GECIĆ | LAW

A Guide to the AI Act

And what it means for us

2024

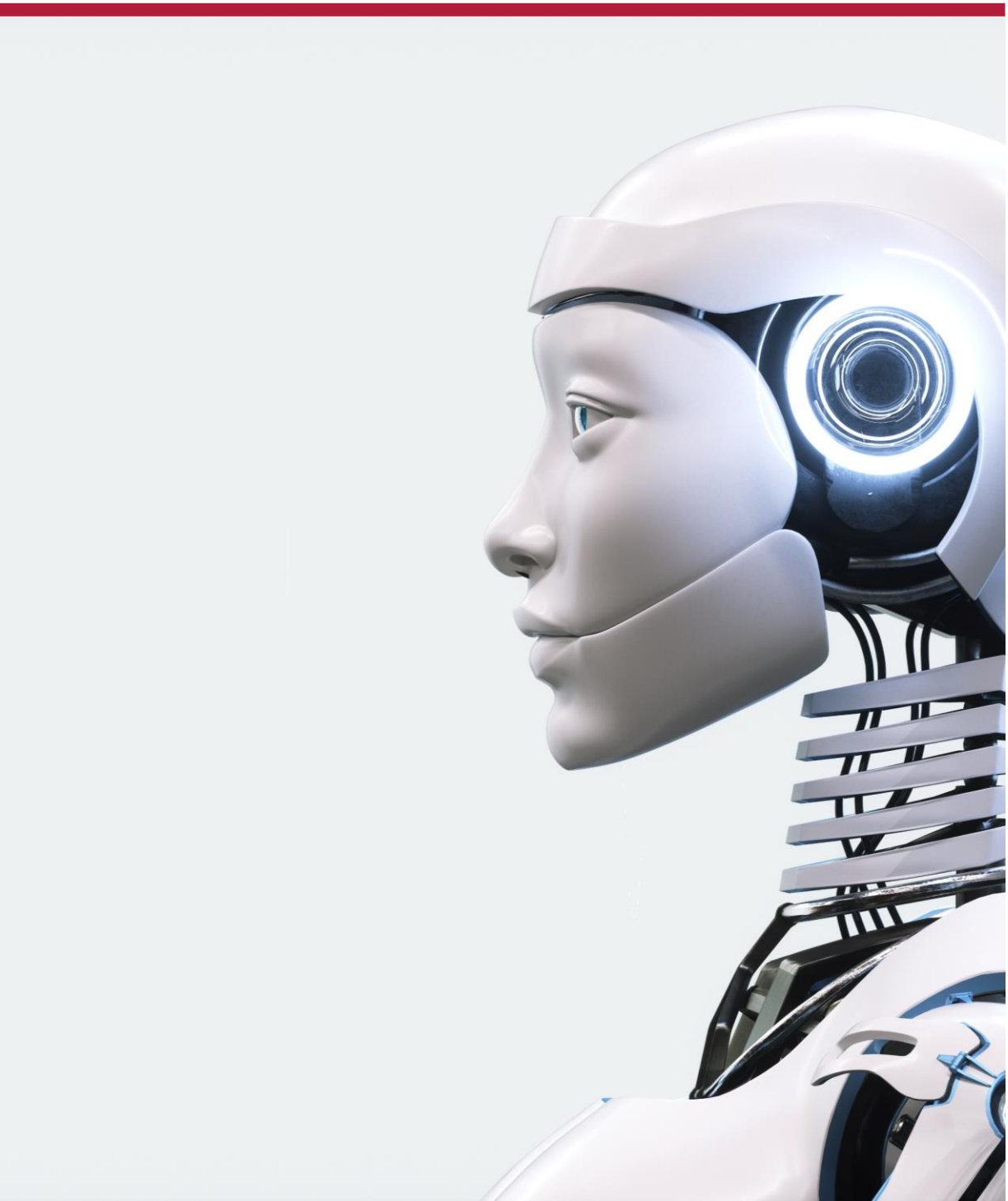
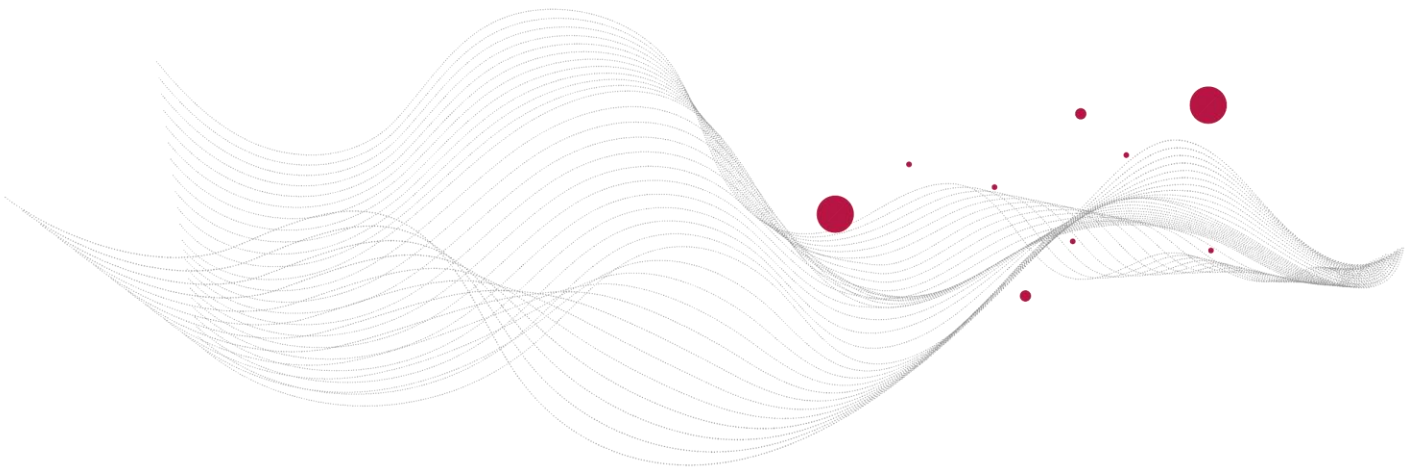


