CLIENT ALERTS & INSIGHTS

European Union Artificial Intelligence Act: An Overview

JANUARY 29, 2025

Authors: Daniel S. Marks, Shivdutt Trivedi

UPDATED January 29, 2025

World's first comprehensive regulation: The European Union Artificial Intelligence Act ("EU AI Act") entered into force on August 1, 2024.

Brief History

In October of 2020, the leaders of the European Union ("EU") requested the European Commission to propose ways to increase investments in AI systems and to provide an overarching regulatory framework for the same. The intention behind this request was that EU leaders wanted to strike a balance between fostering innovation and having AI systems that are transparent, safe and non-discriminatory. In response, a year later, the European Commission proposed an Artificial Intelligence Act on April 21, 2021. The European Parliament approved its version of the EU AI Act on June 14, 2023. This was followed by intense negotiations between the European Institutions (European Parliament, the European Council and the European Commission), and on December 8, 2023, the stakeholders reached a provisional agreement on the draft of the EU AI Act.

Subsequently, on March 13, 2024, the EU AI Act received its final assent from the EU Parliament with 523 votes in favor, 46 against and 49 abstentions, bringing it one step closer to adoption. Thereafter, the final approved version was published in the Official Journal of the EU on July 12, 2024, and the EU AI Act came into effect on August 1, 2024. This is a historic moment, as the EU AI Act is the world's first comprehensive legislation regulating Artificial Intelligence ("AI") systems according to a risk-based approach.

Applicability

The EU AI Act will have broad applicability, much like the EU General Data Protection Regulation ("EU GDPR"), thereby having possible ramifications on companies established outside the EU. The EU AI Act applies to: (a) providers placing AI systems in the EU irrespective of where they are established; (b) deployers of AI systems that have their place of establishment in the EU; (c) providers or deployers located outside the EU but where the output produced by the AI system is going to be used in the EU; (d) importers and distributors of AI systems; (e) authorized representatives of providers of AI systems who are not established in the EU; and (f) affected persons that are located in the EU. One particularly important and intensely negotiated exception: the EU AI Act will not be applicable to AI systems that are used exclusively for military or defense purposes.

Since the EU AI Act is going to apply to providers and deployers irrespective of the place of establishment, the implementation of this Act will have a ripple effect on companies established in

the United States ("US") having operations in the European Union, even though the US has no overarching federal legislation at present governing AI systems akin to the EU AI Act.

Definition of AI Systems

In the absence of any other legislation, the EU AI Act will likely be the 'global standard' for regulating AI systems. To this effect, the definition of AI systems in the EU AI Act is in line with the Organization for Economic Co-operation and Development ("OECD") Guidelines. The EU AI Act defines AI systems as: "a machine-based system 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." This definition of AI systems is well thought-out to ensure that it is not only broad enough to envisage future technological advancements but also ensure that traditional software doing simple automated calculations are not included within the scope of this Act.

Risk-Based Approach

The EU AI Act will be modeled on a risk-based approach wherein high-risk AI systems will be regulated more extensively than the ones that pose less risk. To this effect, the EU AI Act has divided AI systems into four categories:

(a) Unacceptable Risk: These types of AI systems are deemed a clear threat to the safety and livelihood of humankind and go against the ethos of the EU. Therefore, such AI systems are prohibited by the EU AI Act. AI systems with unacceptable risk include (a) social scoring, (b) biometric identification systems used to deduce and categorize individuals on the basis of attributes such as race, sex life, sexual orientation and religious beliefs, (c) AI systems that manipulate human behavior. Even though these AI systems are prohibited, the EU AI Act carves out a narrow exception for such systems used for law enforcement purposes.

(b) **High Risk:** These types of AI systems are deemed to pose a significant threat to health, safety, fundamental rights and the rule of law. This type includes AI systems that are deployed in (a) critical infrastructure (e.g. transport, education, public utilities), (b) essential public services (e.g. credit scoring), (c) law enforcement that might impact a person's fundamental right; (d) administration of justice, (e) employment/recruitment, and (f) remote biometric identification systems. These AI systems will be required to comply with extensive obligations before they are available in the public market, such as, adequate risk assessment, appropriate human oversight and implementing mitigation systems.

