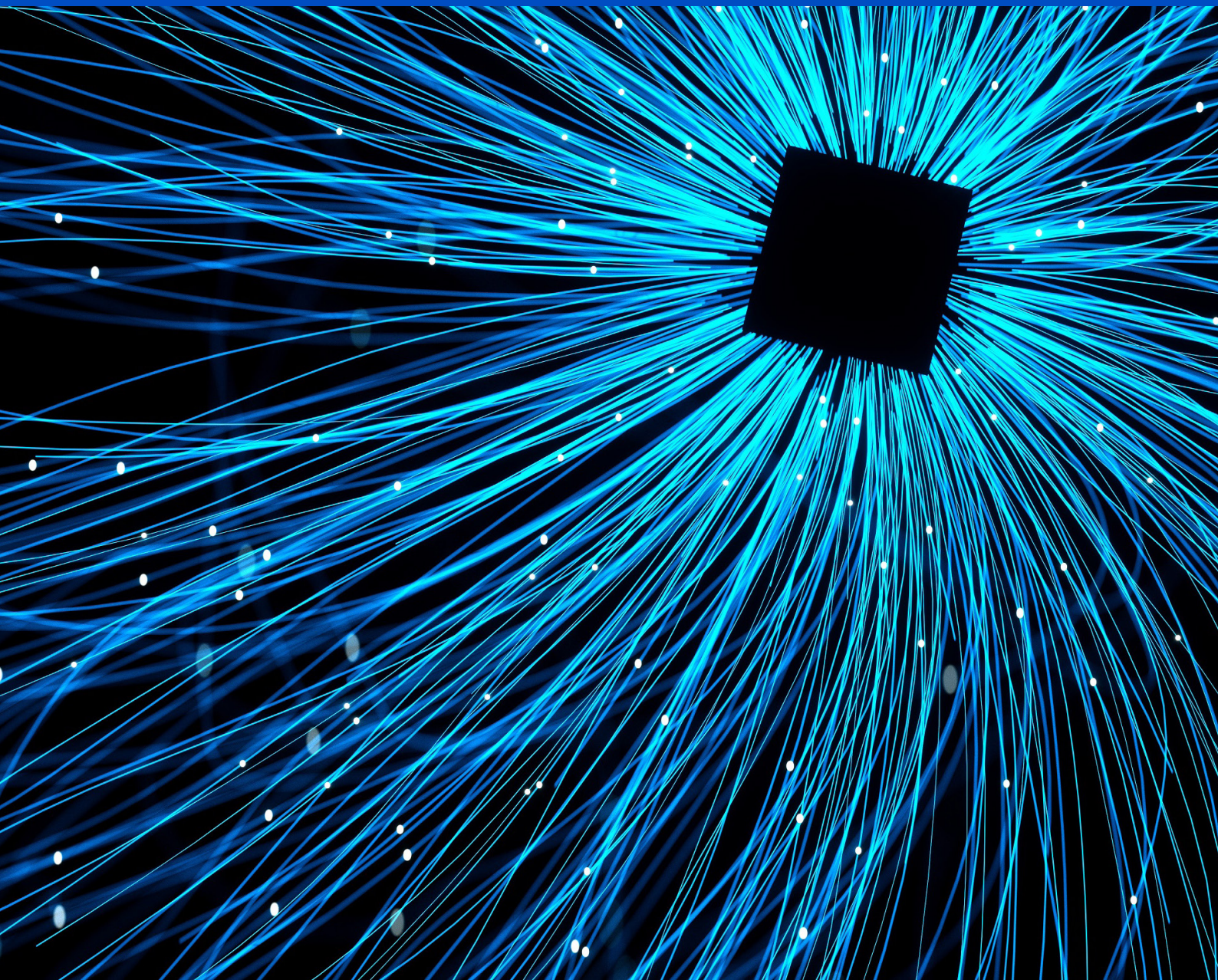
LATHAM & WATKINS

EU AI Act: Navigating a Brave New World

The Act establishes the world's first comprehensive regulatory framework for AI, and is expected to shape the future of AI regulation and governance both within and beyond the EU.