Table of Contents



The AI Act

Understanding the AI Act

The AI Act is a groundbreaking legal framework, marking the EU's proactive stance in addressing the risks associated with AI and positioning the bloc as a global leader in this domain.

In the realm of modern technology, Artificial Intelligence (AI) stands as a frontier, promising transformative advancements across various sectors. However, alongside its potential benefits, AI introduces complex ethical, legal, and societal implications. Recognizing this, the European Union (EU) has embarked on a groundbreaking journey by introducing the AI Act, a legislative framework aimed at regulating AI systems.

Its primary objective is to furnish AI developers and deployers with lucid guidelines and responsibilities concerning specific AI applications. Simultaneously, the legislation endeavors to alleviate administrative and financial burdens, particularly for small and medium-sized enterprises (SMEs).

The AI Act is part of a broader initiative aimed at fostering trustworthy AI, along with the AI Innovation Package and the Coordinated Plan on AI. Together, these measures are designed to safeguard the rights and safety of individuals and businesses while also stimulating adoption, investment, and innovation in AI throughout the European Union.

The AI Act

Understanding the AI Act

As the first of its kind globally, the AI Act signifies a milestone in establishing a comprehensive legal framework for AI. Its overarching goal is to cultivate trust in AI systems within Europe and beyond, ensuring they uphold fundamental rights, safety standards, and ethical principles, while also addressing the risks associated with highly potent and impactful AI models.

The AI Act signifies a pivotal moment in the legislative landscape of the European Union marking a concerted effort to regulate the rapidly expanding domain of artificial intelligence. This landmark legislation, characterized by its comprehensive scope and meticulous guidelines, represents a significant stride toward effectively managing the multifaceted challenges posed by AI deployment.

At its essence, the AI Act aims to navigate a carefully crafted balance between promoting innovation and upholding the fundamental rights and safety of individuals within the AI ecosystem. By establishing clear parameters and obligations across diverse sectors, the legislation strives to foster trust and confidence in AI technologies while addressing potential risks and ethical concerns.

The AI Act plays a crucial role in setting the rules for how AI should be used responsibly in the EU. It shows that everyone is committed to using AI to make things better while making sure it doesn't harm our values or ethics.

According to the AI Act, an AI system is

> *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.*

Therefore, an AI system is a system that is autonomous, adaptable and can generate an output.

Key provisions of the EU AI Act may include:

Classification of AI systems into different risk categories based on their potential harm.

Requirements for high-risk AI systems include conformity assessments, data quality, transparency, and human oversight.

Prohibition of certain AI practices deemed unacceptable, such as social scoring and real-time biometric identification in public spaces.

Enhanced transparency and traceability obligations for AI developers and providers.

Establishment of a European Artificial Intelligence Board to support implementation and enforcement.

What types of AI systems are there?

