June 17, 2024

HIGHLIGHTS AND IMPLICATIONS OF EU ARTIFICIAL INTELLIGENCE ACT

I. Imminent Implementation of EU Artificial Intelligence Act

The EU Artificial Intelligence Act (the "**EU AI Act**"), the world's first comprehensive legislation on artificial intelligence, was approved by the EU Council on May 21, 2024. It will come into force twenty days after its publication in the EU Official Journal, with a phased implementation schedule based on the risk level of AI systems. Complete implementation is expected around June, 2026.

The scheduled implementation dates of the EU AI Act vary from 6 to 36 months depending on the specific provisions. We strongly recommend that companies, supplying goods or services to the EU, even if the AI system is located in Korea, assess the applicability of the Act and their obligations thereunder at this stage.

The EU AI Act classifies AI systems into the following categories based on the level of potential risk and impact: (1) Prohibited AI Systems, (2) High-risk AI Systems, (3) General Purpose AI (GPAI) models, and (4) Limited Risk and Minimal Risk AI Systems. Each category has specific obligations.

As the EU AI Act categorizes systems according to their potential risk and impact and sets different obligations for different risk groups, companies are advised to review the relevant obligations in the following three steps and establish the compliance system.

II. Legal Framework of EU AI Act

[Step 1]: Determine whether it is an "artificial intelligence system" under the Act

An artificial intelligence system is defined as "a machine-based system that is designed to operate with varying degrees of autonomy, that is capable of adapting after it is deployed, and that infers, from inputs it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can affect the physical or virtual environment for explicit or implicit purposes".

[Step 2] Assess Risk Groups for AI Systems

A. Prohibited AI Systems

- AI systems that deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect

of materially distorting the behavior of a person or a group of persons by appreciably impairing their ability to make an informed decision

- AI systems that exploit any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behavior of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm
- AI systems that are 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 (this prohibition does not cover 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)
- AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behavior or known, inferred or predicted personal or personality characteristics, with the social score leading to detrimental or unfavorable treatment of certain natural persons or groups of persons
- AI systems 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 (this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity)
- AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage
- AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons
- AI systems that are 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement

  This prohibition shall not apply to the use of AI systems for certain purposes, in so far as such use is strictly necessary, including but not limited to the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, 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 and foreseeable threat of a terrorist attack, the localization or identification of a person suspected of having committed murder, rape, armed robbery, illicit trafficking in narcotic drugs or weapons, participation in a criminal organization, and environmental crime.

B. High-Risk AI Systems

- An AI system is considered high-risk if it is used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonization legislation listed in Annex I (in connection with the product safety).
- Eight High-Risk AI Systems defined in Annex III (in connection with health, safety, and fundamental rights) of the EU AI Act:
  - Remote biometric identification systems and AI systems intended to be used for biometric categorization
  - AI systems intended to be used as safety components of critical digital infrastructure
  - AI systems intended to be used for education and vocational training
  - AI systems intended to be used for employment, workers management and access to self-employment
  - AI systems intended to be used for access to and enjoyment of essential private services and essential public services and benefits
  - AI systems intended to be used by or on behalf of law enforcement authorities
  - AI systems intended to be used for migration, asylum and border control management
  - AI systems intended to be used for administration of justice and democratic processes
- Although AI systems referred to in Annex III shall be considered to be high-risk in principle, they shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making.

C. General Purpose AI Models

- AI models, 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.

D. Minimal Risk AI Systems

[Step 3] Review the Relevant Obligations under Each System

A. Prohibited AI Systems

- Supply to the EU is not permitted

B. High-Risk AI Systems

- To establish a risk management system

  A risk management system shall be established, implemented, documented and maintained to identify and analyze potential risks to health, safety, or fundamental rights, estimate and evaluate these risks, and adopt measures to manage them throughout the AI's lifecycle.

