PUBLICATION

ChatGPT in the Crosshairs: How the EU's AI Act May Affect Your Use of Generative AI

Authors: Vivien F. Peaden, Alexander Frank Koskey, III
July 12, 2023

The era of generative AI is here. The surge in popularity of ChatGPT has created a massive disruption as companies balance the benefit of accelerated productivity against the potential risks. The tension between innovation and regulation has also become a focal point for legislators tasked with developing governance to manage this generational change.

The European Union has been at the forefront of the global movement to regulate artificial intelligence (AI) with its proposed Artificial Intelligence Act (AI Act). If passed, the AI Act would be the world's first comprehensive regulation governing artificial intelligence. As the AI Act moves to the final stage of adoption, its proposed language provides valuable insight into the substantial compliance hurdles, which companies across all jurisdictions will face in using generative AI. The EU approach will also become the blueprint for future AI regulations across the globe, setting new requirements for data governance, transparency, and security.

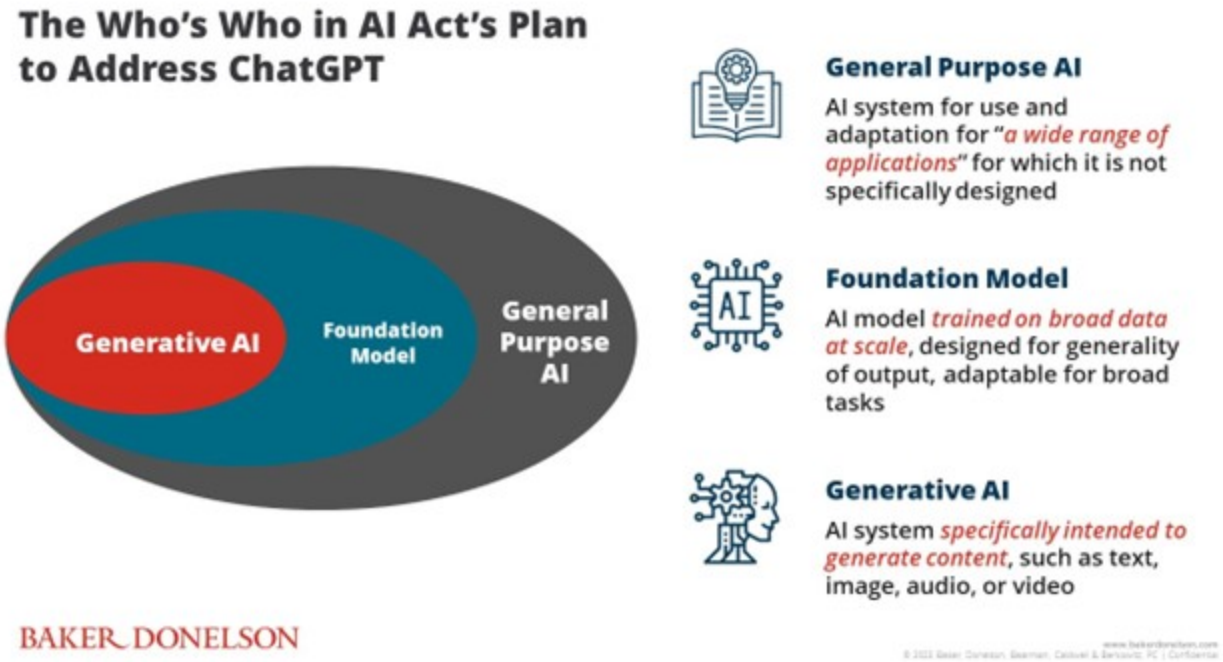
This overview discusses how the AI Act addresses the risks and harms of generative AI and what your organization can be doing now in anticipation of this groundbreaking legislation.

AI Act on Fast Track

On June 14, 2023, the European Parliament adopted its negotiation position on the draft AI Act, setting the stage for a final review among three EU decision-making bodies to adopt the final text. In a rare move, EU lawmakers are pushing to pass the final version of the AI Act by the end of 2023. Once passed, the AI Act will govern developers and users of AI systems globally, in addition to other providers that distribute and use AI systems in the EU. The long arm of the AI Act will reach even those AI systems that merely produce outputs used in the EU market. With its expansive scope, the AI Act is likely to have a more significant impact on U.S. companies than GDPR.