May 2024



Introduction

After three years of legislative debate, the Council of the European Union cast its final vote on the European Union (EU) Artificial Intelligence (AI) Act on 21 May 2024. Once published in the EU Official Journal in June, the EU AI Act will become the first set of AI regulations that has undergone a full legislative approval process. Originating from a European Commission proposal aimed at fostering the development and uptake of AI while ensuring fundamental rights across the EU and a human-centric approach to AI, the final text totals a remarkable 50,000 words, divided into 180 recitals, 113 Articles, and 13 annexes, and is a holistic set of risk-based rules applicable to all players in the AI ecosystem, from developers to exporters to deployers. With its broad reach and extensive remit, and like other EU legislative efforts before it, such as the GDPR, the AI Act is expected to have an impact beyond the EU borders and to shape the future of how this fast-evolving technology will be regulated for years to come.

- ***Timing and entry into force***. The AI Act will enter into force 20 days after its publication in the EU Official Journal. Most of its rules will be applicable 24 months after the Act's entry into force. Shorter applicability deadlines apply to:

  – bans on prohibited practices (six months after entry into force);
  – codes of practice (nine months after entry into force); and
  – most general-purpose AI rules (12 months after entry into force).

  A longer period of 36 months applies to obligations for certain high-risk systems covered by existing EU harmonization legislation and general purpose artificial intelligence systems (GPAIs) that have been on the market before the AI Act applies to them (i.e., 12 months after entry into force).

- ***Scope***. With respect to AI systems (i.e., products and services that are powered by AI) the Act does not regulate AI as such but rather its uses, hence it is organized around those uses that are likely to produce the highest risks. An "AI system" is defined as a machine-based system designed to operate with varying levels of autonomy, 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 aligns with the definitions from the OECD and Biden Administration Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (for further information on the Executive Order, see Latham's Client Alert President Biden's Executive Order on Artificial Intelligence — Initial Analysis of Private Sector Implications).

  One threshold issue is therefore whether a product can be considered out of scope if it does not have the required degree of autonomy, i.e., the ability to make decisions without direct human control. The AI Act clarifies that "systems that are based on rules defined solely by natural persons to automatically execute operations" are out of scope. The AI Act also excludes from its scope AI systems or models specifically developed and deployed for the sole purpose of:

  – scientific research and development;
  – commercial research, development, and prototyping that occur prior to the introduction of a product to the market;
  – individuals using AI systems for purely personal, non-professional activity;
  – AI systems used solely for military, defense, or national security objectives; and
  – certain narrowly defined open source models.

The exclusion of pre-launch development and prototyping is particularly significant, effectively excluding all AI product-related activities before the product becomes available in the EU.

- ***Applicability***. Like the EU Merger Regulation and other regimes that follow the "effects principle," the AI Act's reach extends beyond the EU's geographical boundaries. The Act applies to "providers placing on the market […] AI systems or […] general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country." Business users of AI (aka "deployers") are subject to the AI Act if they "have their place of establishment or are located within the Union." As a result, any business worldwide that targets the EU market is presumptively covered by the AI Act.

