WILSON SONSINI

10

Things You Should Know About the

EU Artificial Intelligence Act

September 2024

Table of Contents

1 – What is the EU AI Act? 2
2 – When will the obligations under the AI Act start to apply? 3
3 – Does the AI Act apply to us? 4
4 – Are all forms of AI subject to the same obligations under the AI Act? 5
5 – Does the AI Act prohibit certain AI systems? 6
6 – What obligations are imposed on providers of high-risk AI systems? 6
7 – What obligations are imposed on providers of GPAI models? 7
8 – Do we need to update our contracts? 8
9 – How will the EU AI Act be enforced? 8
10 – How can we prepare for the AI Act as of today? 9
Staying Up to Date with AI Legislative Developments 10

1. What is the EU AI Act?

The EU Artificial Intelligence Act (AI Act) is the first comprehensive legislation that intends to regulate AI horizontally across all sectors in the European Union (EU), subject to hefty fines of up to EUR 35 million or seven percent of the total worldwide annual turnover, whichever is higher. It has far reaching consequences on all companies developing, implementing, or using AI solutions in the EU and beyond.

The AI Act regulates AI systems according to the level of risk associated with how they are intended to be used, with most obligations imposed on what is defined as "high-risk AI." The AI Act also regulates general-purpose AI (GPAI) models and requirements are tiered according to whether the GPAI has systemic risk. These obligations apply in addition to existing requirements, including the EU General Data Protection Regulation (GDPR).

2. When will the obligations under the AI Act start to apply?

Has the AI Act now finally become law?

Yes, the AI Act officially entered into force on August 1, 2024, but not all provisions apply right away.

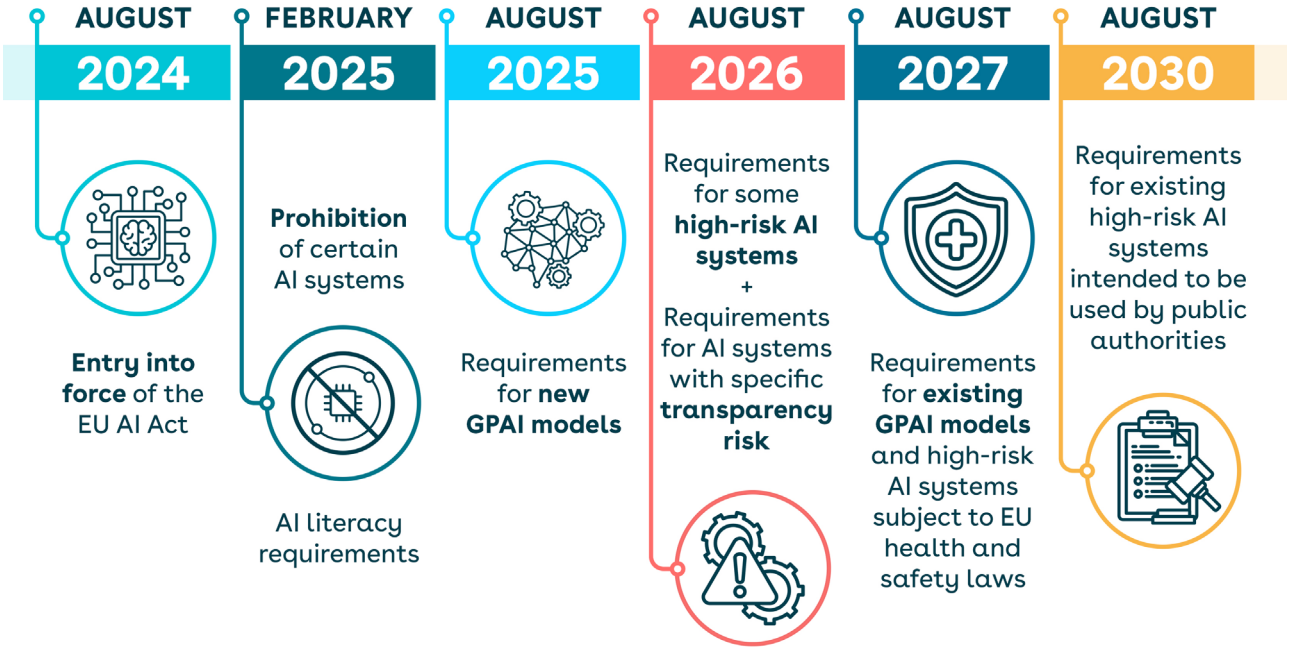
When will the AI Act start to apply?

