LEGAL UPDATE

BAE KIM & LEE

April 1, 2024

THE NEW EU AI ACT APPROVED BY THE EU PARLIAMENT

On March 13, 2024, Members of the European Parliament voted to pass the Artificial Intelligence Act (the "**AI Act**"), the world's first comprehensive law on artificial intelligence ("**AI**"). After the AI Act enters into force, likely in April-May of 2024, the AI Act would then take effect in phases over a 24-month transitional period. Certain provisions, such as bans on prohibited AI systems, will apply six months after the entry into force date, while codes of practice will apply nine months after, and general-purpose AI rules including governance will apply twelve months after. Obligations for high-risk systems will come into effect 36 months after the entry into force.

I. SCOPE OF THE AI ACT

The AI Act primarily applies to the providers that develop AI systems and to deployers (users) of the AI systems. Specifically, it applies to: (i) organizations located in the EU that use AI systems, (ii) importers, distributors or manufacturers of AI systems in the EU, (iii) providers (inside or outside the EU) that place AI systems on the EU market, and (iv) providers and users of AI systems (inside or outside the EU) where the output is used in the EU. Users herein refer to natural or legal persons that deploy an AI system in a professional capacity, not affected end-users.

II. CLASSIFICATION OF AI BASED ON THE LEVEL OF RISK

The AI Act classifies AI systems according to the potential risks and the level of impact, with different rules and obligations applying to each classification. Non-compliance could lead to fines ranging from 7.5 million EUR or 1.5% of total worldwide annual turnover to 35 million EUR or 7% of total worldwide annual turnover, depending on the infringement and size of the company.

A. Prohibited AI Systems

The AI Act 'prohibits' AI systems which (i) deploy subliminal, manipulative, or deceptive techniques to distort behavior and impair informed decision-making, causing significant harm, (ii) exploit vulnerabilities related to age, disability, or socio-economic circumstances to distort behavior, causing significant harm, (iii) are biometric categorization systems inferring sensitive attributes (e.g., race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), except labelling or filtering of lawfully acquired biometric datasets or when law enforcement categorizes biometric data, (iv) are social scoring, i.e., evaluating or classifying individuals or groups based on social behavior or personal traits, causing detrimental or unfavorable treatment of those people, (v) assess the risk of an individual committing criminal offenses solely based on profiling or personality traits, except when used to augment human assessments based on objective, verifiable facts directly linked to criminal activity, (vi) compile facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage, (vii) infer emotions in workplaces or educational institutions, except for medical or safety reasons, or (ix) are 'real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement, unless it falls under a statutory exception.

B. High-risk AI Systems

The AI Act imposes stringent regulations on high-risk AI systems, mandating extensive governance activities to ensure compliance. High-risk AI systems refer to AI systems (i) used as a safety component or a product covered by EU laws and are required to undergo a third-party conformity assessment, or (ii) used for 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, and administration of justice and democratic processes.

Providers of these high-risk AI systems must meet additional requirements including but not limited to (a) establishing of a risk management system throughout the AI system's lifecycle, (b) conducting data governance, (c) drawing up technical documentation, and (d) designing their high-risk AI system for automatic record-keeping, accuracy, robustness and cybersecurity.

C. General purpose AI ("GPAI") Models

GPAI model refers to an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform 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.

All providers of GPAI model must provide technical documentation, instructions for use, comply with the Copyright Directive, and publish a summary about the content used for training. Providers of free and open license GPAI models only need to comply with the Copyright Directive and publish a sufficiently detailed training data summary, unless they present a systemic risk. Providers of GPAI models deemed to present a systemic risk, whether open or closed, must also conduct model evaluations, adversarial testing, track, document and report serious incidents and ensure adequate levels of cybersecurity protection.

D. Limited Risk and Minimal Risk AI Systems

AI systems of limited risk are subject to transparency requirements while minimal risk AI systems are unregulated under the AI Act.

III. IMPACT OF THE AI ACT ON THE LEGISLATION AND ENFORCEMENT IN KOREA

As the AI Act is applicable to providers outside the EU who place AI systems on the EU market, Korean corporations which do not have their place of business in EU would fall under the purview of the AI Act, if they intend to integrate AI systems in their products or services sold in the EU. Consequently, they would be required to comply with the requirements on the design and operation of AI systems stipulated under the AI Act.

Given that the EU AI Act marks a significant milestone as the world's first comprehensive legislation on AI, the Korean legislators have also proposed a number of bills inspired by its structure and approach. More specifically, certain bills proposed at the National Assembly of Korea mirror specific provisions of the AI Act, including but not limited to taking a risk-based approach as well as delineating the responsibilities of high-risk AI developers and high-risk AI users (i.e., 'Act on the Responsibility and Regulation on AI' bill proposed by Cheol Soo Ahn and 10 others).

* * *

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

Related Professionals

Taeuk Kang
Partner
T 82.2.3404.0485
E taeuk.kang@bkl.co.kr

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

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

bkl BAE KIM & LEE

This publication is provided for general informational purposes only, and should not be construed as legal or professional advice on any particular matter, nor create an attorney-client relationship. Before you take any action that may have legal implications, please inquire with your contact at Bae, Kim & Lee LLC, or the authors of this publication.