Table 1. Comparison of Key Aspects of the South Korea AI Framework Act and EU AI Act

Aspects	South Korea AI Framework Act	EU AI Act
Tiered categorization	The AI Framework Act employs a simpler classification than the EU AI Act's. ● The majority of obligations apply to "high-impact AI" (see **Articles 2(4), 31, and 33-36**). ● "Generative AI" is subject to transparency obligations (see **Articles 5, and 31**.	The AI Act classifies AI systems according to four risk levels: ● Prohibited AI systems (see **Article 5**), ● High-risk AI systems (see **Article 6**). ● Limited risk (AI systems subject to lighter obligations, primarily focusing on transparency – see **Article 50**). ● Minimal risk (unregulated). The Act also contains specific provisions on general-purpose AI models with systemic risk (see **Article 51**).
Classification of high-impact / high-risk AI systems	Under **Article 2(4)** of the AI Framework Act, an AI system is considered "high-impact" if it: ● may have a significant impact on, or pose a risk to, human life, physical safety, or fundamental rights; and ● is used in any of the following areas: ○ Energy supply; ○ Production of drinking water;	Broadly, under **Article 6** of the AI Act, an AI system is considered high-risk if it: ● is intended to be used as a safety component of a product, or is itself a product, that is required to undergo a third-party conformity assessment under certain EU product safety laws; or ● poses a serious risk of harm to people's health, safety, or fundamental rights, and is listed in Annex III to the AI Act. **Annex III of the AI Act** lists a range of high-risk AI systems in 8 areas: ● Biometrics;

	○ Establishment and operation of a system for providing and using health care; ○ Development and use of medical devices; ○ Safe management and operation of nuclear materials; ○ Analysis and utilization of biometric information for criminal investigations or arrests; ○ Judgment or evaluation that has a significant impact on the rights and obligations of an individual, such as employment and loan screening; ○ Major operation and management of transportation means, transportation facilities, and transportation systems; ○ Decision-making by the state, local governments, public institutions that affect the public; ○ Student evaluation in early childhood education, elementary education, and secondary education; and ○ Other areas that have a significant impact on the	● Critical infrastructure; ● Education and vocational training; ● Employment, management of workers, and access to self-employment; ● Essential private and public services; ● Law enforcement; ● Migration, asylum, and border control management; and ● Administration of justice and democratic processes.

	safety of human life and body and the protection of basic rights, as prescribed by Presidential Decree.	
Requirements for high-impact / high-risk AI systems	**Articles 34** of the AI Framework Act lists the obligations of AI Business Operators who provide high-impact AI or products or services using high-impact AI. These include: ● Establishing and implementing a risk management plan; ● Establishing and implementing a plan to explain the results of AI decision-making, including the criteria used to derive these results, and the data used to train the AI system; ● Establishing and implementing measures to protect users; ● Ensuring human management and supervision of high-impact AI; and ● Preparing and retaining documents to verify measures taken to ensure the safety and reliability of high-impact AI. This list is nonexhaustive, and the National AI Committee is empowered to supplement the list with additional obligations.	**Section 2** of the AI Act outlines requirements for high-risk AI systems. These include: ● Establishing, implementing, documenting, and maintaining a risk management system (**Article 9**); ● Satisfying data quality and governance requirements (**Article 10**); ● Drawing up, and maintaining technical documentation (**Article 11**); ● Implementing logging capabilities (**Article 12**); ● Ensuring transparency and provision of information to deployers (**Article 13**); ● Implementing human oversight (**Article 14)**; ● Ensuring accuracy, robustness, and cybersecurity (**Article 15**).

Prohibited AI systems	The AI Framework Act does not explicitly prohibit any AI use cases.	Broadly, **Article 5** of the AI Act prohibits eight AI practices: ● Harmful AI-based manipulation and deception; ● Harmful AI-based exploitation of vulnerabilities; ● Social scoring; ● Individual criminal offence risk assessment or prediction; ● Untargeted scraping of the internet or CCTV material to create or expand facial recognition databases; ● Emotion recognition in workplaces and education institutions; ● Biometric categorisation to deduce certain protected characteristics; and ● Real-time remote biometric identification for law enforcement purposes in publicly accessible spaces.
Transparency and user protection	AI Business Operators must notify users in advance when offering High-Impact or Generative AI services and label AI-generated content (**Article 31**). While not strictly a transparency obligation for the end-user, **Article 32(2) requires AI business operators whos**e AI system's cumulative computational volume used for learning exceeds a certain standard	The AI Act introduces specific disclosure obligations to ensure that humans are informed that they are interacting with AI systems (**Article 50**). Providers of generative AI must ensure that AI-generated content is identifiable. Certain AI-generated content – namely deepfakes and text published with the purpose to inform the public on matters of public interest – must be clearly and visibly labelled, (**Article 50(4)**).

