POLSINELLI® | What a law firm should be.™

The European Union Has Assigned Your AI Some Homework

Seeking to build on the success and influence of GDPR, the European Union has spent the last seven years constructing a comprehensive regulatory scheme for artificial intelligence: The Artificial Intelligence Act (**AI Act**).

Now that the AI Act has been formally adopted by the European Parliament, following a last-minute compromise on "General Purpose Artificial Intelligence" (GPAI), businesses need to begin assessing the AI tools that they offer to others and the ones they use themselves, in order to prepare a compliance strategy. Given the extra-territorial reach of the AI Act, even U.S.-centered businesses may need to launch compliance strategies.

The AI Act's complex framework incorporates several other sector-specific regulatory regimes and covers a very broad range of products and services: financial credit, toys, medical devices, aircraft and even forestry and marine vehicles. GDPR and GDPR principles are heavily relied upon throughout the AI Act. Indeed, a core objective of the AI Act is to protect "Fundamental Rights," which (among other things) includes the protection of privacy through consistency with GDPR.

This will be the first in a series of client advisory articles we will publish as we begin unpacking the EU's AI Act to help clients evaluate if, when, and how they need to comply with its requirements.

How does the AI Act define Artificial Intelligence?

Broadly. According to the Act, an Artificial Intelligence system is a "machine-based system…that may exhibit adaptiveness after deployment and that…infers from the input it receives, how to generate output as predictions, content, recommendations, or decisions that can influence physical or virtual environments." Article 3(1). This definition has an incredibly wide reach, as it essentially covers any algorithm that evolves in response to the input it receives. This captures more than just the chatbots and image generators currently in the limelight—it includes many low level and background AIs we have been using now for years: adaptive cruise control, algorithmic suggestions in social media and entertainment, Roombas, pacemakers, noise canceling headsets, firewalls and almost every service or item that we once called "smart."

Who does the AI Act apply to?

The AI Act's broad extra-territorial impact will catch many unsuspecting U.S. players by surprise unless they begin to prepare now. Here are five illustrative scenarios where the EU AI Act will apply to U.S. entities and their products and services:

- A U.S.-based creator of customized AI powered cyber-security tools for clients in the EU. Article 2(1a).
- A U.S.-based manufacturer of sonogram machines that relies on AI to create 4D images, developed in the U.S. and sold in the EU. Article 2(1cb).
- A U.S.-based financial firm that created a risk analysis model using AI and then uses that model to guide securities trades in the EU. Article 2(1c).
- A U.S.-based car manufacturer that incorporates an AI-based collision detection system that's included in cars sold in the EU. Article 2(1c).
- A U.S.-based remote proctoring service, available worldwide through a web portal, that allows for the proctoring of educational, professional exams (and even medical tests) that utilizes AI facial recognition technology to confirm subject identities. Articles 2(1a), 2(1c), and 2(1cb).

Again, the AI Act expressly covers both "providers" and "deployers" of AI systems even if they are located in a third country if the *output produced by the system* is used in the Union. Article 2(1c). "Providers" are anyone who develops an AI system or GPAI and places them on the market or puts them into service under its own name. Article 3(3). "Deployers" essentially means users: anyone that uses an AI system, except for non-professional activities. Importers, Distributors, Product Manufacturers, and Authorized Representatives also have responsibilities under the Act.

What type of AI does the AI Act apply to?

All AI systems, including general-purpose AI (GPAI). The EU defines GPAI as an "AI model…that is capable of competently performing a wide range of distinct tasks." Article 3(63). The AI Act regulates GPAI by what it is; but it also regulates AI, general or otherwise, by what it does. Limited categories of use cases are outright prohibited or prohibited except in special circumstances. For example, an AI system that uses "real-time" biometric identification systems for law enforcement is (with some exceptions) banned, as are AI systems that engage in racial profiling or use subliminal techniques. Article 5(1). Other systems are subject to specific "transparency obligations," such as GPAI or media generating AIs that create synthetic images, audio or video. Article 50. At the other end of the spectrum are AI systems that are largely unregulated – for example, an AI that competes against humans in a video game.

In the middle, however, are so-called "high risk" systems and, despite the name, a vast swathe of AI tools falls in this "high risk" category. Annex III classifies biometric applications, management of critical infrastructure, education and training, HR and employment, "access to essential services" (which includes benefits, creditworthiness and even the dispatch of emergency services), and legal system applications as "high risk." Article 6(2), Annex III. In addition, AI tools included in machinery, toys, vehicles of every description, elevators, radio equipment and medical devices are all considered "high risk." Article 6(1b), Annex I. Finally, any product where the AI tool acts as a safety component is considered high risk. Article 6(1a), Annex I.

