View this email in your browser

The EU AI Act

July 18 , 2024

Dear clients,

You should read this client update if:

- You are a company developing or using AI systems (whether proprietary or provided by third parties),
- You are an investor or a company considering an investment or an acquisition of a target company that develops or uses AI systems, or
- Like us, you simply love AI!

What is the EU AI Act?
Adopted on July 12, 2024, the EU AI Act is the first comprehensive legal framework for artificial intelligence ("**AI**") in the world, and it introduces a risk-based approach to regulate different types of AI systems according to their potential impact on society and individuals. Among other things, the EU AI Act sets out specific requirements for high-risk AI systems, prohibits certain AI practices deemed unacceptable, and introduces transparency obligations for certain AI applications. The EU AI Act will enter into force on August 1, 2024, but with certain provisions becoming applicable on different dates.

To whom does the EU AI Act apply?
The EU AI Act has a broad territorial scope and applies to:

a. **providers** placing on the market or putting into service AI systems or placing on the market general-purpose AI models (defined below) in the EU, even if those providers are not established or located within the EU;
b. **deployers** of AI systems that have their place of establishment or are located within the EU;
c. **providers and deployers** of AI systems that are established or located in a third country, where the output produced by the AI system is **used in the EU**;
d. **importers and distributors** of AI systems;
e. **product manufacturers** placing on the market or putting into service an AI system together with their product and under their own name or trademark;
f. **authorised representatives** of providers, which are not established in the EU; and
g. **affected persons** that are located in the EU.

If your company falls within any of the above-mentioned categories, it is likely that the EU AI Act will apply to you, and you should examine your obligations and consider compliance.

What are the consequences of non-compliance?
Non-compliance with the EU AI Act could result in:

- Loss of business, investment or M&A opportunities.
- Fines of up to €35 million or 7% of global annual turnover (whichever is higher) for the most serious violations, such as performing prohibited AI practices.
- Fines of up to €15 million or 3% of global annual turnover (whichever is higher) for non-compliance with other obligations under the EU AI Act.
- Fines of up to €7.5 million or 1.5% of turnover (whichever is higher) for providing incorrect, incomplete, or misleading information to notified bodies or competent authorities.
- Potential market bans or forced recalls of non-compliant AI systems.
- Reputational damage.
- Possible legal actions from individuals or groups affected by non-compliant AI systems.

What practices are prohibited by the EU AI Act?
Various practices are prohibited by the law and should be stopped as soon as possible and no later than ***February 2025***. These include certain AI systems that deploy **subliminal techniques**, that exploit any of the **vulnerabilities** of natural persons, that engage in **social scoring** or predict the risk of a natural person committing a **criminal offence**, that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage, or that **infer emotions** in the areas of workplace and education institutions.

It also bans the use of certain **biometric categorisation systems** that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation, or use certain **'real-time' remote biometric identification systems** in publicly accessible spaces for the purposes of law enforcement. It is worth noting that this section of the law is full of nuances, so it is crucial to work with legal counsel to determine whether the abovementioned prohibitions apply to your specific use case.

What are high risk AI systems?
Various practices are deemed high-risk systems by the law. These include certain AI systems using biometrics or emotion recognition, or AI systems used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity, as well as certain AI systems used in the context of education and vocational training, employment or employment-related decisions, access to essential private services and essential public services and benefits, law enforcement, migration, asylum and border control management, or for the administration of Justice.

What about GPAIs (General Purpose AI models and systems)?
The EU AI Act includes a whole chapter with obligations concerning GPAIs. 'General-purpose AI systems' are defined as AI systems based on general-purpose AI models and which have the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems (and 'general-purpose AI models' are defined as AI models that display significant generality and are capable of competently performing a wide range of distinct tasks and that can be integrated into a variety of downstream systems or applications). GPAI models have different requirements depending on whether they involve systemic risks or not (this depends on the capabilities of the model in question).

Key compliance aspects
The obligations and requirements under the law depend on the classification of the company and the AI system in question. For example, high risk AI systems involve obligations around risk management systems, data governance programs, technical documentation, record-keeping, information and transparency requirements, requirements around human oversight, registration requirements, and requirements regarding the accuracy, robustness and cybersecurity of the AI systems in question. GPAI models involve obligations around technical documentation, information requirements, copyright policies, and the need to create summaries about the content used for training of the GPAI model and, depending on the existence of systemic risks, the law may also require model evaluations, risk assessments and risk mitigation, obligations around the handling of serious AI incidents, as well as certain cybersecurity requirements.

***

It is crucial to start preparing for compliance as soon as possible, by assessing the impact of the EU AI Act on your current and planned AI activities, identifying the relevant obligations and risks, and implementing the necessary measures and safeguards to ensure compliance. If you have questions or would like to discuss this matter, feel free to contact us.

Contact Information

Ignacio Gonzalez Royo, Partner
+972-3-6103788
ignaciog@meitar.com

David Mirchin, Partner
+972-3-6103199
dmirchin@meitar.com

Nicole Denise Feld, Senior Associate
+972-3-614 2636
nicolef@meitar.com

Sara Weinberger, Senior Associate
+972-3-610 3816
saraw@meitar.com

Laura Serero, Associate
+972-3-610 3802
lauras@meitar.com

Orly Calderon, Associate
+972-3-610 3861
orlyc@meitar.com

Guy Unger Most, Associate
+972-3-610 3603
guyu@meitar.com

For additional information about our firm's Technology group, click here

---

To join our newsletter click here