The AI Act will start to apply in phases.

1. The first provisions to kick in will be i) the ones which prohibit certain applications of AI (e.g., AI systems that exploit individuals' vulnerabilities, untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases) and ii) those which require providers and deployers of AI systems to ensure those operating and using AI systems on their behalf (e.g., staff) have a sufficient level of AI literacy: these provisions will start to apply on February 2, 2025.

2. The second set of provisions to apply will be those imposing requirements in relation to new GPAI models: these provisions will start to apply on August 2, 2025.

3. Most of the rules for high-risk AI systems and AI systems with specific transparency risk will start to apply on August 2, 2026. High-risk AI systems subject to health and safety laws will apply on August 2, 2027.



Is there an additional grace period for AI systems and GPAI already offered in the EU?

Yes. There will be more time to comply with the AI Act for high-risk AI systems and GPAI models that are released on the EU market before the corresponding obligations kick in:

- Operators of high-risk AI systems that are offered in the EU before August 2, 2026 will only need to comply with the AI Act in the event of a significant design change. As an exception to this, if the high-risk AI system offered in the EU is intended to be used by public authorities, the providers and deployers will need to comply with the rules by August 2, 2030, regardless of whether there has been a significant design change or not.
- Providers of GPAI models that are offered in the EU before the corresponding rules for GPAI start to apply (i.e., August 2, 2025) will have an additional two years to comply with the requirements, i.e., by August 2, 2027.

3. Does the AI Act apply to us?

To which players does the AI Act apply?

The AI Act applies to different companies across the AI distribution chain, including providers, deployers, importers, and distributors (collectively referred to as "Operators"):

- *Providers:* Most obligations are imposed on AI providers who develop AI systems or GPAI models to be offered in the EU under their own name or brand. Companies who source AI solutions from third parties could, depending on the circumstances, also qualify as "providers" if they include the AI solution in their own offering.
- *Deployers:* The AI Act also imposes some obligations on deployers of AI systems, such as obligations to be transparent about their AI-generated content. The AI Act has a "household exemption," i.e., the concept of "deployer" does not include persons that use an AI system in the course of a personal nonprofessional activity.
- *Importers and distributors:* The AI Act also applies to companies who import into the EU or distribute AI systems developed by another company.

What if we are not established in the EU?

The AI Act may still apply to your company, even if it is not established in the EU, as it has an extraterritorial reach. For the AI Act to apply to providers located outside the EU, it is enough that they make an AI system or GPAI model available on the EU market. Moreover, even if only the output generated by the AI system is used in the EU, the AI Act still applies to the provider and deployer of the AI system.

This means that many providers of AI systems or GPAI models based outside the EU—including in the United States—could fall under the scope of the AI Act and could face investigations by EU AI regulators.

Non-EU providers of GPAI models and high-risk AI systems are required to appoint an AI representative in the EU to act as a contact point for EU regulators and keep copies of key compliance documentation.

To what systems or models does the AI Act apply?

The AI Act applies to "AI systems" and "GPAI models," which are both broadly defined:

- AI systems include a wide range of software operating with varying levels of autonomy and capable of generating outputs such as content, predictions, recommendations, or decisions and that may exhibit adaptiveness after deployment.
- GPAI models are defined as AI models which i) display significant generality, ii) are capable of competently performing a wide range of distinct tasks, and iii) can be integrated into a variety of downstream AI systems or applications. GPAI models require the addition of further components (e.g., a user interface) in order to become an AI system. The AI Act indicates that large generative AI models which can perform a wide array of tasks are an example of a GPAI model.

