DECODING THE EU AI ACT: COMPLIANCE, IMPACT AND GLOBAL IMPLICATIONS

1. INTRODUCTION

As artificial intelligence ("**AI**") continues to evolve and permeate various sectors, the need for robust regulatory frameworks has become paramount. The European Union ("**EU**") has taken a pioneering step in this direction by enacting the European Union Artificial Intelligence Act ("**EU AI Act**" or "**Act**") in March 2024.[1] The Act came into force on August 01, 2024.[2] This landmark legislation establishes a comprehensive legal framework for the use of AI within the EU and primarily aims to promote a human-centric and trustworthy adoption of AI while safeguarding health, safety and fundamental rights.[3]

The EU AI Act's scope is broad, applying to *inter alia* all providers, importers, distributors and deployers of 'AI systems'[4] that are marketed or used within the EU, regardless of whether those providers or developers are established in the EU or another country.[5] This extraterritorial applicability mandates that companies based outside the EU, including those in India, must comply with the Act should they wish to operate within the EU market. The Act adopts a risk-based approach, categorising AI systems into unacceptable-risk, high-risk, limited-risk and minimal-risk categories. It specifies tailored obligations for each category to ensure ethical, transparent, and safe AI usage.

This article highlights the key compliance requirements under the EU AI Act for various AI systems and examines the significant impact of the Act on companies (including Indian entities providing AI systems in the EU). Additionally, the article discusses the potential global influence of the Act as a model for AI regulation and provides a way forward for businesses to align with this comprehensive regulatory framework.

2. KEY TAKEAWAYS FROM THE EU AI ACT

2.1 COMPLIANCES

Understanding the key compliance requirements under the EU AI Act is essential for companies to ensure that they meet the Act's stringent standards. This section outlines the obligations for the various risk categories of AI systems, including 'General-Purpose AI Models'[6] ("**GPAI**").

(a) Unacceptable-risk AI Systems[7]

[1] Artificial Intelligence Act: MEPs adopt landmark law, can be accessed here; EU AI Act can be accessed here.
[2] AI Act enters into force, European Commission, can be accessed here.
[3] Charter of Fundamental Rights of the European Union, can be accessed here.
[4] Article 3(1) of the EU AI Act: "AI system means a machine-based system that is designed to operate with varying levels of autonomy and 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".
[5] Recital 22 of the EU AI Act.
[6] Article 3(63) of the EU AI Act: "general-purpose AI 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 placed on the market".
[7] Article 5 of the EU AI Act.

Unacceptable-Risk AI systems, including *inter alia* manipulative AI systems, social credit scoring systems, emotion-recognition systems at work and educational institutions, are prohibited due to their potential detrimental impact and risk of leading to discriminatory practices. Consequently, no compliance requirements have been prescribed for these systems.

(b) **High-risk AI Systems**[8]

High-risk AI systems identified in areas[9] such as critical infrastructure, education and vocational training, employment, workers management and access to self-employment, law enforcement, administration of justice and democratic processes, migration, asylum, and border control face stringent compliance requirements. The Act stipulates several requirements for different parties, and some of the more crucial ones are briefly outlined below:

(i) Providers

'Providers' are natural or legal persons who develop an AI system or a GPAI, or those who have an AI system or GPAI developed with the intention to place it on the EU market or put it into service under their own name or trademark.[10] They bear the primary responsibility of ensuring the AI system's compliance with the Act. A few material obligations include:

- ***Technical Documentation***: Preparing technical documentation that will be relied upon throughout the lifecycle of the AI system to demonstrate compliance with the Act, before it is placed in the market.[11]
- ***Registration:*** Registering the AI system with the EU database to facilitate monitoring and compliance checks.[12]
- ***Risk Management System***: Establishing, maintaining and reviewing a risk management system throughout the lifecycle of the AI system for identifying known and reasonably foreseeable risks, evaluating emerging risks and adopting targeted measures to address these identified risks.[13]
- ***Transparency and Human Oversight***: Ensuring transparency to enable users to interpret the AI system's output, capabilities and limitations. Additionally, the design should facilitate human oversight to allow meaningful intervention when necessary.[14]
- ***Quality Management System ("QMS"):*** Maintaining a quality management system to ensure compliance with the Act,[15] and conducting conformity assessments[16] to verify that the AI system meets the requirements before it can be placed on the EU market or put into service and obtaining the Conformité Européenne ("**CE**") marking.

[8] Article 6 of the EU AI Act.
[9] Annex III of the EU AI Act.
[10] Article 3(3) of the EU AI Act.
[11] Article 11 of the EU AI Act.
[12] Article 49 of the EU AI Act.
[13] Article 9 of the EU AI Act.
[14] Article 13 and Article 14 of the EU AI Act.
[15] Article 17 of the EU AI Act.
[16] Article 43 of the EU AI Act.