What do I have to do?

If your AI use cases fall into the high-risk category, the EU may require extensive documentation, planning, testing, and monitoring of the AI systems in question:

- **Risk Management Systems** – the EU considers this to be an iterative process planned and run throughout the life cycle of a high-risk system that requires regular review and updating. It must account for the risks involved in both the AI system's intended purpose and reasonably foreseeable misuse, as well as any emerging risks post-deployment. Article 9.
- **Data and Data Governance** – here, the EU is referring to the use of appropriate training, validation and testing data sets that meet their quality criteria. Article 10.
- **Technical Documentation** – these are generally required *prior* to putting the AI system into the market and kept up-to-date on an ongoing basis. This technical documentation will ensure regulatory authorities have all the information necessary, in a clear and comprehensive format, to verify that the AI system meets the relevant requirements. Article 11. Also included in these documents are instructions for use that deployers can then use to properly operate the AI system, per any use restrictions, human oversight and monitoring requirements established by the provider. Articles 16 and 26.
- **Record Keeping** – high-risk systems must allow for automatic and traceable event logging over the lifetime of the system. Article 12.
- Transparency/Instructions – high-risk systems must enable deployers to interpret the output and use it appropriately. This includes providing instructions, as well as explanations regarding system purpose, limits, accuracy, and foreseeable risks. Article 13.
- **Human Oversight** – high-risk systems must be capable of human oversight commensurate with the risks associated with the system and its level of autonomy. It must enable human oversight capable of intervening to countermand AI actions, disregard, or reverse the results, when necessary. Article 14.
- **Accuracy, Robustness and Cybersecurity** – the accuracy of the system must be part of the instructions, and the system must be resilient against not only third-party attacks but against errors and inconsistencies in uses. This may require technical redundancies, backups and fail safes. Article 15.
- **Quality Management and Conformity Assessments** – high-risk and GPAI systems must maintain a quality management system to ensure compliance with the AI Act and complete a corresponding conformity assessment. The quality management system should consist of written policies, procedures, and instructions that will drive compliance in a systematic and orderly manner (Article 17), whereas the conformity assessment must formally document and demonstrate regulatory compliance prior to putting the AI system on the market or in service (Article 43).

If you are a "provider" of AI systems and are covered by the AI Act, there are additional requirements. Providers must submit contact information, establish and maintain a quality management plan (Article 17), keep additional documentation (Article 18), store the automatic logs (Article 19), ensure that "conformity assessments" are complete prior to placing the system on market (Article 43), register the system (Article 49), and take corrective actions where necessary (Article 20). If, as a provider, you are outside of the EU, you must designate an authorized representative to perform these functions on your behalf. Article 22.

However, *even "deployers"* of AI systems (anyone who uses an AI system except for personal, non-professional activities) are subject to some requirements. For example, deployers using high-risk systems must follow the instructions (Article 26(1)); ensure users have necessary competence, training and support (Article 26(2)); use input data that is "relevant and sufficiently representative" (Article 26(4)); keep logs for at least six months (Article 26(6)); and may have to notify employees subject to the use of the system that a "high-risk system" is involved (Article 26(7)). If as a deployer, you are involved in the provision of public services (e.g., education), you must also conduct a "Fundamental Rights Impact Assessment." Article 27.

When is Your Homework Due?

Thankfully, there is a grace period and some time-limited exemption of systems that were already on the market prior to the passage of the AI Act. Assuming the final language of the AI Act is approved and published this month, the full weight of the AI Act goes into effect in April 2026 (24 months from publication). However, there are certain provisions that would go into effect as soon as April 2025, including some obligations for providers of GPAI systems. Prohibited AI practices would be banned within six months, with enforcement of those bans beginning in the fall of 2024.

What if You Do Not Complete Your Homework on Time or It's Not Correct?

If you use a prohibited AI system, you can be subject to a fine of 35,000,000 EUR or up to 7% of your total worldwide annual turnover (essentially revenue) for the preceding year, whichever is higher. Article 99(3). Failure to comply with other obligations and requirements, such as Article 16, 22-27, and Article 50 will result in 15,000,000 EUR or 3% turnover fines, whichever is greater. Article 99(4). Finally, providing incorrect or misleading information will result in 7,500,000 EUR or 1% turnover fines, whichever is greater. Article 99(5). Although small enterprises like startups may receive special consideration during fee calculations so they receive whichever fine is lower. Article 99(1,6).

Stay tuned for our next update: *"Do I Really Have to?" How to Determine if the EU AI Act Applies to You*