LEGAL UPDATE

PIONEERING AI GOVERNANCE: A FIRST LOOK INTO THE LANDMARK EU AI ACT

1. Artificial Intelligence ("**AI**") is well poised to usher in another technological revolution, replacing the present digital revolution which brought us computers and the Internet. It has now become nearly ubiquitous in modern society, permeating our daily lives with innovative products such as voice recognition devices (e.g., "Siri" and "Alexa"), virtual assistant (e.g. "Google Assistant"), self-driving vehicles (e.g., "Tesla") and facial recognition on smartphones. However, the technology has also raised concerns about its negative impact.

2. On 13 March 2024, the European Parliament approved the **Artificial Intelligence Act** (the "**Act**") to govern AI and the use of AI. While the Act recognises that AI can contribute to a wide range of economic, environmental and social benefits, it can also be abused and used to cause harm to others. As such, there is a need to ensure that AI is "trustworthy and safe", and is "developed and used in accordance with fundamental rights and obligations".

3. Unlike a sectoral or piecemeal approach, the Act is a broad-based legislation that applies to providers, deployers and importers of AI systems as well as product manufacturers that implement AI systems in their products. AI systems falling within the prescribed definition and scope of the Act must comply with the relevant obligations. The failure to comply with these obligations may lead to enforcement actions and penalties under the Act.

4. This update seeks to provide a first look into the Act by providing an overview of the obligations under the Act, its other features, and the possible preparatory steps which local businesses and organisations that deploy AI systems in the European Union ("**EU**") may wish to take ahead of the commencement of the Act which is expected to be in Q2 or Q3 of 2024, with transition periods for complying with various requirements ranging from 6-24 months.

Obligations under the Act

5. The Act distinguishes between "AI system" and "general-purpose AI model" ("**GPAI model**") and subjects them to different obligations. Under the Act, they are defined in a technology-neutral manner.

6. "AI system" is 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*".

15 April 2024

For any queries relating to this article, please contact

Tan Tee Jim, S.C.
tanteejim@leenlee.com.sg

Basil Lee
basillee@leenlee.com.sg

Authors:

Tan Tee Jim, S.C.
Basil Lee
Chee Kai Hao
Poon Chong Ming

Lee & Lee
25 North Bridge Road
Level 7
Singapore 179104
Tel: +65 6220 0666

For more legal updates, please visit the News & Publication Section of Lee & Lee's website at www.leenlee.com.sg, or follow Lee & Lee's Facebook page at www.facebook.com/leenlee.com.sg/ and Lee & Lee's LinkedIn page at https://lnkd.in/g6bNfv8G.

7. GPAI model means "*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 released on the market*".

A. Risk-based approach towards regulation of AI systems

8. The Act adopts a "*clearly defined risk-based approach*" that classifies AI systems according to the risks that they pose. AI systems that pose higher levels of risks are subject to more stringent regulations. AI systems with unacceptable risks are prohibited. This ensures that AI systems are regulated in a proportionate and effective manner.

    a) Prohibited AI practices (Article 5)

    The Act imposes an outright prohibition on AI practices that manipulate or deceive people into harmful decisions, exploit vulnerable groups, infer sensitive biometric traits (such as race, religion, or sexual orientation), unjustly use social scoring, perform biometric identification in public spaces, predict criminal behaviour based on profiling, create facial recognition databases through mass data scraping, and infer emotions in work or education settings except for health or safety reasons.

    b) High-risk AI systems (Articles 6-49)

    AI systems are classified as high-risk if they have a significant potential to impact the safety and fundamental rights of individuals and are typically used in critical sectors and for sensitive applications. Examples include healthcare (medical devices, diagnosis, and patient care), transport and infrastructure (critical infrastructure, traffic management, and public transport), public sector (government services, law enforcement, and administration of justice), private sector essentials (finance, insurance, and energy management), employment and education (recruitment, staff management, and access to education) and biometric identification.

    These AI systems are subject to rigorous obligations under the Act. They must comply with requirements concerning risk management, data governance, technical documentation, record-keeping, transparency, and disclosure to deployers. There are also requirements to maintain human oversight as well as appropriate levels of accuracy, robustness and cybersecurity. Stringent obligations are imposed for providers, importers and distributors.

    c) Limited risk AI systems (Articles 6(3) and 50)

    These systems present a lower level of risk compared to high-risk systems, as they are unlikely to pose a significant risk of harm to the health, safety or fundamental rights of natural persons. Such systems include those that are capable of generating synthetic text and media (e.g. chatbot and deepfake), and those used for emotion recognition or biometric categorisation purposes. While these AI systems may have the potential to mislead individuals, spread misinformation, and misuse private data, they do not inherently pose the same level of risk as high-risks AI systems.

