Insights, News & Events

THE 7 THINGS YOU NEED TO KNOW ABOUT THE EU'S AI ACT

Insights
Dec 12, 2023

The European Union just passed the world's first comprehensive law regulating the use of artificial intelligence – which will put all the more pressure of the US to follow suit in the near future. This landmark law, finalized on December 8, could end up setting the pace when it comes to establishing a system for classifying AI usage by businesses, especially in the areas of transparency and use of AI by employers. But we could also foresee the US taking advantage of the several-year delay before the EU AI Act takes effect to create its own framework and lead the way in this area. For this reason, American companies should pay attention to the EU AI Act as it could end up creating a model that could eventually be mimicked or undercut on this side of the Atlantic. What are the seven things you need to know about the EU AI Act?

1. What is the EU AI Act?

It categorizes all AI into one of four categories in the 27 member countries that comprise the EU:

- Prohibited
- High Risk
- Limited Risk
- Minimal Risk

Obviously the types of AI included on the "prohibited" list will be banned and cannot be developed or used. Those classified as "high risk" will now carry with them extensive

Related People

Nan Sato, CIPP/E, CIPP/C
Partner
610.230.2148

David J. Walton, AIGP, CIPP/US
Partner
610.230.6105

requirements for developers and users, including broad disclosure and rigorous testing requirements.

Some AI is exempted from the law's reach. That includes AI used for national security, military, and defense purposes. For the public's purposes, it also includes some open source AI – those AI systems developed using code that is publicly available to developers so that they can integrate them into their own products and services (such as using ChatGPT services for a company's purposes).

2. What AI is prohibited under the EU AI Act?

The following AI uses, among others, will be prohibited:

- Social credit scoring systems
- Emotional recognition systems at work (and in schools)
- Untargeted scraping of facial images for recognition systems
- Biometric categorization systems using "sensitive" characteristics
- Certain kinds of predictive policing applications
- Behavioral manipulation and circumvention of free will
- AI used to exploit people's vulnerabilities (such as older individuals or those with disabilities)

3. What is "High Risk AI" and what do you need to do with it?

AI used in the following situations, among others, are classified as high-risk:

- Recruitment, human resources, and worker management
- Use in vehicles
- Medical devices or situations
- Access to certain services such as insurance, benefits, banking, and credit
- Education and vocational training
- Emotion recognition systems

Service Focus

AI, Data, and Analytics

Government Relations

International

Resource Hubs

AI Governance Hub

- Biometric identification systems
- Administration of justice

Any high-risk AI needs to registered in a public EU database. Organizations must then follow through with the following requirements:

- Complete a "fundamental rights impact" assessment
- Complete a "conformity" assessment
- Comply with data governance rules related to bias mitigation, representative training data, and more
- Implement risk management system
- Provide a specific transparency overview including instructions for use, technical documentation, and more
- Deliver comprehensive human oversight that includes explainability, auditable logs, humans-in-the-loop, and more
- Implement quality management system
- Ensure accuracy, robustness, and cybersecurity for data through testing and monitoring

4. What requirements exist for General Purpose AI?

There are a few key requirements for General Purpose AI. Organizations must be transparent when they use such AI and provide information such as technical documentation, training data summaries, copyright information, IP safeguards, and more. If the AI will be operating in an area with high-impact and systemic risk, they must also provide model evaluations, risk assessments, adversarial testing, incident reporting mechanisms, and more.

Generative AI (GenAI) has its own separate requirements. Organizations must inform those who are interacting GenAI (such as with chatbots) that they are actually communicating with an AI system. Also, organizations must label GenAI-developed content – such as deepfakes – as such and ensure they are readily detectible.

5. What are the penalties and enforcement mechanisms?

Those organizations that commit violations related to prohibited AI could see fines of up to 7% their annual global turnover or $35m. Most other violations could lead to fines up to 3% or $15m. Supplying incorrect information could see fines up to 1.5% or $7.5m.

Small-and-medium-sized entities, along with start-up businesses, will be spared the heaviest hits thanks to caps on total fines.

We expect to see a plentiful market when it comes to fines because any individual can make complaints about non-compliance. Meanwhile, we will see an AI Office and an AI Board created at the EU level, and market surveillance authorities in each country will enforce the AI Act.

6. When does the EU AI Act take effect?

The next step is for the European Parliament to formally pass the legislation. This is merely considered a formality at this point, so we expect this to happen quite soon – well before the next round of EU elections in May 2024. Once passed, there will be compliance grace periods of between six and 24 months depending on the individual requirements, meaning the EU AI Act will not take hold until 2025 and won't be fully effective until 2026. This delay could create a vacuum that the US could attempt to take advantage of.

7. What should employers do?

Employers operating in the EU should immediately conduct an AI audit to determine the full scope of your AI usage. Make sure you bring aboard your IT and departmental leaders to ensure the AI audit is comprehensive. Once your audit is complete, you will need to develop an implementation plan to ensure you introduce compliance steps well before the deadlines. You will also need to establish new internal compliance protocols to ensure your organization doesn't run afoul of the new rules as you grow and adapt your services.

American companies shouldn't ignore the EU AI Act, however, even if you don't operate overseas. There stands a good chance that this new law could become the global standard when it comes to classifying AI risk and impose transparency requirements, at the very least. Or it could spur federal lawmakers to accelerate their work (led by Senate

forums such as the one held a few months ago) to create an American version that provides greater room for innovation.

While an American regulatory scheme might not mirror the EU AI Act in every respect – and in fact there is reason to believe that any federal legislation would not be as broad or as onerous as the European model – the EU AI Act does provide a solid framework for examining the AI that you deploy and how you might start to classify and oversee its usage.

We suggest American organizations start with the NIST framework – the same simple but effective AI compliance roadmap suggested by Representative Ted Lieu at the recent FP AI Strategies @ Work Conference. You can follow 10 critical steps to follow the roadmap developed by a well-accepted federal agency by clicking here.

Conclusion

If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Artificial Intelligence Practice Group or on our International Practice Group. Make sure you subscribe to Fisher Phillips' Insight System to gather the most up-to-date information on AI and the workplace.