, identification of systemic risk, and documentation of measures ③ Risk assessment and implementation of measures to mitigate risks related to development, sales, use, etc. that may result in systemic risk ④ Creating records of serious incidents and reporting them to the authorities ⑤ Securing cyber security for general-purpose AI models and their physical infrastructure

6. Step 6 Preparations for implementation

The AI Act came into effect on August 1, 2024, and most of its provisions will come into force on August 2, 2026 (Article 113). On the other hand, specific provisions for categories such as AI System had been and will continue to be implemented sequentially as follows.

Category	Date of enforcement
Chapter 1 (General Provisions) and Chapter 2 (Prohibited AI Practice)	February 1, 2025 (Article 113 (a))
High-risk AI system	August 2, 2027 (Article 113 (c))
General-purpose AI model	August 2, 2025 (Article 113 (b)). However, for providers that have already placed their products on the market before August 2, 2025, it is sufficient to achieve compliance by August 2, 2027 (Article 111 (3)).

The takeaway

As the use of AI becomes an important and essential issue for businesses, discussions on rules applicable to AI are intensifying in Japan. For example, the Ministry of Economy, Trade, and Industry (METI) published the "AI Business Guidelines" in April 2024, and the Cabinet Office released "Considerations on the AI Regulatory Framework" in May 2024. The AI Act has been established as the world's first comprehensive legal regulation for AI.

As mentioned above, depending on the type of AI and the level of involvement, Japanese companies may also be subject to the AI Act. It is anticipated that the AI Act will significantly influence future discussions on AI-related legal regulations in Japan. Japanese companies are required to understand the provisions of the AI Act, assess their involvement with AI, identify the potential impacts on their business, and take appropriate measures, such as establishing internal systems for regulatory compliance.

Let's talk

For a deeper discussion of how this issue might affect your business, please contact:

PwC Legal Japan
Dai-Ichi Tokyo Bar Association

Otemachi Park Building,1-1-1 Otemachi, Chiyoda-ku, Tokyo 100-0004
TEL: 03-6212-8001
Email: jp_tax_legal-mbx@pwc.com
www.pwc.com/jp/e/legal

Satoshi Mogi
Partner, Attorney-at-Law
satoshi.mogi@pwc.com

Yasuyuki Iwasaki
Partner, Attorney-at-Law / CPA
yasuyuki.iwasaki@pwc.com

Yusuke Kobayashi
Partner, Attorney-at-Law
yusuke.y.kobayashi@pwc.com

Makoto Hibi
Director, Attorney-at-Law
makoto.hibi@pwc.com

Naoki Mizuta
Attorney-at-Law
naoki.mizuta@pwc.com

Ryo Sakamoto
Attorney-at-Law
ryo.r.sakamoto@pwc.com

Makiko Hasuwa
Attorney-at-Law
makiko.hasuwa@pwc.com

Ken Mochizuki
Attorney-at-Law
ken.mochizuki@pwc.com