As such, these systems are primarily subject to transparency obligations, whereby providers must inform users that they are interacting with an AI system. Data protection requirements under the General Data Protection Regulation (the "**GDPR**") also continue to apply to these systems.

d) Minimal risk AI systems

AI systems implemented in applications such as AI-enabled video games and spam filters are considered low-risk in nature because they are unlikely to adversely impact one's fundamental rights or pose serious safety implications. These systems are not regulated under the Act.

B. Differentiated obligations for providers, product manufacturers, importers, and deployers of high-risk AI systems

9. In high-risk AI systems, the Act differentiates the responsibilities between providers, product manufacturers, importers, and deployers.

10. **Providers** are parties (whether a natural or legal person, public authority, agency, or other body) who place on the market or put into service AI systems in the EU, and these providers can be located outside of the EU. In addition to complying with the requirements for high-risk AI systems set out above in paragraph 4(b), providers must also, amongst others, implement a quality management system (Article 17), keep necessary documentation (Article 18), ensure that the AI systems undergo relevant conformity assessments (Article 43), provide a declaration of conformity, affix CE marking, and adhere to registration requirements (Article 49).

11. **Product manufacturers** are creators of products which utilise AI system(s). Product manufacturers would also be considered as providers, and subject to the same requirements as providers, if the AI system used in their product is high-risk, and the high-risk AI system is a safety component of a product under EU harmonisation legislation (as listed in Section A of Annex I of the Act), and is placed on the EU market together with the product under the name or trademark of the product manufacturer (or put into service under the name or trademark of the product manufacturer after the product has been placed on the EU market) (Article 25(3)).

12. **Importers** are natural or legal persons located or established within the EU that place on the market an AI system bearing the name or trademark of a natural or legal person established in a non-EU country. Importers are obligated to confirm that high-risk AI systems meet the requirements of the Act (Article 23(1)), and if not, to reject placing the system on the market (Article 23(2)). If placed on the market, importers must work with authorities to reduce and mitigate risks (Article 23(7)). Separately, importers could also be considered as providers if they brand an existing high-risk AI system with their name or trademark, substantially modify a high-risk AI system already in the market or service in a manner that maintains its high-risk status, or alter the intended purpose of a non-high-risk AI system such that it is reclassified as high-risk (Article 25(1)). Consequently, such importers would be subject to the same requirements as the providers.

13. **Deployers** are parties (whether a natural or legal person, public authority, agency, or other body) who use an AI system in a professional capacity, and are not end-users (Article 26). Deployers must take measures to ensure that high-risk AI systems are being used in accordance with their instructions (Article 26). This includes overseeing human interaction with the AI system,

ensuring input data relevance, and maintaining logs. They must also monitor the system's operation and inform providers of any risks or serious incidents (Article 26).

C. GPAI model

14. Unlike AI systems, AI models may be described as components of AI systems, and lack other components such as a user interface. An AI model is only regulated under the Act if it falls within the definition of GPAI model (see [6] above). However, AI models *"used for research, development or prototyping activities before they are released on the market"* are expressly carved out from the definition of GPAI model.

15. Under the Act, providers of GPAI models must keep updated technical documentation of their models, covering training and testing processes, for oversight by the AI Office and national authorities (Article 53(1)(a)). Providers are also required to share essential information with other AI system providers using their GPAI models, ensuring understanding of capabilities and compliance (Article 53(1)(b)). Adherence to EU copyright law and the public sharing of summary of training content are also mandated (Article 53(1)(c-d)).

16. For GPAI models with systemic risk (i.e. if there are actual or reasonably foreseeable negative effects such as major accidents, disruption in critical sectors, threats to public health, safety, and democracy), additional responsibilities include rigorous evaluations for risk mitigation, documenting and reporting of serious incidents, and the implementation of adequate cybersecurity protection (Article 55(1)(a-d)). Notably, providers outside the EU must also appoint a representative within the EU (Article 54).

D. Enforcement and penalties

17. Under the Act, Member States are required to establish rules for penalties that are effective, proportionate and dissuasive. In particular, Member States shall take into consideration the interests of SMEs and startups, and their economic viability when determining the penalties (Article 99(1)). Violations of prohibited AI practices can lead to fines up to €35 million or 7% of the undertaking's total worldwide annual turnover, whichever is higher (Article 99(3)). Other specific breaches and non-compliance by providers, importers, and others can result in fines up to €15 million or 3% of the undertaking's annual turnover (Article 99(4)). Supplying incorrect or misleading information to authorities may be penalised with fines up to €7.5 million or 1% of annual turnover (Article 99(5)). Factors influencing the amount of fine include the nature of the infringement, duration, operator's size and previous violations (Article 99(7)).