- ***Data Governance:*** Conducting data governance to ensure the relevance and accuracy of the training, validation, and testing datasets.[17] This would also include observance of compliances stipulated under the EU General Data Protection Regulation ("**GDPR**") for the purposes of processing personal data.

Some other key compliances outlined in the EU AI Act vis-à-vis the providers include (a) enabling automatic recording of events (logs) over the lifetime of the AI system[18], (b) ensuring adherence to appropriate levels of accuracy, robustness and cybersecurity, post-deployment monitoring,[19] and (c) incident reporting to the relevant authorities of serious incidents, including taking corrective measures and cooperating with them.[20]

(ii) Deployers[21]

'Deployers' are natural or legal persons, public authority, agency or any other body who use an AI system under their own authority[22] and are required to adhere to certain critical obligations under the Act. Similar to providers, deployers must ensure human oversight of the AI systems by assigning this responsibility to persons who have the necessary competence, training and authority. At the same time, deployers also have similar incident reporting obligations to the relevant authorities as the providers. In addition to the above, deployers who are employers are given the responsibility of informing workers' representatives and affected workers that they would be subject to the use of a high-risk AI system in the event such an AI system is used at a workplace. Another significant obligation is to monitor the operation of the AI system basis the instructions for use provided by the provider.

(iii) Importers[23]

An importer refers to a natural or legal person located or established in the EU who places on the market an AI system bearing the name or trademark of a natural or legal person established in a third country.[24] A few material obligations of importers include:

- ***Conformity Assessment:*** Ensuring that the provider has carried out the appropriate conformity assessment procedure and prepared the required technical documentation.
- ***CE Marking and Documentation:*** Verifying that the AI system bears the required CE marking and is accompanied by the necessary documentation and instructions.
- ***Cooperation with Authorities:*** Cooperating with national authorities in any actions taken by them to eliminate risks posed by AI systems placed by them on the market.

(c) **Limited-risk AI Systems**

Limited-risk AI systems pose moderate manipulation risks primarily associated with a lack of transparency. Accordingly, the Act, similar to providers of high-risk AI systems, stipulates

[17] Article 10 of the EU AI Act.
[18] Article 12 of the EU AI Act.
[19] Article 72 of the EU AI Act.
[20] Article 21 of the EU AI Act.
[21] Article 26 of the EU AI Act.
[22] Article 3 of the EU AI Act.
[23] Article 23 of the EU AI Act.
[24] Article 3 of the EU AI Act.

transparency related obligations for the providers and deployers of these AI systems. As part of these obligations, providers and deployers of such AI systems are required to ensure that users are informed when they are interacting with an AI model. Additionally, AI systems that either generate or manipulate images, audios or video content, such as deepfake, are also required to make necessary disclosures informing the final viewers that the content has been artificially generated or manipulated.[25] This obligation, however, is not applicable to specific use-cases authorised by law to detect, prevent or investigate a criminal offense.[26]

(d) **Minimal-risk AI Systems**

Minimal-Risk AI systems, which include spam filters, inventory management systems, and AI-enabled video games, are not subject to any mandatory obligations under the Act. However, these systems are encouraged to follow voluntary codes of conduct to promote ethical AI use and transparency.[27]

(e) **GPAI Models**

GPAI models include models that are trained on vast data sets and can perform a wide range of tasks, but exclude those used before release on the EU market for research, development and prototyping activities.[28] Such models are *inter alia* required to adhere to transparency obligations, maintain technical documentation, implement policies to ensure compliance with the EU laws on copyright and related rights, and publicly share a detailed summary of the content used for training the GPAI model, among others.[29] The providers of GPAI models are also required to ensure that users in downstream applications comply with the Act's requirements.[30] It is also important to note that providers of GPAI models established in third countries must appoint an authorised representative established in the EU, before making their GPAI available in the EU market.[31]

2.2 ENFORCEMENT AND SUPERVISION/NON-COMPLIANCES

The Act entrusts the responsibility of overseeing compliance and enforcement activities to the EU AI Office, supported by a scientific panel of independent experts.[32] Non-compliance with the Act can result in severe penalties, including substantial fines depending on the severity and nature of the non-compliance, market access restrictions whereby non-compliant AI systems may be barred from entering or continuing to operate within the EU, and reputational damage significantly impacting the company's market standing. Further, non-compliance can also lead to operational disruptions which can affect a company's overall efficiency and productivity, potentially leading to a competitive disadvantage in the market.

