Artificial Intelligence: EU Regulation, Global Impact

On April 21, the European Commission announced its landmark proposal for regulating artificial intelligence. The proposed rules represent an attempt to establish global standards for artificial intelligence (AI) like the EU's General Data Protection Regulation (GDPR) enacted in 2018, and to provide a robust and flexible legal framework for trustworthy AI that is innovation-friendly and human-centered.

The EU's proposed regulation takes a proportionate and risk-based approach: the higher the risk posed by the AI, the stricter the rules governing its use, and greater the burden placed on those operators of the AI. It applies to any company or government agency that develops or uses the broadly-defined AI technology that potentially affects an EU citizen, including importers and distributors, and is expected to have a strong economic impact on many companies. Companies that violate the rules would face heavy fines.

KEY TAKEAWAYS

- **"AI" is defined broadly** to include nearly any software or firmware using machine learning, logic- and knowledge-based approaches, (e.g., knowledge bases, inference/deductive engines, expert systems), statistical approaches, and search and optimization methods.
- **Risk-based approach** categorizes AI applications according to the risk they pose to health, safety or fundamental rights. The risk analysis considers the intended purpose of the AI system, functions performed, and modalities for which the system is used, and classifies AI systems according to 4 risk levels: minimal risks, limited risks, high risks and unacceptable risks.
- **Minimal-risk AI applications do not face new restrictions beyond existing consumer protection laws.** Examples of minimal risk AIs include applications such as email spam filters and systems to optimize the use of resources in a factory.
- **Limited-risk AIs are allowed, but subject to transparency obligations** to ensure that users understand they are interacting with an AI. Examples of limited-risk AIs include chatbots and deepfake technology.
- **High-risk AIs are subject to strict requirements.** AI systems are considered high risk that significantly impact aspects of human life. This includes medical devices, software for autonomous vehicles, and AI systems that are safety components of regulated products or themselves a regulated product; real-time and post, remote biometric identification systems, including facial recognition; and applications for critical infrastructure, education, employment, access to essential and public services including emergency response services, law enforcement, border control, and the administration of justice including AI-based legal software.

  High-risk AIs are subject to strict requirements including specified data governance practices and the use of high-quality data that is relevant, representative, free of errors, and complete in view of the intended purpose of the AI; disclosure and transparency including detailed documentation about how the AI system works and instructions of use; human oversight in design and implementation; implementing a risk management system and post-market monitoring; maintaining accuracy; and cybersecurity. These systems also may be subjected to a regulatory sandbox that facilitates testing, validation, and compliance before their placement into the market.

- **AIs posing unacceptable risks to security and fundamental rights are prohibited.** These include technologies that have significant potential to manipulate behavior or exploit vulnerable groups and AI-based social scoring by public authorities. The use of real-time, facial recognition and other remote biometric identification systems by law enforcement on populations of people in public spaces is also prohibited, except in limited and judicially approved situations for identifying victims of a crime and missing children, identifying serious criminals, and threats to public safety or terrorism.
- **Steep penalties imposed for noncompliance.** Companies that violate the prohibition of AI systems or the data and data governance requirements would face fines of up to 30 million EUR or 6% of worldwide turnover, whichever is greater. Noncompliance with other rules would subject a company to fines of up to 20 million EUR or 4% of worldwide turnover, whichever is greater.
- **Disclosure and testing requirements for high-risk AIs may necessitate rethinking approach to protecting intellectual property (IP).** For instance, IP protection strategies that previously relied on trade secret protection for backend aspects of AI systems may shift towards a patenting strategy. Additionally, as training data sets are subjected to inspection and reporting, companies will need to ensure appropriate mechanisms are in place to preserve their trade secrets on proprietary data.

WHAT'S NEXT

As the EU's recent actions have exhibited, governments are starting to pay attention to and are taking steps to regulate AI. In the global economy, it is vital that companies engage experienced counsel with knowledge of their specific AI and digital technologies to help navigate the changing regulatory landscape. Knowledgeable counsel can provide comprehensive guidance that not only avoids regulatory landmines, but also considers the company's position and business objectives to leverage digital technologies effectively.

CONTACT

James Devaney

Partner | Kansas City
jdevaney@shb.com
816.559.2677/direct dial