(c) Limited Risk: These types of AI systems are deemed not to pose any serious threat and the primary risk associated with such AI systems is due to lack of transparency. The EU AI Act has introduced certain transparency obligations to ensure that all human users are well-informed that they are interacting with an AI system. An example of AI systems with limited risk is chatbots. As long as human users are made aware that they are interacting with a limited risk AI system, such system is not deemed to pose any significant threat under the EU AI Act.

(d) Minimal Risk:

These types of AI systems are deemed to have no real associated risk and can be deployed without any restrictions. Examples of minimal-risk AI systems include AI-enabled video games and inventory-management systems.

General Purpose AI (GPAI) Systems

As the name suggests, GPAI systems are those AI solutions that can be used for a variety of different purposes. The AI Act will not apply to GPAI systems that are used exclusively for the purpose of scientific research and development. However, GPAI systems used for other purposes will be regulated by the AI Act with a focus on maintaining transparency. For instance, the provider of a GPAI system will be required to make technical documentation available to the enforcement authorities for training and testing purposes. Further, the GPAI systems must be modeled in a way to respect the national copyright laws of the member states.

If a GPAI system's computational power is greater than 10^25 floating point operations (FLOPs), then such GPAI model is presumed to have high impact capabilities and will be subject to additional regulations. Further, the EU Commission intends to release a periodic list of such GPAI models with systemic risk to ensure compliance.

Fines

Much like the EU GDPR, the EU has proposed stringent fines to ensure compliance with the AI Act. The majority of the violations under the legislation will be subject to administrative fines of up to 15 million Euros or 3% of the violator's total worldwide turnover for the preceding financial year ("Total Turnover"), whichever is higher. However, violation of Article 5 (prohibited AI practices) will be subject to administrative fines of up to 35 million Euros or 7% of the violator's Total Turnover, whichever is higher. Further, the supply of incorrect, incomplete or misleading information to the notified bodies or national regulators in response to a request will be subject to administrative fines of up to 7.5 million Euros or 1% of the violator's Total Turnover, whichever is greater.

National Regulators

EU member states have been given until August 2, 2025, to nominate the relevant National Competent Authorities ("NCA") that will regulate the AI Act in each such member state. Each member state will be required to establish or designate three authorities at the national level: (1) Notifying Authority ("NA"): It will be tasked with setting up and carrying out procedures for assessing, designating and monitoring conformity assessment bodies; (2) Market Surveillance Authority ("MSA"): It will be tasked with taking measures to ensure that AI products comply with the legal requirements (NA and MSA will together be the NCA for respective member states); and (3) National Public Authorities ("NPA"): It will be tasked with enforcing fundamental rights obligations with respect to the High-risk AI Systems. The EU member states were required to nominate their respective NPAs by November 2, 2024.

The member states can use their own discretion in ascertaining the structure and design of these three authorities. For instance, Spain's Agency for the Supervision of Artificial Intelligence ("AESAI") is going to act as the country's single MSA. However, Finland is thinking of designating ten pre-existing market surveillance authorities as their MSA.

At this stage, it is premature to speculate who will be the final NCAs for respective member states. We will know about the final decision on NCAs only when they officially notify these appointments to the EU Commission. As of now, only Malta has officially designated both the MSA and NA.

Timeline for Implementation

Even though the EU AI Act came into force on August 1, 2024, its implementation will be phased over time. The following are effective dates for certain key provisions of the EU AI Act:

(a) February 2, 2025: Prohibitions on AI systems with unacceptable risk.

(b) August 2, 2025: Provisions relating to NCA, GPAI models, Governance, Confidentiality and Penalties.

(c) August 2, 2026: The remainder of the EU AI Act except for provisions relating to AI systems with high-risk.

(d) August 2, 2027: Provisions relating to AI systems with high-risk.