3. IMPACT ON THE MARKET

[25] Article 50 of the EU AI Act.
[26] Article 50 of the EU AI Act.
[27] Article 95 of the EU AI Act.
[28] Article 3 of the EU AI ACT.
[29] Article 53 and Article 55 of the EU AI Act.
[30] Article 53 and Annex XII of the EU AI Act.
[31] Article 54 of the EU AI Act.
[32] Article 68 of the EU AI Act.

The EU AI Act introduces a complex regulatory framework that will significantly impact the way companies develop, deploy and use AI systems. To effectively navigate the Act's extensive compliance requirements, companies must adopt a strategic and proactive approach. The first step involves conducting a comprehensive assessment of their AI systems to determine their classification under the Act and identifying corresponding obligations. This foundational assessment is essential for developing a targeted and effective compliance strategy.

Companies dealing with unacceptable-risk AI systems must reduce the risk levels of such systems, or if remedial measures are not feasible within the prescribed timeframe, withdraw their products from the EU market. This assessment is critical considering the provision banning unacceptable-risk AI systems will come into force 6 (six) months after the Act's entry (i.e., February 2025), while the other provisions will be implemented later [for instance, the obligations of high-risk AI systems will come into force 24 (twenty-four) months (i.e., August 2026) after the Act's entry].[33]

Companies will also need to invest significantly in compliance infrastructure, ongoing monitoring mechanisms and human oversight measures. Additionally, they will need to formulate relevant policies and procedures for responsible AI development and deployment. Implementing these measures will involve substantial costs and resources as they will have to be undertaken throughout the AI system's lifecycle. These costs and operational complexities could deter smaller companies from entering the EU market or require them to seek partnerships with larger firms to share the compliance obligations.

Maintaining a robust QMS is essential to ensure that the AI system consistently meets quality standards and regulatory requirements. This involves conducting regular internal audits to evaluate the QMS's effectiveness, identifying areas for improvement and implementing continuous improvement processes. Additionally, companies must establish mechanisms to detect and identify incidents, promptly notify relevant authorities and stakeholders about serious incidents, and implement corrective actions to mitigate their impact and prevent recurrences in future.

Continuous education and training of personnel also becomes vital as they will need to be updated on regulatory changes and best practices. Companies must foster a culture of transparency and ethical AI usage by informing stakeholders about the AI systems' capabilities, limitations, and ethical considerations. AI systems that generate or manipulate content, such as deepfakes, must explicitly inform users when interacting with AI-generated or manipulated content

4. WAY FORWARD

The EU AI Act represents a landmark piece of legislation that sets a global precedent for regulating AI. By adopting a risk-based approach and imposing stringent compliance obligations, the Act seeks to balance innovation with the protection of fundamental rights. Although companies will be required to make significant investments in resources, expertise and infrastructure, the Act also presents opportunities for companies to demonstrate leadership in responsible AI development and gain a competitive advantage.

The Act's extraterritorial application highlights the EU's ambition to shape the global AI landscape. Due to the EU's large market size and its impact on global trade, companies worldwide often adopt EU standards to access this market, a phenomenon known as the '*Brussels Effect*'[34]. Similar to the GDPR, which sets a global benchmark for data privacy, the Act is expected to shape AI practices worldwide. This

[33] AI Act Implementation: Timelines & Next steps, can be accessed here.
[34] The Brussels Effect: How EU's law affects AI regulations globally, can be accessed here.

harmonisation can benefit companies by providing a consistent regulatory environment and smoother operations across different markets.

In the context of India, embracing the principles of the EU AI Act can position Indian companies as leaders in responsible AI deployment. Indian businesses can leverage the Act's framework to develop robust AI systems that prioritise ethical considerations and transparency. This proactive approach not only ensures compliance but also builds trust with stakeholders. Adhering to the Act's standards may be particularly important in the event the Indian Government implements similar compliance requirements for high-risk AI systems under the proposed Digital India Act.[35] Separately, making necessary disclosures while using AI-generated content can help companies align their practices with the advisories[36] issued by the Indian Government to address issues such as deepfakes and digital replicas, particularly on social media platforms. Through proactive compliance and a commitment to ethical practices, companies can enhance their brand reputation, build customer trust and position themselves as leaders in the evolving AI landscape.

Authors: Shreya Suri | Shivani Kapur Jeet | Akshita Singh

Date: August 16, 2024

Practice Areas: Technology, Media and Telecommunications

[35] The Proposed Digital India Act, 2023, can be accessed here.
[36] Union Government issues advisory to social media intermediaries to identify misinformation and deepfakes, can be accessed here; Platforms and Intermediaries Commit to Tackling Deepfakes Under Existing Laws, can be accessed here and; Interaction of Minister of Railways, Communications and Electronics & IT Shri Ashwini Vaishnaw with stakeholders on issues arising out of deepfake, can be accessed here.