4. Are all forms of AI subject to the same obligations under the AI Act?

No. As the AI Act follows an approach based on the level of risk ("risk-based approach"), the scope of obligations depends on the level of risk associated with the purpose of the AI system or with the GPAI model.

- **Categories of AI systems.** The AI Act prohibits certain AI systems which pose a level of risk deemed unacceptable in the EU (see #5) and impose stringent requirements on AI systems considered to pose high risks (see #6). Other AI systems which are not considered to pose a high risk are nonetheless subject to transparency obligations, such as informing individuals i) that they are interacting with an AI system, ii) whether the AI system generates "deep fakes," and iii) whether they are exposed to an emotion recognition system or a biometric categorization system. In addition, when an AI system generates synthetic audio, image, video, or text, such content must be marked in a machine-readable format and detectable as artificially generated or manipulated.
- **Categories of GPAI models.** The AI Act imposes specific obligations on GPAI models. The European Commission (EC) will designate more powerful GPAI models that could pose "systemic risks." Providers of such models are subject to additional obligations.

5. Does the AI Act prohibit certain AI systems?

Yes. The AI Act bans certain AI systems, including AI systems that manipulate or exploit individuals, AI systems that perform social scoring, criminal predictions, untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases, AI systems that infer individuals' emotions in the areas of workplace or education institutions, and AI systems that perform biometric categorization to deduce sensitive data about individuals, such as their ethnicity or religion. The use of real-time facial recognition systems by law enforcement in public areas is also banned, subject to narrow exceptions.

6. What obligations will be imposed on providers of high-risk AI systems?

High-risk AI systems include systems used for biometric identification, biometric categorization, emotion recognition, assessing creditworthiness, managing critical infrastructure, assessing students, risk assessment and pricing in relation to life and health insurance, making employment-related decisions, certain activities related to law enforcement, migration controls, administration of justice and elections and other systems listed in the law. In addition, an AI system that is a safety component of a regulated product (e.g., a product subject to EU health and safety legislation), or that is itself a regulated product, also qualifies as "high-risk" (e.g., cars, toys, aviation).

Such high-risk AI systems are subject to a range of requirements, including to:

- establish a risk management system, covering risk identification, testing, and the adoption of risk-mitigation measures;
- apply data governance and management practices when training models;
- draw up and update technical documentation and maintain automatic recording of events (logs);
- provide instructions for use to the deployers who use the AI system;
- ensure human oversight (e.g., including a "stop" button for human reviewers to interrupt the AI system);
- achieve an appropriate level of accuracy, robustness, and cybersecurity of AI systems;
- develop a post-market monitoring system to be able to detect any instances of malfunctioning;
- undergo conformity assessment procedures before being released on the market;
- register the AI system in a public database maintained by the EC; and
- notify EU regulators if the AI system poses risks to individuals' health and safety, or to fundamental rights, or in the event of a serious incident.

7. What obligations are imposed on providers of GPAI models?

Providers of GPAI models are required to:

- draw up (and keep updated) technical documentation;
- provide documentation to companies who plan to integrate the GPAI in their AI systems;
- draft and implement policies for compliance with EU copyright law; and
- publish a summary of the data used for training.

The EC will designate more powerful GPAI models that could pose "systemic risks."

For instance, a GPAI model will be presumed to pose "systemic risk" if the cumulative amount of compute used for training the GPAI model is greater than 10^25 floating point operations (FLOPs). Other types of GPAI models with high impact capabilities may also be considered to pose systemic risks, unless the provider demonstrates that its GPAI model does not have a significant impact on the EU market due to its limited reach, or due to the lack of negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain (e.g., through the dissemination of false content).

Providers of such models are subject to additional obligations including to:

- conduct model evaluation to identify systemic risks, including through adversarial testing;
- assess the systemic risks that the model may present and implement measures to mitigate them;
- monitor serious incidents and notify them to the AI Office and regulators in the relevant EU countries; and
- ensure an appropriate level of cybersecurity.

Codes of practice will be developed to operationalize these new obligations.