Apart from AI systems employing prohibited practices, which are consequently banned, the AI Act highlights several categories of AI systems. It's imperative to acknowledge that all AI systems, regardless of type, are subject to certain basic obligations outlined in the AI Act, such as transparency requirements.

Risk classification – given that the AI systems in question are categorized based on risk, it's valuable to understand the AI Act's definition of risk. As per the AI Act, risk is defined as the amalgamation of the likelihood of harm occurring and the magnitude of that harm.

⚠ **Limited-risk AI systems** are AI systems that are implemented with measures in place to mitigate potential risks and ensure that their deployment is safe and ethical. Unlike prohibited or high-risk AI systems, which pose significant dangers to individuals, society, or the environment, limited-risk AI systems are characterized by their adherence to principles of responsible AI development.

Transparency: Limited-risk AI systems are transparent in their operations, making it clear how they reach their decisions or recommendations.

Fairness: These systems are designed to mitigate biases and ensure fairness in their outcomes, especially in areas such as hiring, lending, and criminal justice.

Privacy protection: Limited-risk AI systems prioritize the protection of individuals' privacy by implementing robust data security measures, anonymization techniques, and compliance with relevant privacy regulations such as GDPR.

Safety and reliability: These systems undergo rigorous testing and validation to ensure their safety and reliability in real-world scenarios.

Human oversight and control: Limited-risk AI systems maintain human oversight and control, particularly in high-stakes decision-making processes.

Ethical considerations: These systems are developed and deployed with ethical considerations in mind, adhering to ethical guidelines and principles such as beneficence, non-maleficence, and respect for autonomy.

High-risk AI systems are systems that are intended to be a safety component of a product or systems that are used in areas such as:

Biometrics: remote identification, biometric categorization, and emotion recognition.

Critical infrastructure

Education and vocational training: admission to educational institutions, evaluation of learning outcomes, assessment of the level of education, and monitoring prohibited activities during tests.

Employment: recruitment or selection.

Enjoyment of essential public and private services: assistance and benefits, creditworthiness, emergency calls, insurance.

Law enforcement: assessment of the risk of a natural person becoming a victim, polygraphs, assessment of evidence, assessment of the risk of offense or re-offense.

Migration

Administration of justice and democratic processes

Prohibited risk AI systems realize their objective of devising a framework for trustworthy AI, the AI Act envisages certain AI practices that are deemed to be prohibited. Some common areas for prohibited risk AI include:

Healthcare: AI systems used for diagnosing diseases, prescribing treatments, or managing patient data may pose risks if they are not accurate or transparent.

Finance: AI systems employed for credit scoring or fraud detection could pose risks if they lead to financial losses, unfair lending practices, or erroneous decisions based on biased algorithms.

Employment: AI systems involved in hiring processes, performance evaluations, or workforce management could introduce risks related to discrimination, privacy violations, or job displacement if they are not implemented carefully.

Transportation: AI systems powering autonomous vehicles or air traffic management may pose risks if they are not sufficiently reliable or capable of handling unforeseen circumstances, potentially leading to accidents, injuries, or loss of life.

A risk management system must be established and maintained for high-risk AI systems. This system covers the lifecycle of such systems and involves regular review and updating. It includes steps such as identifying and analysing known and foreseeable risks, estimating potential risks from misuse, assessing additional risks from post-market monitoring data, and implementing targeted risk management measures.

These measures should focus on **risks that can reasonably be mitigated through system development or design, or by providing adequate technical information.**

General-purpose AI systems are AI systems that are based on a general-purpose AI model and can serve a variety of purposes, both for direct use as well as for integration into other AI systems.

A general-purpose AI model is deemed to have a systemic risk if it meets certain criteria, including high-impact capabilities evaluated through appropriate technical tools or methodologies, or upon Commission decision prompted by a qualified alert.

In particular, a general-purpose AI model is considered to possess significant impact potential when the volume of computational resources employed in its training surpasses 10^25 floating point operations.

The Commission is empowered to adjust thresholds, benchmarks, and indicators through delegated acts to ensure they remain aligned with technological advancements and the current state of the art.

Who is obliged under the AI Act?

1. Entities that introduce AI systems or general-purpose AI models to the market or utilize them within the EU, regardless of their establishment or location within the EU or in a third country.
2. Deployers of AI systems that have their place of establishment or who are located within the EU.
3. Providers and deployers of AI systems that have their place of establishment or who are in a third country, where the output produced by the system is used in the EU.
4. Importers and distributors of AI systems.
5. Product manufacturers placing on the market or putting into service an AI system together with their product and under their name or trademark.
6. Authorized representatives of providers, which are not established in the EU.
7. Affected persons that are located in the EU.