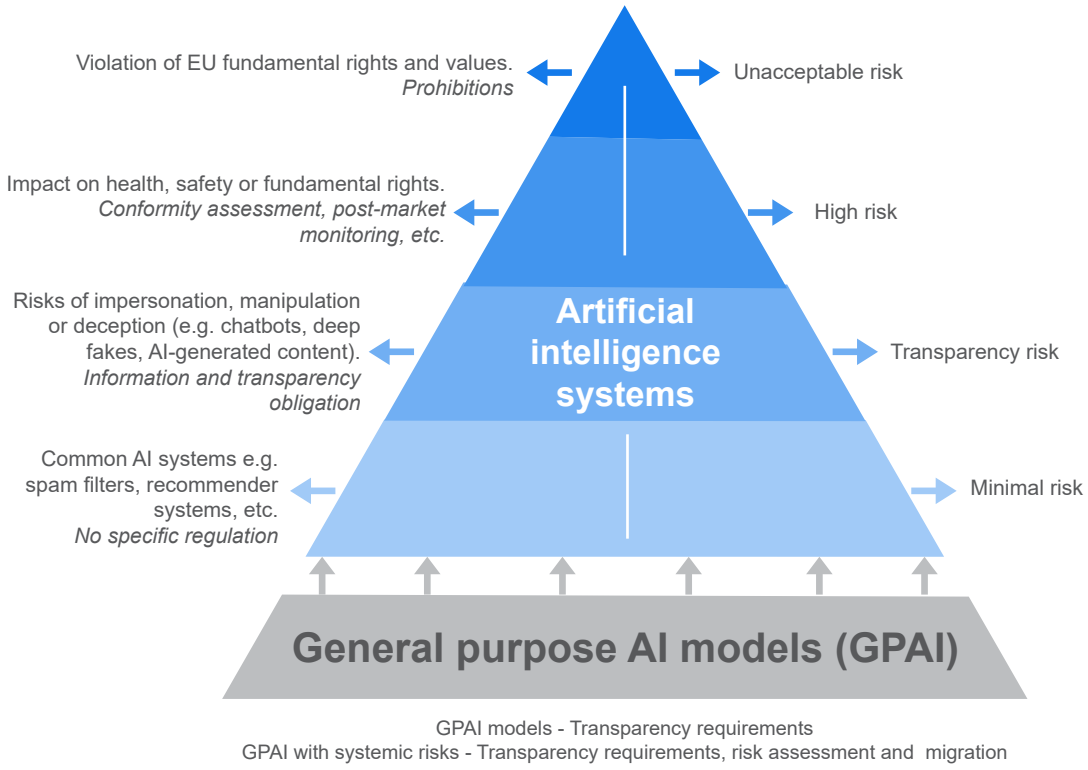
- ***Objects and Subjects of Regulation***. The AI Act is drafted on the basis of the EU's product liability and consumer protection legislative template and borrows many of its core concepts from there. The AI Act thus creates a primarily product-focused, risk-based approach, by which the product is either the AI system itself (e.g., a chatbot) or a product that uses or incorporates third-party AI systems or models (e.g., e-commerce platforms using AI systems to predict what customers might want to buy). Commonly, AI systems will be connected to or embedded in other products or services; e.g., a fraud detection AI system could be part of an online payment service, or an AI autopilot system could be part of an automobile. The subjects of regulation are primarily the provider (who develops and supplies the AI system or GPAI) and the deployer (who uses the AI system or GPAI in a professional capacity). The obligations of the provider are primarily centered around creating and maintaining a safe AI system, while deployer obligations center around the responsible and safe use of AI systems. Other subjects of regulation are importers, distributors, product manufacturers, and (to a lesser degree) other providers in the AI value chain.

- ***Penalties***. The consequences for noncompliance can be significant, with the highest fines reaching the greater of (or, in the case of SMEs, the lower of) €35 million or 7% of global revenue, depending on the infringement.

- ***Enforcement***. The AI Act relies on a double-layered enforcement mechanism divided between the EU and Member States. The European Commission will be at the center of enforcement with the EU AI Office, which will be established imminently. The EU AI Office will enforce the GPAI rules, foster international cooperation, and, most importantly, follow the developments of AI and propose guidance, as well as amendments and integrations to the Act. The AI Office will be assisted by a scientific panel of independent experts, by the European Artificial Intelligence Board (composed of one representative per Member State) and by a forum of stakeholders. In parallel, Member States will have to establish or appoint market surveillance and notifying authorities to implement the rules governing AI systems at the national level under the coordination of the Commission. The AI Act does not explicitly provide for a private right of action but is part of a package of reforms introduced by the EU Commission and so must be read in conjunction with the proposed AI Liability Directive and revised Directive on Liability for Defective Products which provides rules for a fault-based liability regime for damages caused by AI Systems (as defined under the EU AI Act). Furthermore, as with any EU regulation, affected parties will be able to invoke the rules of the AI Act directly in front of EU national courts. In addition, the AI Act will be added to the list of legislative instruments that can be actionable on the basis of the Representative Actions Directive, meaning that it can also be used as a source of collective damage actions in Europe. Further, affected individuals will be able to complain to the market surveillance authorities appointed in each Member State.

AI System Categorization and Key Requirements

The EU AI Act establishes a risk-based approach, categorizing AI systems based on their capacity to cause harm to society. The higher the risk, the stricter the rules and obligations. Complying with the AI Act will therefore require companies to understand which risk category each of their AI systems or GPAIs fall into. The risk classification will inform which set of obligations applies. The risk levels are:



Source: European Commission

- **Prohibited AI practices** are those that violate fundamental EU rights and values. AI systems are banned from the EU if their purpose is to:
  - purposefully manipulate or use deceptive techniques;
  - exploit vulnerabilities of a person due to age, disability, or their social or economic situation;
  - generate certain social scores to groups or individuals;
  - assess or predict whether an individual is likely to commit a crime, i.e., “minority report”-style crime prediction/predictive policing;
  - create facial recognition databases via untargeted scraping;
  - infer emotions in the workplace or in educational institutions;
  - create biometric categorizations for race, political views, sex, etc.; or
  - generate certain real-time biometric ID in publicly accessible spaces for law enforcement.