Future-proofing the AI Act: Generative AI is in Scope

Since its initial proposal in April 2021, the AI Act has undergone several rounds of amendments. These revisions, in part, were to address recent developments and controversies created by the launch of ChatGPT in November 2022. In response, EU lawmakers swiftly amended the proposed AI Act to address the fast advancement of generative AI by introducing three key terms: "General Purpose AI," "Foundation Model," and "generative AI," which are explained in this chart.



By unveiling these new additions, the AI Act becomes the first AI regulation to tackle risks associated with this nascent technology and represents a deliberate attempt to impose additional regulatory oversight on models that enable generative AI. Notably, the AI Act mentioned the term "**cybersecurity**" more than 30 times and "**human oversight**" more than 20 times, highlighting its commitment to promote human-centric and trustworthy AI.

A Tale of Two ChatBots: Regulating Generative AI

The establishment of the terms "Foundation Model" and "generative AI" represents a material shift from initial drafts of the AI Act. The current version of the Act classifies AI systems based on the purposes for which they were built, and acknowledges that generative AI can be used for either benign or malignant purposes: While it can create content with ease, such as images and videos, it also has the potential to deliver misinformation at scale. As the EU lawmakers succinctly put it in the proposed Recital 60(e):

"Foundation models are a recent development … [E]ach foundation model can be reused in countless downstream AI or general purpose AI systems. These models hold growing importance to many downstream applications and systems."

Foundation Models: The proposed AI Act focuses on regulating Foundation Models by imposing far-reaching obligations, including:

1. **Risk Management** as a continuous iterative process throughout the AI model's entire lifecycle to mitigate risks and improve performance. This process involves the identification and analysis of the risks most likely to occur regarding the intended purpose(s) of that AI system.

2. **Data Governance** to validate data sources and mitigate bias; in other words, a developer of Foundation Models (known as "Provider" under the AI Act) should not allow the AI system to process and use datasets that are not appropriate for AI trainings.

3. **Security and ESG-by-Design** to achieve performance and cybersecurity, and reduce energy use.

4. **Technical Documentation**, including "instructions for use" to enable downstream AI Providers to meet transparency obligations for certain high-risk use cases, including a general description of the AI system, intended purpose, and expected output, among others. The retention period for this technical documentation is 10 years after the Foundation Model is distributed or used in the EU market.

5. **Quality Management**, which ensures a robust post-market monitoring system and ongoing compliance with the AI Act.

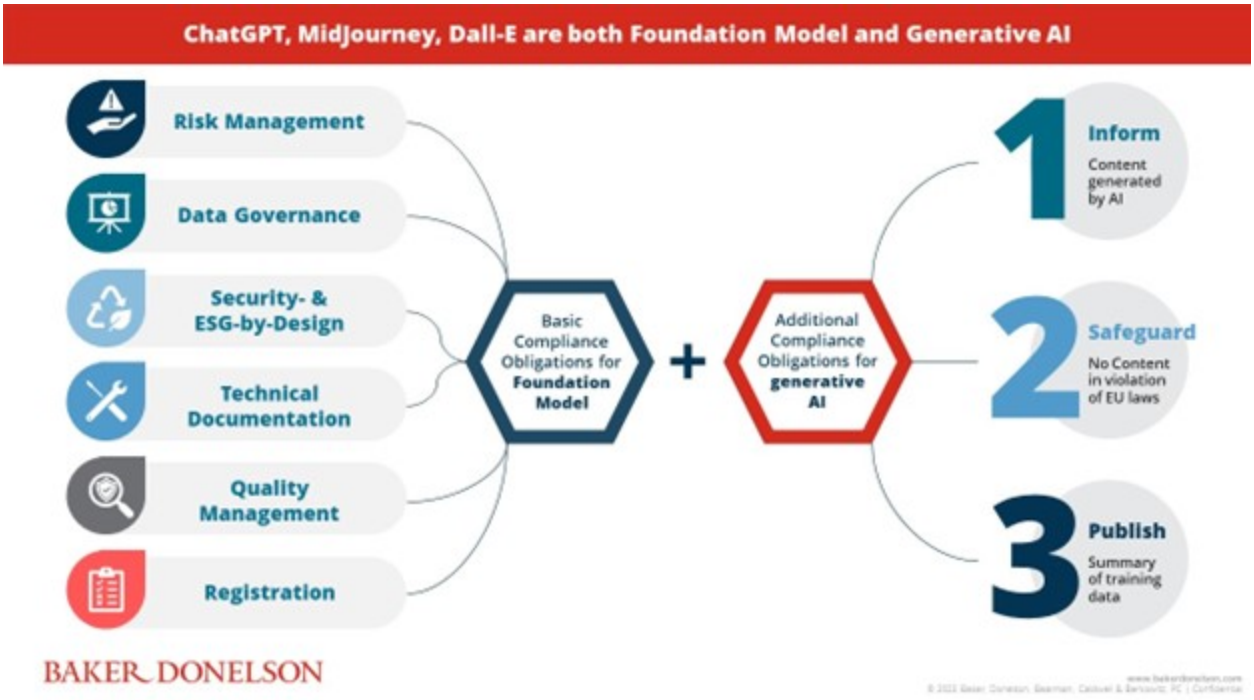
6. **Registration** in an EU database, among other obligations.

