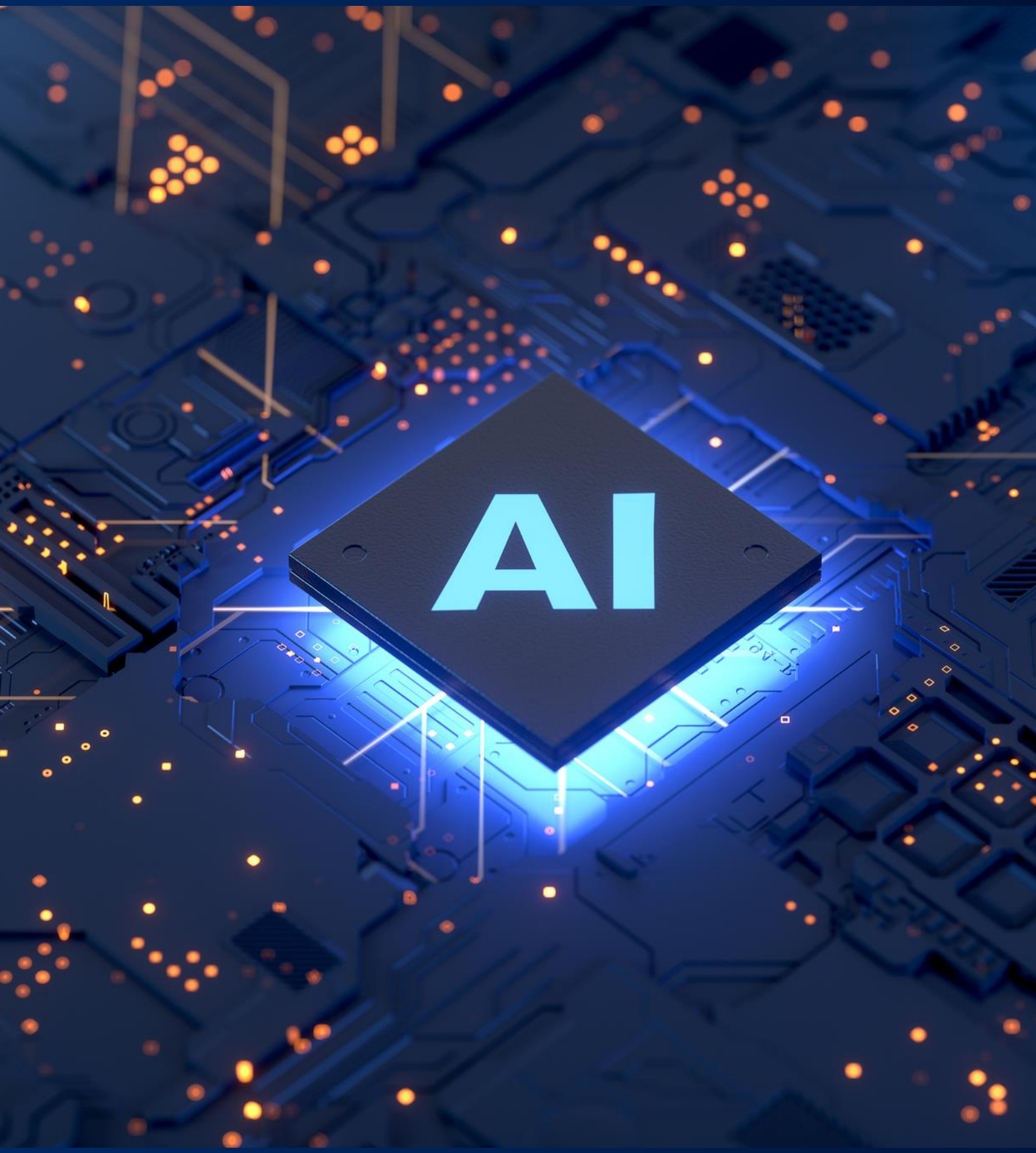
KYRIAKIDES GEORGOPOULOS
LAW FIRM



STARTUPS & INNOVATION

The European Union Adopts the Artificial Intelligence Act

April 8, 2024

The European Union Adopts the Artificial Intelligence Act

BY ELISABETH ELEFTHERIADES, NIKOLAOS VELLIOS, SOFIA KOUTRA

On March 13th, 2024, the EU Parliament adopted the new Regulation on Artificial Intelligence (the "**AI Act**" or the "**Regulation**"). The AI Act will be the world's first comprehensive regulation on artificial intelligence (AI), and aims to strike a balance between, on the one hand, stimulating AI investment and innovation and, on the other hand, ensuring safe AI systems and respect of fundamental rights in the EU.

Following the Parliament's vote, the AI Act will undergo final linguistic approval by lawyer-linguists, a step considered a formality, before being published in the Official Journal. Formal adoption of the Regulation is expected in April 2024. Following its entry into force, a **two-year period** will be allowed for stakeholders to comply with most of the new rules, during which time the EU will issue a series of supporting guidelines and standards. However, rules for so-called General-Purpose AI systems will exceptionally apply after **twelve (12) months** and rules on prohibited AI systems will apply after **six (6) months**, while national Data Protection Authorities (DPAs) across Europe could start enforcing the data-related requirements of the new Regulation even sooner.