- To Establish Data Governance
  - To identify the legal basis for using the data
  - To review the bias and relevance of the data (considering that the synthetic data may not be able to detect bias)
- Technical Documentation

  Documentation in accordance with Annex IV

- Logs for Transparency and Traceability
  - To maintain event logs to ensure traceability of AI system functionality
  - To create documentation to ensure transparency of deployers
- Human Oversight

  High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use

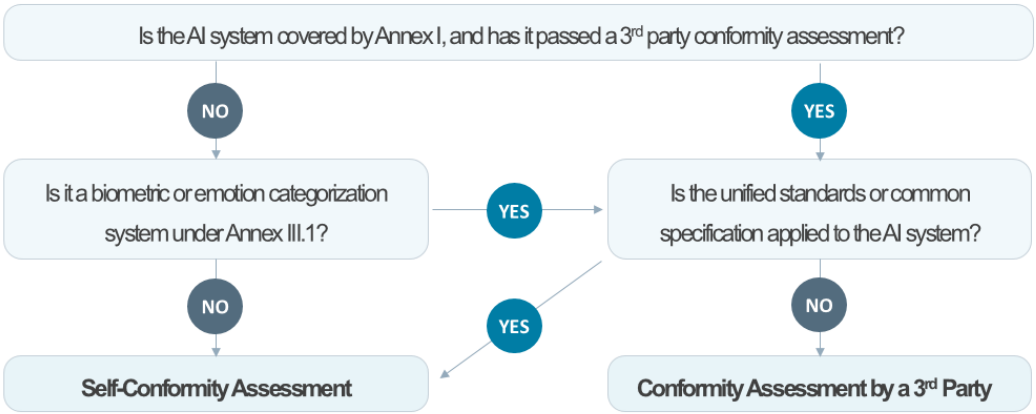
- Cybersecurity

  To create instructions of use to achieve an appropriate level of accuracy, robustness, and cybersecurity

- Quality Management System

  Documentation and implementation for conformity assessment procedures, techniques, procedures, and measures for the design, design control and design verification

- Conformity Assessment



- CE Marking
- Registration

  High-risk AI systems intended to be used for critical infrastructure shall be registered at national level, and the rest shall be registered in the EU database.

C. General Purpose AI (GPAI) Model

- A general-purpose AI model shall be classified as a general-purpose AI model with systemic risk. An AI model is classified as having systemic risk where:
  - high impact capabilities are evaluated on the basis of appropriate technical tools and methodologies or based on a decision of the Commission; and
  - the cumulative amount of computation used for its training measured in floating point operations is greater than 10(^25).
- Obligations for the GPAI classified as having systemic risk
  - To notify the Commission
  - To draw up the technical documentation of the model
  - To draw up a summary about the content used for training of the general-purpose AI model
  - To implement a measure to comply with the Copyright Directive
  - To conduct risk assessment including the systemic risks
  - To put in place internal incident reporting procedures and comply with reporting requirements
  - To ensure an adequate level of cybersecurity protection
- Obligations for the PGAI not classified as having systemic risk
  - To draw up the technical documentation of the model (to applicable to a free and open-source license)
  - To draw up a summary about the content used for training of the general-purpose AI model
  - To implement a measure to comply with the Copyright Directive

D. Limited Risk and Minimal Risk AI Systems

- Voluntary compliance

III. Implications

While the deployers are also subject to obligations in addition to the providers, such as ensuring transparency, some obligations are applicable only within the scope of the deployer's control. Accordingly, it is advisable to address the relevant obligations clearly in the contract with a provider to avoid future disputes.

In addition, the European Commission has delegated the specific implementation of the obligations under the AI Act to subordinate acts (implementing acts) and guidelines. Companies should carefully refer to these establishing a compliance system.

AI regulation is attracting a great deal of attention around the world, with several AI-related bills pending in Korea. Companies are advised to review their obligations in advance, as the EU AI Act is expected to influence future domestic AI regulations.

* * *

For any inquiry or questions regarding the content of this newsletter, please contact us.

Related Professionals

Juho Yoon
Partner
T 82.2.3404.6542
E juho.yoon@bkl.co.kr

Jeonghee Kang
Partner
T 82.2.3404.6480
E jeonghee.kang@bkl.co.kr

Jiyoung Sohn
Senior Foreign Attorney
T 82.2.3404.0241
E jiyoung.sohn@bkl.co.kr