AI systems used for prohibited AI practices must be withdrawn from the market within six months of the AI Act coming into effect. Organizations will need to be alert to the Commission amending the list of prohibited AI practices under the AI Act. Violations carry fines of up to the greater of (or, in the case of SMEs, the lesser of) €35 million or 7% of global revenues.

- **High-risk AI systems** are those that are deemed a high risk to the health and safety or fundamental rights of individuals. The high-risk AI system classification captures the following:
  - AI systems that are products, or safety components of products, covered by specified, existing EU laws (including certain medical devices, toys, machinery, etc.) if that product is required to undergo a third-party conformity assessment under such EU laws.
  - AI systems used for specified high-risk purposes (listed in Annex III of the AI Act). Those include AI systems intended to be used for:
    - profiling;
    - (certain) biometric identification and categorization;
    - as safety components in critical infrastructure (traffic, electricity, gas, water, etc.);
    - determining access to educational and vocational training, evaluating learning outcomes, or detecting cheating;
    - evaluating job applications and making decisions about promotions and job descriptions in the workplace;
    - determining access to public and private essential services, such as healthcare, credit, insurance, and emergency responses; and
    - the administration of the justice system and immigration.

  Importantly, the AI Act excludes from the high-risk AI system category those systems listed in Annex III that are used: (1) for narrow procedural tasks; (2) for the improvement of a previously completed human activity result; (3) to detect decision-making patterns or deviations from it instead of replacing human decision; and/or (4) to perform a preparatory task to an assessment (unless such activities involve profiling of individuals, in which case the AI system will always be considered high risk), on the basis that such a use case "does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons". The Commission and AI Board will develop practical guidance on this exception.

  Providers or high-risk AI systems are subject to strict requirements. In effect, they have to implement a comprehensive life-cycle risk management program for the AI system.

  Before placing a high-risk AI system on the market, providers must, among other things, perform a conformity assessment and register the AI system in a central, public EU database. Once launched, the provider must continuously update the conformity assessment. Most conformity assessments will be conducted internally, which reduces delays but also means that the provider launches "at risk." Only a limited number of high-risk systems (e.g., those related to biometric IDs) require independent conformity assessments by an accredited body before launch. On the basis of the conformity assessment, the high-risk system should visibly bear a CE marking, which indicates that the AI system is compliant with the AI Act. Conformity will be monitored by the European Artificial Intelligence Board (AI Board) and the relevant national supervisory authorities. Violations carry fines of up to the greater of (or, in the case of SMEs, the lesser of) €15 million or 3% of global revenues.

- **Other (limited-risk) AI systems** are subject to disclosure and transparency obligations. For example, chatbots, applications generating deepfakes of images, audio, and video, as well as generative AI creating "text […] published with the purpose of informing the public on matters of public interest" (e.g., news or press releases) must disclose that the content was generated by an AI. Most output of generative AI applications must be watermarked in a machine-readable format. Violations can trigger fines of up to the greater of (or, in the case of SMEs, the lesser of) €15 million or 3% of global revenues.
- **All other AI systems (**not prohibited, not high-risk, not subject to transparency requirements) are not subject to regulation by the AI Act. The Commission notes that "the vast majority" of AI systems will fall into this category, although achieving that regulatory calibration may require clarifications by the Commission, given the rapid replacement of traditional, deterministic program architectures with trained models in a wide range of applications.

General Purpose AI Models

General purpose AI systems (GPAIs) are subject to a separate classification and regulation regime.

The AI Act defines a GPAI model as:

"an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are released on the market."

What exactly is captured by this definition will likely be subject to debate going forward. While the AI system definition hinges (in large part) on the level of autonomy enjoyed by an AI system, the GPAI definition hinges on the generality of the model in question. Models that do not "display significant generality" or are not "capable of performing" a "wide range of tasks," are not GPAIs. Based on that definition, it stands to reason that certain model architectures that do not enable the creation of generalizable classifications are not GPAIs. One example of a class of models that can clearly be captured by the GPAI definition (in fact, that inspired the GPAI definition) are large language models (LLMs).