A. Scope of the AI Act

Obligations under the AI Act primarily concern **AI systems**. These are "*machine-based system[s] designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, [infer], from the input [they receive], how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*"[1].

General-Purpose AI (GPAI) models are also covered by the new Regulation. GPAI models are "*AI models, including when trained with a large amount of data using self-supervision at scale, that [display] significant generality and [are] capable to competently perform a wide range of distinct tasks regardless of the way the model[s] [are] placed on the market and that can be integrated into a variety of downstream systems or applications*"[2]. GPAI models are the basis for GPAI systems, i.e., systems that have the capability to serve a variety of purposes, such as ChatGPT and DALL-E.[3]

Exceptionally, the AI Act will not apply to systems used exclusively in national security (defense, military), research and innovation, nor to – non-high risk – systems released under free and open-source licenses.[4]

B. Structure of the AI Act – how will it apply?

The AI Act adopts a risk-based approach; the greater the risk an AI system presents to the fundamental rights of individuals, the greater the regulatory burden for its providers and/or other operators. In this context, the Regulation introduces the following categorization of AI technologies:

- Prohibited AI systems: Some AI systems are deemed as posing unacceptable risks and are

[1] Art. 3(1) of the Regulation.
[2] Art. 3(63).
[3] Art. 3(66).
[4] Art. 2.

therefore banned. Specifically, these are systems used for:[5]

- manipulative and deceptive practices;
- exploitation of vulnerabilities;
- biometric categorisation;
- social scoring;
- real-time biometric identification;
- risk assessment in criminal offences;
- facial recognition databases;
- emotion inference in workplaces and educational institutions.

- High-risk AI systems: Certain AI systems are considered to pose high risks to fundamental rights of individuals; these will not be banned but will be subject to significant requirements. The list of high-risk systems provided in the Regulation is not exclusive and may be supplemented in the future; currently, it includes, amongst others, systems used for:[6]
  - remote biometric identification;
  - managing and operating critical infrastructure, such as the supply of water, gas and electricity;
  - education, particularly the assessment of students or of potential students' applications for admission to institutions;
  - law enforcement and certain judicial contexts;
  - recruitment and employment;
  - banking and insurance;
  - determining access and enjoyment of essential private and public services and benefits; and
  - other AI systems covered by certain EU harmonization legislation.
- General-purpose AI models: The AI Act introduces specific regulatory requirements for providers of GPAI models. In principle, the requirements are limited and apply to all GPAI systems. However, when such systems are deemed as presenting "systemic risks"[7], they will be subject to additional regulation. The classification of GPAI models is determined based on their capabilities and impact, also considering the cumulative amount of compute used for their training.
- Low-risk AI systems: Systems not falling in one of the above categories will be considered as posing low risk to individuals' rights, and, as such, will be subject to limited obligations.

C. Obligations relating to High-Risk AI (HRAI) systems

The AI Act introduces significant obligations in relation to HRAI systems, addressed primarily to the provider, i.e., the "*natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general purpose AI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge*".

Specifically, providers of HRAI systems shall comply with the following obligations:[8]

- Establishing a **risk management system** aimed at identifying, analyzing and mitigating risks throughout the entire lifecycle of the HRAI system.

[5] Art. 5.
[6] Art. 6.
[7] Art. 51 and Art. 52.
[8] Art. 16.

- Adopting **data governance measures**, particularly regarding the quality of data sets used in the development of HRAI system.
- Drawing up comprehensive **technical documentation** ('manual') illustrating compliance of the HRAI system with the AI Act's requirements.
- Designing the HRAI system to automatically **keep records** of events ('logs') throughout the system's lifecycle.
- Preparing **instructions** for the use of the HRAI system by deployers, including the characteristics, capabilities and limitations of the system.
- Designing the HRAI system in such a manner that allows for effective **human oversight**.
- Designing and developing the HRAI system with a view to achieving an appropriate level of **accuracy, robustness and cybersecurity**, and to performing consistently in those respects throughout its lifecycle.
- Establishing a **quality management system**, in the form of written policies, procedures and instructions, to ensure compliance with the AI Act.
- Establishing and documenting a **post-market monitoring system** to collect, document and analyze data relevant to the performance of the HRAI system following its deployment and throughout its lifecycle.
- Ensuring that the HRAI system undergoes a **conformity assessment procedure**.
- Affixing the '**CE marking of conformity**' to the HRAI system.
- **Registering** the HRAI system in the relevant EU-wide database.
- **Reporting** serious incidents or malfunctioning to the competent authority within 15 days.