Generative AI: A Provider of generative AI must take further steps to comply with the AI Act, including:

- **Inform**: Provider must inform natural persons that they are interacting with an AI system and the content is not created by a human;

- **Safeguard**: Provider must also ensure safeguards against generation of content that breaches EU laws; and

- **Publish**: Provider will also make a summary available of its use of training data.



By setting AI governance rules specific for Foundation Models, the draft AI Act seeks to put a firm handle on the ChatGPT economy. As companies worldwide rush to integrate Foundation Models in their products and services, they should also consider adding the looming AI governance rules in their product roadmaps. These new rules apply whether ChatGPT is provided as a stand-alone model or embedded in an AI system, as a high-risk AI system or as components of a high-risk AI system, or supplied under a free and open source license or an enterprise edition.

U.S. Companies Must Be Proactive in Addressing the AI Act

The draft AI Act attempts to be forward-thinking and clearly envisions a time when ChatGPT or Midjourney become ubiquitous components in AI-powered products, just as cloud-based applications today rely on AWS and Azure. This creates a power imbalance when downstream AI providers cannot effectively mitigate the risks of an AI system without holding OpenAI or other big tech companies accountable for product performance, data governance, and information security.

As AI technologies continue to evolve, the AI Act is paving the way for a more transparent and regulated AI landscape with far-reaching global impacts. These include significant compliance hurdles for U.S. companies using AI technology in a variety of industries. With the passage of the AI Act on the horizon, U.S. companies should be proactive in addressing these potential requirements, which include the following best practices.

- **Identify Specific Use Cases**: The AI Act emphasizes setting up appropriate governance based on the purpose(s) for which AI models are used. Therefore, it is paramount for companies to define and document how these AI technologies are being used in their business operations.

- **Assess Risk Classifications for AI Technologies**: The AI Act will require organizations to classify AI solutions in risk-based categories based upon their use case(s). The current draft already identifies AI systems as "high-risk" for their applications in certain highly regulated industries, including healthcare, financial services, and HR operations. Companies should begin assessing how they might integrate AI technologies into their business operations and assigning the appropriate risk classification(s).

- **Evaluate Technologies for Transparency**: The AI Act also promotes transparency in using Foundation Models. Companies developing or incorporating certain AI models will have to provide descriptions of the training data used, validation and testing procedures used, and instructions for output interpretation and human oversight. These new requirements represent a seismic shift in disclosure requirements, and companies should begin planning and self-assessment to proactively address these issues.

Summary

We went directly to ChatGPT to ask what AI regulations should do to regulate it. The benign bot delivered a somewhat insightful answer and closed with the following:

"Remember, the goal of the AI Act is to ensure that I, ChatGPT, am here to be a delightful and reliable companion."

If you have any questions about the proposed AI Act, contact Vivien F. Peaden or Alexander F. Koskey, or any other member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.