PUBLICATION

EU AI Act Tightens Grip on High-Risk AI Systems: Five Critical Questions for U.S. Companies

Authors: Vivien F. Peaden
August 01, 2024

A new era of AI legislation has begun as the EU AI Act enters into force on August 1, 2024. With broad extraterritorial reach, significant penalties of up to seven percent of worldwide annual turnover, and an emphasis on risk-based governance, the EU AI Act will have a profound impact on U.S. businesses that develop, use, and distribute AI systems. The next 24 months will usher in a continued shift across the AI industry, during which *various AI key actors* must carefully *implement measures to mitigate risks, promote transparency and oversight, and enhance accuracy and security*. We have featured these key actors in a previous alert. Now, we turn to the top five questions that companies are asking as they navigate the AI compliance landscape:

1. What is "AI" Under the EU AI Act?

The EU defines "**AI System**" as:

"**a machine-based system** that is designed to operate **with** varying levels of **autonomy** and 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."

The scope is intentionally broad to ensure that it is technology- and industry-agnostic. There is a strong emphasis on the "**autonomy**" and "**infer**" components of this definition in order to distinguish AI from traditional software, which neither adapts nor learns independently and, thus, is not subject to the EU AI Act. The new law also governs general-purpose AI models (e.g., ChatGPT or Meta's Llama), which we will discuss in a separate client alert.

2. What are "High-Risk" AI Systems?

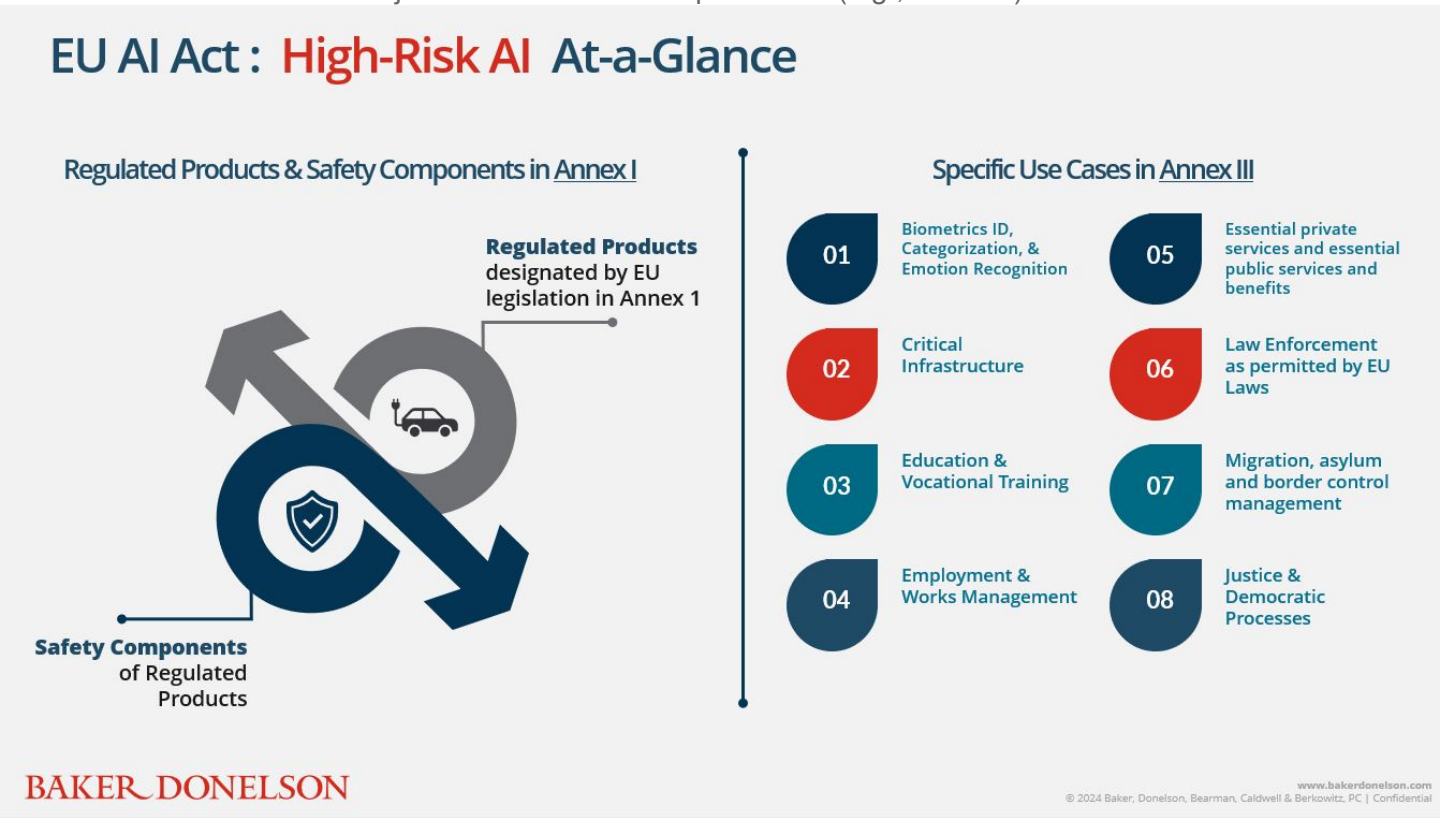
"AI Systems" under the EU AI Act are divided into four "risk-based" classifications: Prohibited AI, High-Risk AI, Limited-Risk AI, and Minimal risk, as described in this alert. The focus is clearly on "**High-Risk AI Systems,**" as referenced in more than half of the 113 Articles in the EU AI Act. *Subject to certain exceptions*, AI Systems are considered "High Risk" when they fall under one of the following two categories:

