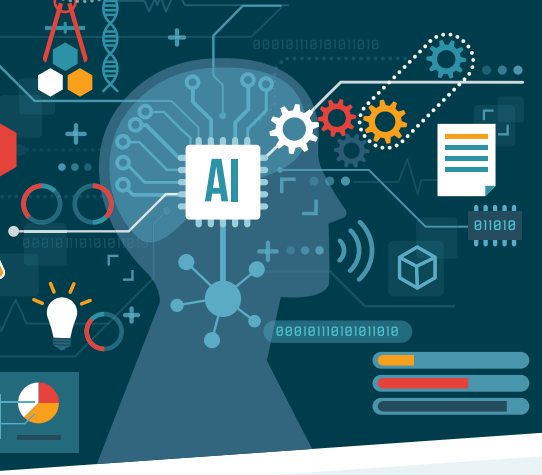


WILSON SONSINI

10 Things You Should Know About the EU Artificial Intelligence Act

1. What is the EU AI Act, and how to get ready?

The Artificial Intelligence Act (AI Act) is the first comprehensive legislation that intends to regulate AI horizontally across all sectors in Europe. It will have far reaching consequences on all companies developing, implementing, or using AI solutions in the EU and beyond.

These FAQs provide key information you should know before the AI Act is adopted, and some tips on what you can already be doing to prepare.

Is the EU AI Act already applicable?
No, it is still a draft law. It was proposed by the EU Commission in April 2021. Currently, the EU Parliament and the EU Council are negotiating the final text of the AI Act to be enacted as law. We expect that a final text will be agreed upon before the end of 2023. When adopted, the law will allow a period before it becomes enforceable, which could be between 12 to 36 months.

How will the EU AI Act work?
The AI Act will regulate 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." These obligations will apply in addition to existing requirements, including those defined in the EU General Data Protection Regulation (GDPR).

2. Will the AI Act apply to us?

The AI Act will apply to different companies across the AI distribution chain:

- **Providers:** Most obligations are imposed on AI providers who develop AI systems intended to be placed on the EU market. Companies who source AI solutions from third parties could also qualify as "providers."
- **Importers and distributors:** The AI Act also applies to companies who import in the EU or distribute AI systems developed by another company.
- **Users:** The AI Act imposes some obligations on users of AI systems, such as obligations to be transparent about their AI-generated content. In this context, "user" does not have the same meaning as "data subject" under the GDPR.

The definition of "**AI system**" continues to be negotiated. It is likely to include a wide range of software operating with varying levels of autonomy and capable of generating outputs such as content, predictions, etc.

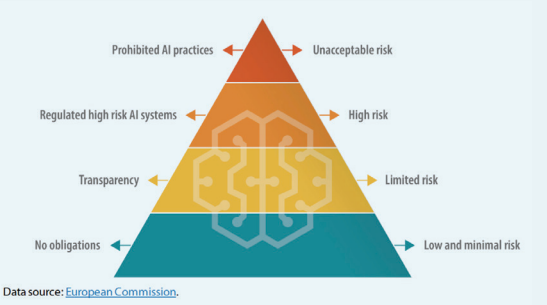
The EU Parliament proposed that the AI Act should lay down specific rules for "**foundation models**" which would include AI models designed for generality of output and adaptable to different tasks (such as LLMs). The EU institutions are still negotiating how to regulate foundation models in the final text of the AI Act.

3. What if we are not established in the EU?

The AI Act may apply to you 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 available on the EU market. Moreover, even if only the output generated by the AI system is used in the EU, the AI Act would apply. This means that **many providers of AI systems 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.

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 type of AI system, in particular its purpose and the risk that it presents:



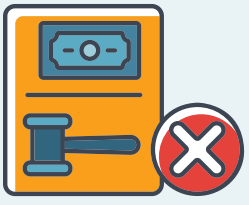
Data source: European Commission.