8. Do we need to update our contracts?

Providers, deployers, and other parties in the AI value chain need to carefully assess their obligations under the AI Act and consider the implications on their contracts. For instance, a party could consider requiring the other party's assistance to comply with its own obligations under the AI Act. With regard to high-risk AI systems, the AI Act requires such assistance to be set out in a written agreement between the provider of the AI system and the third party supplying AI elements used in the AI system. The new AI Office may develop voluntary model terms for such contracts. In the meantime, companies can draw inspiration from the EC's model contractual clauses for public organizations wishing to procure AI systems developed by an external supplier, which are available **here**.

9. How will the EU AI Act be enforced?

What are the maximum fines under the AI Act?

Violations of the AI Act are subject to hefty fines of up to EUR 35 million or seven percent of the total worldwide annual turnover, whichever is higher.

Can regulators ban AI systems?

Yes, regulators can require an operator to withdraw their AI system from the EU market.

Who will enforce the AI Act?

- Rules on GPAI models will be enforced by the newly created AI Office of the EC, which is expected to become the EU center of AI expertise.
- Enforcement of the rules on AI systems will primarily be at the national level. Each EU country needs to identify the competent regulators to enforce the AI Act by August 2, 2025. Some countries have already announced their intentions, e.g., Spain has already created a distinct AI authority. In some other countries, existing data privacy regulators may be entrusted with the task of overseeing compliance with the AI Act.

10. How can we prepare for the AI Act as of today?

What should we be doing now?

Companies should consider:

- determining whether the AI Act applies to them and whether they are considered a provider or deployer of a high-risk AI system;
- identifying the obligations of the AI Act which entail changes to their products or services and assessing how to implement such changes on time;
- identifying and documenting risks posed by their AI systems (as well as their risk mitigants / safeguards) and revising the datasets used to train algorithms;
- anticipating requirements on risk assessments and data governance;
- appointing an AI governance working group to steer AI Act compliance efforts; and
- developing a compliance strategy and assigning sufficient resources for compliance.

Can we use our GDPR documentation for compliance with the AI Act?

Companies that are subject to the AI Act and GDPR should be able to leverage some of their GDPR compliance documentation. For instance:

- a Data Protection Impact Assessment can serve as basis for parts of the risk management system;
- a Data Handling Policy that lays down rules on how employees should handle personal data can be expanded to cover the use of (personal) data with respect to AI systems (e.g., training data);
- a Privacy by Design Policy can be used to anticipate some key AI compliance steps, e.g., AI risk assessments, AI data governance, transparency;
- a Data Security Policy can be expanded to include a company's AI system in its data security program; and
- an Incident Response Policy can be expanded to include the steps employees should take when they identify an AI system which malfunctions or poses a risk to individuals.

Staying Up to Date with AI Legislative Developments

Wilson Sonsini is closely following the developments in the AI global regulatory landscape. You can stay up to date with developments concerning the AI Act by registering for our AI Working Group Quarterly Newsletter **here**. For more information on the legislative history of the AI Act, please see our client alerts on the EU Council's position **here** and the EU Parliament's position **here**.

Wilson Sonsini has more than 150 attorneys across the U.S., Europe, and Asia with unparalleled experience spanning multiple decades, representing over 1,000+ AI companies of all stages and in every sub-sector of the AI/ML industry around the world, including one-quarter of the Forbes 2023 AI 50 list. For more information about our team, please visit our website **here**.

Cédric Burton
Partner
Data, Privacy, and Cybersecurity
cburton@wsgr.com
32-2-2745722

Laura De Boel
Partner
Data, Privacy, and Cybersecurity
ldeboel@wsgr.com
32-2-2745718

Yann Padova
Partner
Data, Privacy, and Cybersecurity
ypadova@wsgr.com
32-2-2745716

Nikolaos Theodorakis
Partner
Data, Privacy, and Cybersecurity
ntheodorakis@wsgr.com
32-2-2745709

WILSON SONSINI

650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | www.wsgr.com

Wilson Sonsini has 19 offices in technology and business hubs worldwide. For more information, visit **wsgr.com/offices**.