While most of the regulatory burden is borne by the provider, other operators (deployers, distributors and importers) may also be required to comply with certain – more limited – obligations. In particular, the deployer, as the entity under whose authority a HRAI system is used, is responsible for the following:[9]

- Adopting measures to ensure that the HRAI system is used according to the **instructions of use** prepared by the provider.
- Assigning **human oversight** to natural persons who have the necessary competence, training and authority, as well as the necessary support.
- Ensuring that any **input data** they provide or otherwise control is relevant and sufficiently representative, taking into account the intended purpose of the HRAI system.
- **Reporting** any potential risks identified and/or any incidents resulting from the use of the HRAI system.
- Ensuring sufficient **transparency** towards impacted individuals regarding the intent to use a HRAI system to make or assist in making decisions relating to them.
- Using information by providers to carry out a **Data Protection Impact Assessment** (if required according to the applicable data protection legislation).
- Conducting a **fundamental rights impact assessment** prior to deployment (applicable particularly to certain AI systems used in the banking and insurance sectors).
- Keeping a **record of the events** ('logs') generated by the HRAI system.

[9] Art. 26.

- For AI-generated decisions that result in legal or similarly significant effects, explaining in a clear and meaningful manner the **role of the HRAI system in the decision-making process**.

D. Obligations relating to General-Purpose AI (GPAI) models

GPAI models must also meet a series of requirements under the AI Act, although such requirements are far less burdensome than the ones envisioned for providers of HRAI systems.

Specifically, for all GPAI models, providers shall:[10]

- draw up and keep up-to-date **technical documentation** of the model, including its training and testing process,
- put in place a policy to comply with **EU copyright law**, in particular to identify and respect any reservation expressed by the rightsholder(s) in relation the use of their work on the basis of the 'text and data mining exception'[11]; and
- provide a sufficiently **detailed summary** of the content used for training the model.

Moreover, in addition to the above obligations, providers of GPAI models deemed to pose 'systemic risk' are also required to:[12]

- perform model **evaluations**, including adversarial testing;
- assess and mitigate possible **systemic risks** arising from the development, deployment or use of the GPAI model;
- document and report to the competent authorities without undue delay any serious **incidents** and possible corrective measures to address them; and
- ensure an adequate level of **cybersecurity** protection.

E. Obligations relating to Low-risk AI systems[13]

Lastly, for low-risk AI systems, the AI Act introduces limited obligations, exclusively in relation to transparency. These moreover refer specifically to AI systems intended to interact with individuals and require that they be designed and developed in a manner that such individuals are aware they are interacting with an AI system. Similarly, for AI systems (including GPAI systems) that generate audio, images, video or text content, such outputs must be clearly marked as artificially generated or manipulated.

G. Penalties[14]

The AI Act provides for significant financial penalties, each time determined on the basis of the type of violation. In particular:

- Violations of rules on banned applications could result in a fine of up to €35 million or 7% of the offender's global annual turnover.
- Violations of the AI Act's obligations could result in a fine of up to €15 million or 3% of the offender's global annual turnover.
- The supply of incorrect information about an AI system could result in a fine of up to €7.5 million or 1.5% of the offender's global annual turnover.

H. Next steps for companies

Although the provisions of the AI Act will not apply immediately, it is strongly recommended that companies proactively take steps to prepare for full

[10] Article 53.

[11] See Article 4 of Directive (EU) 2019/790, which introduces an exception from copyright protection: copyrighted works may be used without authorization for the purposes of 'text and data mining' (TDM), unless the rightsholder(s) have expressed their reservation to such use of their work.

[12] Article 55 of the Regulation.

[13] Art. 50.

[14] Art. 99.

and timely compliance with the legislation. This involves understanding the way in which the new regulatory framework and initiating measures well in advance. More specifically, AI stakeholders are advised to take the following steps:

1. Assess AI Systems: Conduct a comprehensive assessment of their AI systems to determine their classification under the regulation. This includes identifying whether their AI systems fall under prohibited-risk, high-risk, limited-risk, or exempt categories.

2. Risk Assessment: Perform a thorough risk assessment of AI systems to evaluate potential risks to fundamental rights, safety, and societal values. This will help in understanding the level of compliance required and the necessary mitigation measures.

3. Understand their role in the AI value chain: Examine whether their role is that of the developer, deployer, distributor, etc. of the system, and their corresponding obligations.

4. Compliance Planning: Develop a compliance plan tailored to the specific requirements of the regulation. This may involve implementing technical and organizational measures to ensure compliance.

5. Gap Analysis: Conduct a gap analysis to identify any existing gaps in compliance with the regulation. Addressing these gaps early on will help in avoiding potential penalties and ensuring smooth compliance.

6. Training and Awareness: Train employees and stakeholders on the requirements of the regulation and their roles in ensuring compliance. Awareness programs can help foster a culture of compliance within the organization.

7. Stay Informed: Stay updated on best practices, industry standards, and developments in AI regulation to ensure ongoing compliance and mitigate potential risks.

Contact Us

Elisabeth Eleftheriades

PARTNER

e.eleftheriades@kglawfirm.gr

Follow Us

ATHENS OFFICE

28, Dimitriou Soutsou Str.,
115 21 Athens

T +30 210 817 1500
E kg.law@kglawfirm.gr

THESSALONIKI OFFICE

31, Politechniou Str.,
551 34 Thessaloniki

T +30 2310 441 552
E kg.law@kglawfirm.gr

www.kglawfirm.gr