With respect to GPAIs, the AI Act creates three categories:

a. GPAI models with systemic risk, which require "high impact capabilities" that are presumed if the cumulative training compute of the model exceeds 10^25 FLOPs

b. Normal GPAI models (without systemic risk) that are proprietary

c. Normal GPAI models (without systemic risk) that are released as open source models.

Open source models benefit from somewhat lighter-touch regulation than proprietary models, which is a policy decision in favor of open source and decentralized development that runs throughout the AI Act. However, if the GPAI falls into the systems risk category, proprietary and open source models are treated the same. The GPAI provider obligations include:

Requirements/Obligations	Systemic Risk	Normal, Proprietary	Normal, Open Source
Technical documentation for regulators, upon request	⊗		
Documentation for downstream AI system providers	⊗		
Copyright and reservation of rights policy	⊗	⊗	⊗
Public summary of training content	⊗	⊗	⊗
Cooperation with authorities	⊗	⊗	⊗
For ex-EU providers, appoint authorized representative	⊗	⊗	
Model evaluation, adversarial testing	⊗		
Risk assessment and mitigation	⊗		
Report and address serious incidents	⊗		
Cybersecurity and physical model security	⊗		

The GPAI provider must notify the Commission if and when a GPAI model meets the criteria for "systemic risk," and must comply (and document compliance with) the applicable requirements. The Commission has wide-ranging investigative powers to monitor and ensure compliance. Providers of GPAIs outside of the EU must appoint an "authorized representative" in the EU before launch. The authorized representative is the keeper of all relevant compliance information and documentation, and acts as the Commission's first point of contact. The Act also provides for the creation of "codes of practice" that will specify the requirements and facilitate compliance. Those codes of practice will be highly significant for the practical impact of the AI Act going forward, and we expect significant industry engagement on those codes.

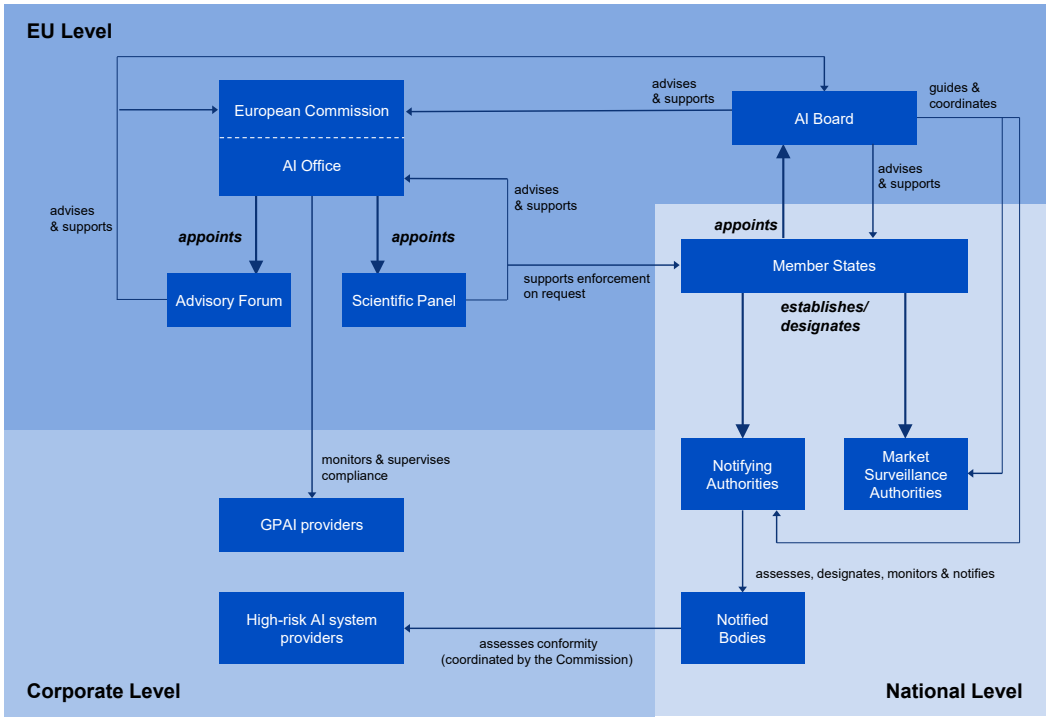
Although the GPAI provisions create a special regime for GPAIs, they are not *lex specialis* to the rest of the AI Act. Thus, if a GPAI system also qualifies as a "high-risk" AI system, then both regimes would apply.