Hence, situations may arise where individuals outside the EU could be held accountable for violating the AI Act, necessitating their consideration of the Act when engaging with counterparts from the EU.

Key categories of responsible persons and entities include the following:

A provider, whether an individual or entity, can be a natural person, legal entity, public authority, agency, or any other organization. This provider engages in the development of AI systems or general-purpose AI models or may possess such systems or models developed by others. They introduce these systems into the market or deploy them for use under their name or trademark, regardless of whether such services are offered for payment or free of charge.

Obligations: Ensuring compliance of high-risk AI systems with the requirements set out in the AI Act; utilizing a quality management system; keeping adequate documentation; ensuring conformity assessment etc.

A deployer is any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used during personal non-professional activity.

Obligations: Using high-risk AI systems following the instructions of use accompanying the systems; ensuring that people overseeing the high-risk AI systems have the necessary competence, training and authority as well as the necessary support; monitoring the operation of the high-risk AI system based on the instructions etc.

An authorized representative is any natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation.

Obligations: performing tasks specified in the mandate received from the provider; ensuring that conformity assessments have been carried out; cooperating with national competent authorities etc.

An importer is any natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established outside the Union.

Obligations: Ensuring that conformity assessments have been carried out; verifying technical documentation, verifying CE conformity, etc.

A distributor is any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.

Obligations: Verifying CE conformity, ensuring that providers and importers have complied with their obligations, etc.

What are the potential penalties?

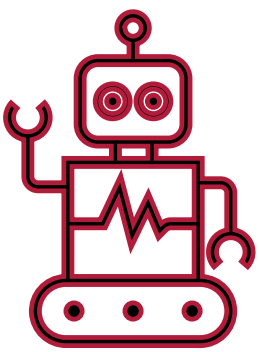
The AI Act sets out harsh monetary fines for non-compliance with its provisions.

- Non-compliance with the prohibition of the artificial intelligence practices referred to as "Prohibited Artificial Intelligence Practices" shall be subject to administrative fines of up to EUR 35,000,000 or, if the offender is a company, up to **7% of its total worldwide annual turnover** for the preceding financial year, whichever is higher.
- Non-compliance with other requirements and obligations (transparency obligations, obligation of providers, deployers, distributors, importers, and authorized representatives) shall be subject to administrative fines of up to EUR 15,000,000 or, if the offender is a company, **up to 3% of its total worldwide annual turnover** for the preceding financial year, whichever is higher.
- The supply of incorrect, incomplete, or misleading information to notified bodies and national competent authorities in reply to a request shall be subject to administrative fines of up to EUR 7,500,000 or, if the offender is a company, **up to 1% of its total worldwide annual turnover** for the preceding financial year, whichever is higher.

To conclude, the AI Act stands as a beacon of progressive regulation in the realm of artificial intelligence, symbolizing the European Union's commitment to fostering innovation while safeguarding individuals and society. By delineating clear parameters and obligations for stakeholders, this landmark legislation aims to instill trust and confidence in AI technologies, mitigating potential risks and ethical concerns.

However, the effectiveness of the AI Act hinges not only on its formulation but also on its enforcement across member states. Therefore, robust enforcement mechanisms must be put in place to ensure compliance and accountability.

Member states must prioritize the implementation of the AI Act, including the establishment of monitoring bodies, enforcement agencies, and penalties for non-compliance. Only through rigorous enforcement can the AI Act fulfill its mission of promoting responsible AI governance and advancing the EU as a global leader in AI innovation while safeguarding the rights and safety of its citizens.



Gecić Law AI Team

Our team of extraordinarily well-trained and experienced individuals and their in-depth knowledge of the regional market builds our unique position to best address our clients' most pressing needs. Below is our dedicated AI & Robotics team that includes:

Ognjen Colić
Partner, Head of M&A and Corporate Law
ognjen.colic@geciclaw.com

Miodrag Jevtić
Counsel, Banking and Finance
miodrag.jevtic@geciclaw.com

Nemanja Sladaković
Senior Associate, Corporate Law and Employment
nemanja.sladakovic@geciclaw.com

Bojan Tutić
Associate, Intellectual Property
bojan.tutic@geciclaw.com

Žarko Popović
Associate, Dispute Resolution
zarko.popovic@geciclaw.com