	to submit the results of their risk identification, assessment, and mitigation efforts, as well as their risk management system establishment, to the Minister of Science and ICT. **Article 34(1)**, which outlines the obligations of AI Business Operators regarding high-impact AI also includes elements of transparency by requiring such Operators to establish and implement a plan to explain the results of AI decisions.	Providers of general-purpose AI models must also maintain technical documentation on these models, and make this documentation and other information available to providers of AI systems who intend to integrate the general-purpose AI model into their AI systems. They must also make publicly available a detailed summary about the content used for training of the model (**Article 53 and Annex XI**). The Act also includes transparency and the provision of information to deployers (**Article 13**). The Act also grants individuals the right to receive clear explanations from deployers about the role of high-risk AI systems in decisions that legally affect them or significantly impact their health, safety, or fundamental rights (**Article 86**).
Oversight and Implementation	The Act mandates transparency obligations for AI Business Operators providing high-impact or generative AI, requiring advance notification and clear indication to users (**Article 31**). Operators of AI systems exceeding a computational threshold must ensure AI safety through risk management (**Article 32**). Providers of high-impact AI face obligations for safety and reliability (**Article 34**), and are also encouraged to conduct impact assessments (**Article 35**).	Broadly, high-risk AI systems are subject to strict obligations (see **Articles 9-14** of the AI Act) before they can be put on the European market. Once an AI system is on the market, providers, importers, distributors, and deployers of high-risk AI systems are subject to a range of further obligations (see **Articles 16-27** of the AI Act). Providers of general-purpose AI models with systemic risk are also subject to specific obligations (see **Articles 53-55** of the AI Act).

Governance bodies	The main governance body responsible for administering the AI Framework Act is the **MSIT**, which holds significant responsibility for the administration of the Act and is tasked with, among others, establishing and implementing the triennial Basic AI Plan (**Article 6**). Other relevant bodies include: ● The **National AI Committee** under the President, which is tasked with deliberating on major AI-related policies (**Article 7**). ● The **National AI Policy Center** designated by MSIT, which is tasked with performing various tasks necessary for the development of AI-related policies and the establishment and dissemination of international standards (**Article 11**). ● The **AI Safety Research Institute** operated by MSIT, which is tasked with research policies, standards, and methods to protect citizens from AI-related risks (**Article 12**).	The main governance bodies responsible for administering the AI Act include: ● The **EU AI Office** (built inside the European Commission) has several key functions in administering the AI Act, especially concerning general-purpose AI models. ● **Individual EU Member States' designated AI authorities and market surveillance authorities** are responsible for implementing, supervising, and enforcing the EU AI Act. ● The **European Data Protection Supervisor** (EDPS) acts as the competent market surveillance authority for AI systems put into service or used by EU institutions, agencies, offices, and bodies, except when the Court of Justice of the European Union is acting in its judicial capacity. The EDPS also has the power to impose fines on these entities. The EU AI Act's governance is steered by: ● The **EU AI Board (Board)**, which is composed of representatives from the EU Member States and is tasked with advising and assisting the Commission and the Member States in order to facilitate the consistent and effective application of the AI Act. The EDPS and the AI Office can participate but they don't have voting rights (see **Articles 65-66**). ● The **Advisory Forum**, which represents a diverse selection of commercial and

		non-commercial stakeholders and is tasked with providing technical expertise and advising the Board and the Commission (see **Article 67**). ● The **Scientific Panel**, composed of independent experts in the field of AI (see **Articles 68-69**).
Enforcement and penalties	The AI Framework Act has significantly lower monetary fines than those provided by the EU AI Act. The maximum fines under the AI Framework Act is KRW 30 million (approx. USD 21,000), which only applies to certain violations of the Act (**Articles 42-43**).	The AI Act imposes strict financial penalties, ranging from €7.5 million to €35 million (approx. USD 7.8 million to USD 36.5 million), or 1% to 7% of global turnover, depending on the violation (**Article 99**).
Innovation support	The Act aims to foster the development and application of AI technologies and the growth of the AI industry. It mandates the MSIT Minister to establish a Basic AI Plan to promote AI technology and industry and enhance national competitiveness (**Article 6**). Chapter III of the AI Framework Act also contains detailed provisions on developing AI technology and promoting AI technology. For instance, it enables the government to support projects related to AI technology development, research,	**Articles 57-63** of the AI Act outline in detail a framework for AI regulatory sandboxes. Member States must create at least one sandbox per State by August 2026 to provide controlled environments for AI innovation. These sandboxes allow developers to test AI systems under regulatory supervision, with provisions for personal data processing, real-world testing protocols, and informed consent requirements. Special measures support small and medium enterprises (SMEs) and startups, including priority sandbox access, simplified compliance options for microenterprises, and targeted awareness campaigns.

	commercialization, and information sharing, as well as the standardization of AI technology and the establishment of policies related to AI learning data (**Articles 13-15**). Furthermore, **Articles 16-18** outline support for the introduction and use of AI technology by enterprises, with special consideration for SMEs, and includes measures to activate startups in the AI industry. **Articles 19-26** of the Act promote AI innovation and growth through cross-industry collaboration, regulatory improvements, and securing AI talent. The Act also supports international cooperation, AI clusters, and a verification base. Additionally, it addresses AI data center policies and establishes the Korea Artificial Intelligence Promotion Association.	