How Will Implementation Unfold?

Timeline

Once published in early June, the Act should be in force by the end of June 2024. The timeline for implementation will therefore be as follows:

- **End of December 2024:** Prohibited AI practices must be withdrawn from the market.
- **End of March 2025:** Codes of practice will be ready.
- **End of June 2025:** GPAI must be in compliance. Governance structure (AI Office, European Artificial Intelligence Board, national market surveillance authorities, etc.) will have to be in place.
- **End of December 2025:** EC to adopt Implementing Act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan.
- **End of June 2026:** All rules of the AI Act become applicable, including obligations for high-risk systems defined in Annex III (list of high-risk use cases). Member States shall ensure that their competent authorities have established at least one operational AI regulatory sandbox at national level.
- **End of June 2027:** Obligations for high-risk systems defined in Annex II (list of EU harmonization legislation) apply.



Monitoring at the EU Level

The European Commission has the overall responsibility to ensure the correct implementation of the AI Act, including amending through delegated and implementing acts, such as adding criteria for classifying the GPAI models as presenting systemic risks. The Commission, through the work of the AI Office, is also expected to develop guidelines on the practical implementation of the AI Act.

The Commission has exclusive powers to supervise and enforce the obligations of GPAI, including to monitor and supervise compliance with the AI Act of an AI system which is based on a GPAI model, when the model and the system are developed by the same provider.

The European Commission's AI Office will be responsible for implementation in relation to GPAI. Its tasks include drawing up codes of practice, classifying models with systemic risks, and monitoring the effective implementation and compliance with the AI Act. The latter is facilitated by the powers to request documentation drawn up by the provider or any additional information to assess compliance, conduct model evaluations, investigate upon alerts, and request providers to take corrective action. The Commission may impose fines on providers of GPAI of up to €15 million or 3% of global revenues, after communicating its preliminary findings to the provider of the GPAI model and giving it an opportunity to respond.

The AI Office will be supported by a scientific panel of independent experts.

In addition, **a European Artificial Intelligence Board (Board) will be established**. The Board will be composed of one representative per Member State. It will advise and assist the Commission and the Member States in order to facilitate the consistent and effective application of the AI Act, notably by contributing to the coordination among competition authorities, providing advice, collecting and sharing technical and regulatory expertise, and issuing recommendations. **An advisory forum**, composed of representatives of industry, start-ups, small and medium-sized enterprises, civil society, and academia, will also be established to provide technical expertise and advise the Board and the Commission, and to contribute to their tasks.

Monitoring at the National Level

With respect to AI systems, each Member State will have to establish or designate at least one market surveillance authority, in addition to at least one notifying authority.

Market surveillance authorities established or designated by each Member State will report annually to the Commission and relevant national competition authorities, disclosing any information identified in the course of market surveillance activities that may be of potential interest for the application of EU law on competition rules.

The market surveillance and notifying authorities will have **investigative powers** and may send reasoned requests to providers and deployers. They can carry out evaluations of AI systems which they have sufficient reason to consider that they present a risk, as well as of AI systems classified by the provider as non-high-risk, when the authority has reason to believe that these AI systems may in fact be high-risk. In case of non-compliance, the authority can require the relevant operator to take all appropriate corrective actions to bring the AI system into compliance, to withdraw the AI system from the market, or to recall it within a period the market surveillance authority may prescribe. It can also take all appropriate provisional measures to prohibit or restrict the AI system's national market availability or deployment, to withdraw the product or the standalone AI system from that market or to recall it, or to impose fines. If the market surveillance

authority considers that the non-compliance is not restricted to its national territory, it must inform the Commission and the other Member States without undue delay of the results of the evaluation and of the actions which it has required the operator to take.

The Commission will coordinate the action of the market surveillance authorities and oversee the measures they take. If the market surveillance authority of a Member State raises objections against a measure taken by another authority, or if the Commission considers the measure to be contrary to EU law, the Commission evaluates and decides whether the measure is justified or not.

If the market surveillance authority of a Member State finds an example of non-compliance (e.g., the CE marking has not been affixed, or the registration in the EU database has not been carried out), it must require the relevant provider to become compliant. If the non-compliance persists, the market surveillance authority can take appropriate and proportionate measures to restrict or prohibit the high-risk AI system's availability on the market or to ensure that it is recalled or withdrawn from the market without delay.

