15 June 2023

AI Act: A New Era of AI Regulation - Part 1

Introduction

Artificial Intelligence (AI) has been a significant driver of technological innovation for several years now. Its applications range from autonomous vehicles and predictive analytics to personalized marketing and advanced healthcare diagnostics. However, with the rapid advancement and widespread use of AI, there has been a growing need for a comprehensive legal framework to govern its use and address the ethical, legal, and societal implications.

In April 2021, the European Commission took a bold step in this direction by proposing the first-ever legal framework on AI, known as the Artificial Intelligence Act (AI Act). The draft was published with the aim of ensuring that AI systems are used in a way that respects European values and regulations, and it has been discussed and amended since then.

Today, we find ourselves at a pivotal moment in the journey of the AI Act. The European Parliament has just adopted its position on the legislation, marking a key step towards setting unprecedented restrictions on how companies use artificial intelligence. This move solidifies Europe's position as a de facto global tech regulator.

The AI Act is now closer than ever to becoming law, and as we approach the final stages of its adoption, it is crucial for businesses and individuals involved in the development, deployment, and use of AI systems to understand the implications of this ground-breaking legislation.

In this three-part series, we will delve into the details of the AI Act, starting with a general overview of its purpose, general implications, prohibited AI practices, and the concept of high-risk AI systems. This first part is a brief yet comprehensive overview of the AI Act, serves as a basis for the following discussion in the specific actual steps required for complying with its provisions.

Purpose of the AI Act

The AI Act is a response to the need for a legal framework that can keep up with the rapid advancements in AI technology. It aims to:

- **Ensure AI respects European values and regulations**: The AI Act is designed to ensure that AI systems are developed and used in a way that respects fundamental rights, including privacy and data protection, non-discrimination, and freedom of expression. For example, it prohibits AI practices that manipulate human behaviour, exploit vulnerabilities of specific groups, or use real-time remote biometric identification systems in public spaces.
- **Establish clear rules for high-risk AI systems**: The AI Act introduces strict rules for AI systems considered high-risk in terms of their impact on safety and fundamental rights. These systems are subject to stringent obligations before they can be put on the market, including adequate risk assessment and mitigation systems, high-quality datasets to minimize biases,

provision of clear and adequate information to users, and appropriate human oversight measures.

- **Promote innovation and competition**: By providing legal certainty and a harmonized set of rules across the EU, the AI Act aims to foster innovation and competition in the AI market. It also includes provisions to support small and medium-sized enterprises (SMEs) involved in AI.
- **Establish a European AI Board**: The AI Act proposes the establishment of a European AI Board, composed of representatives from each EU member state and the European Commission. The Board will play a key role in contributing to the consistent application of the AI Act across the EU, and it demonstrates again the similarities to other data and technology-oriented legislations in the EU, such as the GDPR and it supervising authority, the EDPB.

General Implications of the AI Act

The AI Act has far-reaching implications for all stakeholders involved in the AI lifecycle, from developers and deployers to users and affected parties. Here are some of the key implications:

- **Compliance requirements for products that utilize AI Systems in the EU Market**: This includes: (a) product design and development, as AI systems will need to be built from the ground up with compliance in mind; and (b) further implications regarding providers' ongoing conduct as they will need to adapt comprehensive compliance plans.
- **Impact on AI Training and Data Management:** The AI Act has significant implications for the way AI systems are trained. The Act requires that training, validation and testing data sets used for high-risk AI systems are relevant, representative, free of errors and complete. This will require companies to invest in robust data management practices and may impact the types of data that can be used to train AI systems.
- **Data Privacy and Ownership concerns:** The Act also emphasizes the importance of privacy and data protection in the context of AI training. It mandates that AI systems must be designed and developed in a manner that respects privacy and data protection principles, including data minimization and purpose limitation. This means that only the minimum amount of data necessary should be used, and it should only be used for the specific purpose for which it was collected. Furthermore, the AI Act acknowledges the potential intellectual property issues that may arise in the context of AI. It emphasizes the need for clear rules on the ownership and use of data and algorithms and encourages the development of fair and equitable data sharing mechanisms.
- **Transparency obligations**: The AI Act imposes transparency obligations on all AI systems that interact with humans, are used to detect emotion, or determine association with social categories or generate or manipulate content (deep fakes). Users must be informed that they are interacting with an AI system and be provided with meaningful information about the system's capabilities and limitations.
- **Accountability and governance**: The AI Act requires providers of AI systems to implement appropriate governance and risk management systems. This includes establishing a post-market monitoring system to detect and mitigate any risks that arise during the use of the AI system.

- **Sanctions and fines**: Non-compliance with the AI Act can result in significant fines. For serious infringements, such as non-compliance with the rules for high-risk AI systems or the use of prohibited AI practices, fines can reach up to €40 million or up to 7% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Scope and Applicability of the AI Act

The AI Act applies to a broad range of entities and activities, and similarly to the GDPR it has extraterritorial scope. That means, the AI Act applies to AI systems placed on the EU market, put into service, or used in the EU, regardless of whether the provider is established in the EU. This wide scope of applicability reflects the EU's intention to ensure that all AI systems that affect EU citizens and businesses comply with the AI Act.