Impact of the EU AI Act on Businesses

With the three-year phased implementation of the EU AI Act, businesses in the EU should start building a thorough roadmap to comply with all the obligations. Further, as discussed above, **the EU AI Act has extra-territorial applicability and therefore, even businesses outside of the EU should become cognizant of the required compliance obligations**. Generally, every business should first ascertain the AI systems it is currently using/developing or will likely be using in the near future. This list should be comprehensive and should cover AI systems used across departments. Once the repository is created, the next step is to classify each of the AI systems into four risk categories as set forth under the EU AI Act (and as discussed above). Such categorization will not only streamline the implementation process, but also make it easy for businesses to ascertain and comply with the numerous obligations under the EU AI Act. Lastly, to ensure timely implementation, businesses should consider (a) organizing internal trainings and awareness programs; and (b) establishing formal governance models that would oversee compliance with the EU AI Act.

Under the EU AI Act, all parties that are involved in the development, manufacturing, import, distribution or usage of AI systems will have certain obligations. However, the two main players to be regulated in the market would be ‘providers’ and ‘deployers’, both of which are defined under the EU AI Act. A ‘provider’ is a natural or a legal person that either develops an AI system or a GPAI, or places either of these into service under its own name or trademark, irrespective of whether it receives a payment for the same. In other words, a ‘provider’ could either be a developer or a business engaged that ‘white label’ AI systems. Since the EU AI Act has been modeled on a risk-based approach, providers of high-risk AI systems will have greater obligations. Some of the major obligations include (a) formulating written policies to ensure a thorough quality management system; (b) ensure it conducts a conformity assessment before the applicable AI system is placed on the market; (c) compulsory registration with the EU and affix the ‘CE’ mark suggesting that the AI system meets the compliance requirements; (d) report major incidents including serious physical harm of person/property or violation of fundamental rights to the relevant MSA; and (e) comply with

accessibility requirements. Therefore, providers under the EU AI Act will be held accountable for the overall safety of AI systems.

'Deployers' are defined as any entity that is using the AI system in a professional capacity under its authority. In other words, any business that uses an AI system in the US for either internal purposes or for providing services to its customers will fall within the definition of deployers. Additionally, as stated earlier, even if an AI system is not in the EU, but if the output generated by such AI system is going to be used in the EU, such deployers would also be required to comply with the applicable obligations. Therefore, majority of the businesses will fall under the category of 'deployers'.

Moreover, specifically for high-risk systems, a 'deployer' may also be considered as a 'provider' if (a) uses its mark on the high-risk AI systems; (b) makes major modifications to a high-risk AI system; or (c) substantially modifies an AI system that it subsequently becomes a high-risk AI system. In either of the above scenarios, the deployer will now have to also adhere to all the obligations applicable to a 'provider' under the EU AI Act.

With respect to all AI systems, irrespective of the risk associated with it, deployers are obligated to ensure a suitable level of AI literacy of their staff or any other stakeholder using the AI system. Deployers also have a duty to cooperate with the NCA and NPA for any AI system that poses some risk. Further, deployers of specific AI systems have certain transparency obligations. For instance, deployers of emotion recognition or biometric categorization systems must notify the individuals that are subject to such AI systems and must process their personal data in accordance with the applicable data protection laws. Similarly, deployers of generative AI and deepfakes must disclose that the output is generated by an AI system.

Some of the major obligations for a deployer of a high-risk AI system includes: (a) using the AI systems in accordance with use instructions. Additionally, provider must continue monitoring the use and notify the provider of any discrepancy with the use instructions; (b) assign a natural person(s) to oversee the training and overall implementation of the AI system; (c) notify its employees that the AI system they are using is categorized as a high-risk AI system. Additionally, if a high-risk AI system is used for critical infrastructure, similar notice must also be given to the end-users; (d) before first using the high-risk AI system, it must conduct a fundamental rights impact assessment to assess the risks associated with it and formulate mitigation actions that will be taken by the provider; (e) reporting serious incidents to the MSA; and (f) cooperate with the NCA in implementing the EU AI Act.

While the EU AI Act imposes various obligations on deployers and providers of AI systems, a structured and timely approach can ensure compliance with this new legislation. By integrating these requirements systematically, providers and deployers can stay ahead of the curve and foster legally compliant AI development.

With the EU AI Act being effective and moving towards a phased implementation, and as other countries and US states begin to follow the EU's lead, the Benesch AI Commission remains your trusted partner for all things Artificial Intelligence and can assist your organization as you navigate these new rules and compliance obligations. For more information, please reach out to a member of the team.