Member States will lay down the rules on **penalties and other enforcement measures**, which may also include warnings and non-monetary measures, applicable to infringements of the AI Act by operators.

Cooperation Between the AI Office and the National Market Surveillance Authorities

The Commission and the market surveillance authorities will be able to propose joint activities, including joint investigations, to be conducted either at national level or jointly with the Commission. The aim will be to foster compliance, identify non-compliance, raise awareness, or provide guidance in relation to the AI Act with respect to specific categories of high-risk AI systems that present a serious risk across two or more Member States. The AI Office shall provide coordination support for joint investigations.

If the relevant market surveillance authorities have sufficient reason to consider **GPAI systems** that can be used directly by deployers for at least one purpose that is classified as high-risk to be non-compliant with the requirements laid down in the AI Act, they must cooperate with the AI Office to carry out compliance evaluations, and must inform the Board and other market surveillance authorities accordingly. If a market surveillance authority is unable to conclude its investigation of the high-risk AI system due to its inability to access certain information related to the GPAI model (despite having made all appropriate efforts to obtain that information), it may submit a reasoned request to the AI Office, by which access to that information shall be enforced.

Common Questions About the AI Act

1. **I am based in the US. Do I need to worry about the EU AI Act?**

   The AI Act only applies to systems that are intended to be used in the EU. Therefore, organizations outside the EU will fall under the Act only if they supply their products to the EU, or if the output produced by their AI systems will be used in the EU. Third parties who buy the rights and place the AI system on the EU market (e.g., importers) are considered providers.

2. **I created and use AI tools, but only for internal use. Does the AI Act apply to me?**

   In principle, the AI Act does not apply to AI models that are used exclusively for internal processes. However, in order to qualify for this exemption, these internal AI tools must not be essential for providing a product or service to third parties and should not affect the rights of natural persons.

3. **I provide a free and open source AI model. How does the AI Act affect me?**

   The regulation of open source AI models is complex. First, the definition of "open source" in the AI Act is narrow. Only non-monetized models (directly or indirectly) qualify as "open source." Open source AI systems are effectively regulated like non-open source systems if they fall into the prohibited, high-risk, or limited-risk categories. Open source GPAIs are regulated like non-open source models if they exhibit systemic risk. Open source models that do not exhibit systemic risk are exempted from the model requirements, except for the obligations to implement a copyright policy and publish a summary of the training data. Open source model providers located outside of the EU seeking to limit the application of the AI Act should attempt to restrain access to the model by EU-based persons, for example by limiting the license grant to jurisdictions outside of the EU.

4. **Where do I start preparing for compliance?**

   First of all, categorize your AI system. AI providers, deployers, importers, and distributors should identify their AI and GPAI systems and use cases, and assess whether each AI system should be categorized of limited, high, or unacceptable risk, or involving systematic risk in the case of GPAI systems (or minimal risk and therefore not regulated by the AI Act). Such assessments are potentially complex exercises in practice, due in particular to the various exclusions applicable to the high-risk category. AI developers and providers may wish to consider whether they can modify their potentially high-risk AI systems in order to benefit from such exclusions, and therefore avoid the high-risk category obligations (bearing in mind that the Commission will provide further guidance on these exclusions, and that the list of high-risk AI systems may be amended in the future).

5. **Can I already use any other tool to ensure compliance?**

   To help AI providers prepare for compliance with the EU AI Act, the Commission has launched an initiative called the "AI Pact," which seeks the commitment of AI providers to start implementing the requirements of the Act on a voluntary basis as of its adoption. This should allow providers to prepare their systems and internal processes before compliance becomes mandatory.

Whether high-risk or not, providers should consider developing and using a code of conduct voluntarily. The Commission will assess codes of practice and, if approved, will give them validity within the EU.

Contacts

Elisabetta Righini
Partner
Brussels
elisabetta.righini@lw.com
+32.2.788.6238

Hanno F. Kaiser
Partner
San Diego / San Francisco
hanno.kaiser@lw.com
+1.858.509.8458

Tim Wybitul
Partner
Frankfurt
tim.wybitul@lw.com
+49.69.6062.6560

Fiona M. Maclean
Partner
London
fiona.maclean@lw.com
+44.20.7710.1822

Michael H. Rubin
Partner
San Francisco
michael.rubin@lw.com
+1.415.395.8154