- **High-risk AI systems face the most stringent requirements.** AI systems used for biometric identification, assessing creditworthiness, managing critical infrastructure, or making employment-related decisions, and AI systems that similarly impact fundamental rights or create health and safety risks, could qualify as high-risk AI systems (subject to limited exemptions). The scope of high-risk AI systems is still being discussed. Such systems will be subject to a range of requirements, including requirements to:
  - establish a risk management system;
  - apply data governance and management practices when training models;
  - draw up and update technical documentation and maintain automatic recording of events (logs);
  - comply with transparency requirements;
  - ensure human oversight (e.g., including a "stop" button for human reviewers to interrupt the AI system);
  - achieve accuracy, robustness, and cybersecurity of AI systems;
  - undergo conformity assessment procedures before being released on the market; and
  - register the AI system in a public database maintained by the EU Commission.
- The EU institutions are still negotiating how to regulate **foundation models**, but they will likely be subject to certain transparency obligations. "Very capable" foundation models (also called "high impact" foundation models) may also be subject to ex-ante vetting and risk mitigation requirements. Developers of generative AI may be subject to additional obligations, such as implementing safeguards to prevent the AI system from generating illegal content.
- Providers of AI systems designed to interact with individuals must inform individuals:
  - that they are interacting with an AI system;
  - whether the AI system generates 'deep fakes'; and
  - whether they are exposed to emotion recognition system or a biometric categorization system.

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

Before the AI Act comes into force, companies should consider:

- determining whether the AI Act will apply to them and whether they will be considered a provider of a high-risk AI system;
- identifying the obligations of the AI Act which would entail changes to their products or services and assessing how to implement such changes once the law is adopted;
- 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; and
- developing a compliance strategy and assign sufficient resources for compliance.



6. How will the AI Act be enforced?

Violations of the AI Act may result in harsh penalties. It is expected that the final version of the AI Act will provide for high fines for the most serious infringements, potentially up to the greater of €40 million or seven (7) percent of a company's global annual turnover.

The AI Act will be enforced by **national authorities** appointed by each EU country. These authorities may conduct investigations and impose fines in cases of violations.

In some countries, existing data privacy regulators will be entrusted with the task of overseeing compliance with the AI Act (for example, the CNIL in France). Other countries, like Spain, will set up new independent supervisory agencies. High-risk AI systems subject to sectorial product safety laws will be supervised by the relevant sectorial regulator. There will also be a new AI body at the EU level, whose role is still subject to negotiations. There is a growing consensus among lawmakers that enforcement against AI systems with the highest risks should be centralized at EU level.

7. Will we need to update our contracts?

Providers, users, and other parties in the AI value chain will 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. However, the AI Act will likely prohibit imposing certain unfair contractual terms on SMEs or start-ups. Companies can draw inspiration from the EU Commission's model contractual clauses for public organizations wishing to procure AI systems developed by an external supplier, which are available here.

8. Will the AI Act prohibit certain AI systems?

Yes. The EU institutions are still negotiating which AI systems should be prohibited. AI systems that manipulate or exploit individuals, or perform social scoring, will likely be banned. The use of real-time facial recognition systems by law enforcement in publicly accessible spaces will likely also be banned, subject to exceptions which are still being negotiated by the EU Institutions.

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

Companies that are subject to the AI Act and GDPR will 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 risks 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.

10. How can we stay up to date on the legislative developments?

As the final text of the AI Act is taking shape, some obligations it imposes may be expanded or restricted. Wilson Sonsini is closely following the developments in the AI global regulatory landscape and has created a group of attorneys dedicated to advising clients on AI.

For more information on the legislative history of the AI Act, please see our Fact Sheet on the draft AI Act proposed by the European Commission here, and our client alerts on the EU Council's position here and the EU Parliament's position here.

For more information, please visit: https://www.wsgr.com/en/services/industries/artificial-intelligence-and-machine-learning.html#people.

You can stay up to date on the legislative process by registering to our AI Working Group Quarterly Newsletter here.

Key Contacts

Cédric Burton
Partner, Head of European Data Regulatory Practice
cburton@wsgr.com

Laura De Boel
Partner
lde boel@wsgr.com

Yann Padova
Partner
ypadova@wsgr.com

Nikolaos Theodorakis
Of Counsel
ntheorodrakis@wsgr.com

WILSON SONSINI