Regulated Products and related **Safety Components**: An AI System is considered "high risk" when it is either a regulated product designated by EU legislations in Annex I of the EU AI Act (Regulated Products) or a safety component used in a Regulated Product. These regulated products include medical devices, vehicles, aircraft, toys, lifts, machinery, and agricultural vehicles, among others; and

Specific Use Cases in eight specific areas outlined in Annex III to the EU AI Act:

1. Biometric remote identification, biometric categorization, or emotion recognition;
2. Critical infrastructure;
3. Education and vocational training;
4. Employment, workers management, and access to self-employment;

5. Essential private services, and essential public services and benefits;
6. Law enforcement;
7. Migration, asylum, and border control management; and
8. Administration of justice and democratic processes (e.g., election).



When the requirements for High-Risk AI Systems take effect in the next 24 months, many High-Risk AI providers will seek exemptions from the "High-Risk" AI classification. To qualify and rely upon these exemptions, these AI providers will still need to document their determinations and register their AI systems in an EU database before placing these AI systems on the EU market.

3. When Does the EU AI Act Apply to U.S. Companies Operating High-Risk AI Systems?

As outlined in this alert, the EU AI Act applies to U.S. companies across the entire AI value chain that develop, use, import, or distribute AI Systems in the EU market. Further, a U.S. company is subject to the EU AI Act where it operates AI Systems that produce output used in the EU market.

In other words, even if a U.S. company develops or uses a "High-Risk" AI System for job screening or online proctoring purposes, the EU AI Act still governs if outputs produced by such AI System are used in the EU for recruiting or admissions purposes. In another use case, if a U.S. auto OEM incorporates an AI system to support self-driving functionalities and distributes the vehicle under its own brand in the EU, such OEM is subject to the EU AI Act.