In terms of material scope, the AI Act defines an 'AI system' as software that is developed with one or more of the following AI techniques and approaches, and for a given set of human-defined objectives, can generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with:

- **Machine Learning Approaches**: These include supervised, unsupervised, semi-supervised, and reinforcement learning. Machine learning involves the use of algorithms that improve automatically through experience and the use of data.
- **Logic - and Knowledge-Based Approaches**: These include expert systems, which are AI systems that emulate the decision-making ability of a human expert, and knowledge graphs, which are a type of AI that uses graph theory to store, manipulate, and retrieve knowledge.
- **Statistical Approaches**: These include Bayesian estimation, search, and optimization methods. Statistical approaches in AI involve the use of statistics to infer patterns and learn from data.

Risk-Based Approach

The AI Act adopts a risk-based approach in two key aspects. First, it uses this approach to determine which AI systems fall under its scope, with stricter requirements applying to high-risk AI systems. In addition, certain categories of AI utilizations are completely prohibited due to their potential “unacceptable” risk to EU residents’ freedoms and rights. While this approach aims to avoid overregulation and allow for innovation in low-risk AI systems, it means that AI systems that operate in significant fields such as health, banking, insurance, governmental activities, public safety and health, etc., are fully exposed to the implications of the regulation, and need to comprehensively adapt their conduct to its requirements.

Second, within the category of high-risk AI systems, the Act requires the provider to conduct a risk analysis to identify the inherent risks of the specific AI system, in order to determine the concrete measures that need to be implemented. The higher the potential risk to safety and fundamental rights, the stricter the requirements for the AI system.

Prohibited AI Practices

The AI Act prohibits certain AI practices that are considered to create an unacceptable risk. These include AI systems that deploy subliminal techniques beyond a person's consciousness to materially distort their behaviour in a manner that could cause physical or psychological harm. It also prohibits AI systems that exploit any vulnerabilities of a specific group of persons due to their age, physical or mental disability, to materially distort their behaviour in a manner that is likely to cause them physical or psychological harm. AI systems used for social scoring by public authorities are also prohibited.

High-Risk AI Systems

As mentioned above, the AI Act introduces restrictive rules for AI systems that are considered high-risk. These systems are subject to stringent obligations before they can be put on the market, including conformity assessments and certification procedures. High-risk AI systems include those used for critical infrastructures, educational and vocational training, employment, workers management 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.

For high-risk AI systems that are safety components of products or systems, or which are themselves products or systems, existing sector-specific legislation, such as the Medical Devices Regulation or the Machinery Directive (i.e., require CE mark), will continue to apply, but will include additional AI-related obligations and restrictions.

The AI Act outlines several requirements for high-risk AI systems before they can be put on the market. These requirements are designed to ensure that these systems are safe, reliable, and respect fundamental rights. Here are the key requirements:

- **Risk Management System**: High-risk AI systems must have a risk management system in place. This system should be able to identify and analyse the potential risks associated with the AI system. It should also be able to take appropriate measures to eliminate or mitigate these risks.
- **Data Governance and Management**: High-risk AI systems must use high-quality datasets during their development phase. These datasets should be relevant, representative, free of errors and complete. They should also respect privacy and data protection rules.
- **Documentation**: Providers of high-risk AI systems must maintain technical documentation that provides detailed information about the system. This includes the system's purpose, its development, monitoring, operation and maintenance.
- **Fairness and Bias Mitigation**: High-risk AI systems must be designed and developed with fairness in mind. This means that they should not perpetuate or amplify biases that could lead to unfair outcomes. Providers of these systems are required to use techniques and methodologies that minimize bias in the outputs of the AI system. This includes bias in data collection and processing, algorithmic bias, and bias in decision-making. The AI Act emphasizes

the importance of ensuring that AI systems do not lead to discriminatory outcomes and that they respect the principle of equal treatment.

- **Transparency and Provision of Information**: High-risk AI systems must be transparent. They should provide users with information about the system's capabilities and limitations. They should also inform users when they are interacting with an AI system.
- **Human Oversight**: High-risk AI systems must have an appropriate level of human oversight. This means that there should be human involvement in the system's decision-making process.
- **Robustness, Accuracy and Security**: High-risk AI systems must be robust, accurate and secure. They should be able to withstand attacks and operate correctly.
- **Post-Market Monitoring**: Providers of high-risk AI systems must have a post-market monitoring system in place. This system should be able to monitor the performance of the AI system after it has been put on the market.

In the next part of this series, we will dive deeper into the requirements for high-risk AI systems and focus especially on the conformity assessment procedures, and the obligations of different actors involved in the AI system lifecycle. Stay tuned for more insights on the EU's forthcoming AI Act.

This document is intended to provide only a general background regarding this matter. This document should not be regarded as binding legal advice, but rather a practical overview based on our understanding. APM & Co. is not licensed to practice law outside of Israel.

APM Technology and Regulation Team.

Adv. Itamar Cohen
Partner, Technology and Regulation Practice

03-5689000
itamarc@apm.law