Other features of the Act

A. Extra-territorial effect of the Act

18. As the Act applies to any AI systems that are either introduced into the EU market or used within the EU, the Act can have extra-territorial effect. Developers or providers of AI Systems outside of the EU who intend to introduce their AI systems into the EU market or are already doing so should therefore look to comply with the Act ahead of its commencement dates, and may wish to take the following preparatory steps:-

    a. Assess how the AI systems will be regulated under the Act, including whether the AI systems are among those prohibited by the Act (Article 5), or whether their AI systems

will be regulated as a high-risk, limited risk or minimal risk AI systems. Depending on the applicable requirements, the relevant stakeholders should take steps and implement measures to adhere to the relevant obligations such as risk management, data governance, transparency and human oversight.

b. Determine if the AI systems involve a GPAI, and if so, to adhere to the standards of ensuring high-quality data, transparency, and compliance with data protection and privacy standards (Articles 53 and 54).

c. Consider if there is a need to appoint a representative within the EU to facilitate compliance and communication with the EU authorities (Article 22).

B. Standardisations of requirements and obligations

19. To provide clarity on complying with the Act, the Act allows the Commission to request the European standardisation organisations to develop standards for complying with the requirements applicable to high-risk AI systems as well as the transparency obligations for limited risk AI systems (Article 40). If approved and published harmonised standards have been adhered to, there can be a presumption of conformity under the Act (Article 40). This means that if a high-risk AI system can conform to the corresponding standards that cover the obligations or requirements under the Act, the AI system is presumed to comply with those obligations or requirements.

20. The development of standards by standardisation organisations for complying with the Act is a step in the right direction. Notwithstanding the difficulty of developing such standards, developing precise guidelines and a comprehensive standards framework will bring much needed legal certainty and reduce ambiguity for all stakeholders involved. This will also reduce compliance costs.

21. Stakeholders who are involved in providing or deploying AI and AI systems will likely stand to gain from closely monitoring and, where possible, aligning themselves with the development of standards for AI governance in various jurisdictions and sectors, including industry-led initiatives.

C. Facilitating AI innovations and compliance

22. Although the Act imposes stringent obligations on the use of AI, it also strives to foster AI innovation. The Act requires Member States to establish at least one AI regulatory sandbox, which aims to foster development and testing in a risk-controlled environment (Article 57).

23. Further, Member States shall give SMEs and startups priority in accessing sandboxes and facilitate their participation in standardisation development processes (Article 62). To ease the burden on microenterprises, the Act provides that guidelines will be developed to help smaller companies comply with the requirements concerning the quality management system. As these requirements can be challenging or expensive for smaller companies to adhere to, such guidelines that shall be developed will support the involvement of smaller companies in high-risk AI sectors (Article 63).

Conclusion

24. As mentioned earlier, there are transitional periods for complying with the various requirements of the Act. They include bans on prohibited practices (6 months after entry into force of the Act), codes of practice (9 months after entry into force), rules concerning GPAI models (12 months after entry into force), and obligations concerning high-risk AI systems (36 months after entry into force).

25. The Act is the first legislation of its kind in the world. Like the European Union's General Data Protection Regulation governing the use of data, the Act could set a global standard for governing AI and the use of AI. It would therefore do well for companies and other stakeholders in Singapore to be familiar with its rules and regulations, especially how their businesses and operations in Singapore can be impacted by the Act.

26. If you have any question regarding the Act, please contact our Mr. Tan Tee Jim, SC (tanteejim@leenlee.com.sg) or Mr. Basil Lee (basillee@leenlee.com.sg).

About Lee & Lee

Lee & Lee is one of Singapore's leading law firms being continuously rated over the years amongst the top law firms in Singapore. Lee & Lee remains committed to serving its clients' best interests, and continuing its tradition of excellence and integrity. The firm provides a comprehensive range of legal services to serve the differing needs of corporates, financial institutions and individuals. For more information: visit www.leenlee.com.sg.

The following partners lead our departments:

Kwa Kim Li Managing Partner kwakimli@leenlee.com.sg	Quek Mong Hua Litigation & Dispute Resolution quekmonghua@leenlee.com.sg	Owyong Thian Soo Real Estate owyongthiansoo@leenlee.com.sg
Tan Tee Jim, *SC* Intellectual Property tanteejim@leenlee.com.sg	Adrian Chan Corporate adrianchan@leenlee.com.sg	Louise Tan Banking louisetan@leenlee.com.sg