4. What are the Requirements for "High-Risk AI Systems"?

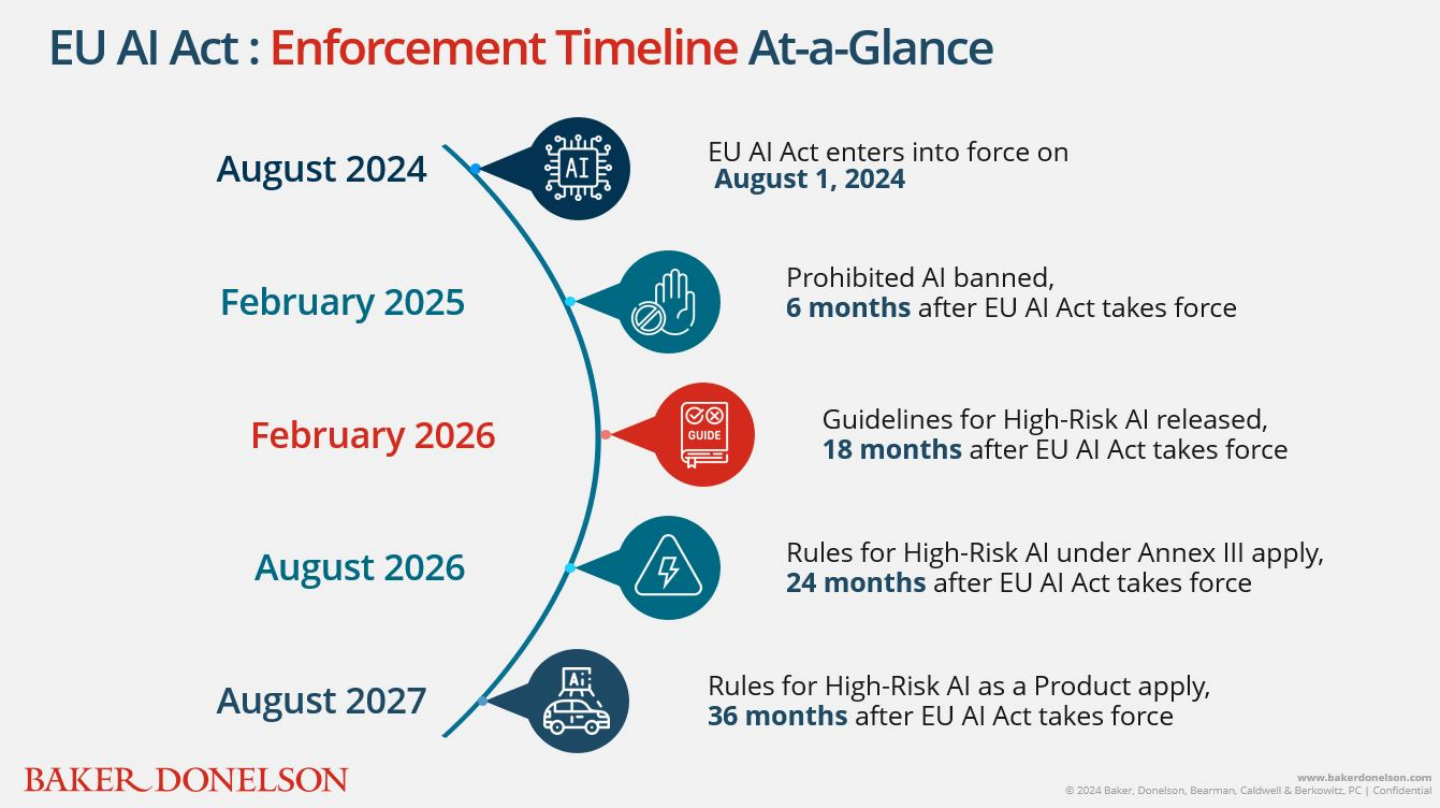
The EU AI Act lays out an extensive list of compliance obligations to promote transparency and accountability for developing or using "High-Risk" AI systems. These specific requirements are:

- **Risk management system** to identify and mitigate foreseeable risks throughout the AI lifecycle;
- **Data governance** to ensure the use and validation of high-quality data;

- **Technical Documentation** to provide descriptions of "High-Risk" AI's intended purposes, design specifications, and required human oversight;
- **Record-keeping** to keep logs of functionalities and monitor performance;
- **Transparency and Instructions for Use** to enable users to interpret outputs;
- **Human Oversight** to mitigate risks to health, safety, or fundamental rights; and
- **Accuracy, Robustness, and Cybersecurity** to ensure High-Risk AI Systems are commercially resilient against hallucination, errors, or third-party exploitations, such as data poisoning.

In addition, for those AI systems classified as "High-Risk" under the "**Specific Use Cases**" in Annex III, they must also complete a conformity assessment to certify that such AI systems comply with the EU AI Act. Where AI Systems are themselves "**Regulated Products** or related **safety components**," the EU AI Act seeks to harmonize and streamline the processes to reduce market entrance costs and timelines. Instead, the AI Providers must follow the applicable product conformity procedures prescribed under those EU legislations, which are expected to incorporate AI-related compliance requirements in the next 24 months.

5. What's Next?



The EU AI Act takes effect on August 1, 2024, with most rules for High-Risk AI Systems classified under the "Specific Use Cases" in Annex III entering into force after August 1, 2026, i.e., 24 months following the effective date. Additional compliance obligations for "High-Risk" AI Systems that are "Regulated Products or used as related safety components" are slated to apply after August 1, 2027, with a sweeping impact on a wide range of products, such as medical devices, machinery, toys, and other equipment.

Takeaways

U.S. companies that incorporate AI systems in their service offerings or business operations with global reach should stay vigilant of the evolving AI regulatory landscape and proactively ask themselves the following:

1. Do we use AI for internal operations or external-facing purposes?
2. Have we created a comprehensive inventory of AI use cases and related AI suppliers?
3. Do these use cases fall under the "High-Risk" classifications under the EU AI Act or other AI laws (e.g., the Colorado AI Act as mentioned in this Alert)?
4. Have we reviewed the data quality and permissions in advance to assess the sources, permissions, use restrictions, and recipients?

The arrival of the EU AI Act is a trend-setting moment that reshapes the way AI systems are developed, used, and regulated on a global scale. The next 24 months will be critical for U.S. companies that are deeply embedded in the global AI value chain. The EU AI Act's broad reach, extensive compliance obligations, and hefty fines highlight the need for a proactive and meticulous AI risk management program. For more information or assistance on this topic, please contact Vivien Peaden, AIGP, CIPP/US, CIPP/E, CIPM, PLS, or a member of Baker Donelson's AI Team.