protiviti®
Global Business Consulting

EU Lawmakers Reach Agreement on AI Act, Creating Regulatory Framework Addressing Risks of AI

December 13, 2023

On December 8th, after two and a half years of negotiation, the Council of the EU and the EU Parliament finally reached a provisional agreement on the EU AI Act, which was first proposed by the European Commission in 2021. The agreement creates legislation that introduces harmonized rules and definitions for those using artificial intelligence (AI) systems and putting those systems into service and bans certain types of AI practices.

The AI Act is the first comprehensive law in the world that also impacts general-purpose AI systems and includes safeguards and prohibitions that will reduce the risk presented by AI for government agencies, businesses and individuals. It will enter into force gradually.

- The prohibitions on specified categories of banned AI will apply after six months.
- The requirements for high-risk AI, governance and conformity will apply after 12 months.
- All other provisions will apply after two years.

Organizations should act quickly to identify if their AI capabilities fall into any of the banned categories and develop a plan to resolve any issues before the six-month window closes.

Without question, the AI Act represents a game-changer for organizations operating in the EU and could have a broader impact than many realize due to its extraterritoriality implications. What's more, the AI act may be the first salvo in a lengthy political and regulatory campaign to rein in the power of AI and protect consumers and data.

Summary of the AI Act

The AI Act regulates areas where using AI poses the most significant risk to fundamental rights, such as health care, education, border surveillance and public services. AI systems deemed "high-risk" – such as those related to critical infrastructure, education access assessment, law enforcement or biometric identification – are subjected to stricter requirements. The AI Act requires detailed documentation, higher quality data governance and management, human oversight, and risk-mitigation systems.

Currently, many AI systems fit within the "minimal or no risk" category, which is the classification used for spam filters, for example. Participation in AI codes of conduct for providers of such services will be voluntary for those that fit into the “minimal or no risk” category.

In addition, the new legislation calls for prohibiting certain applications of AI that create a potential threat to citizens’ rights and democracy; the co-legislators agreed to prohibit the use of:

- Biometric categorization systems that use sensitive characteristics (e.g., political, religious, philosophical beliefs, sexual orientation, race)
- Untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases
- Emotion recognition in the workplace and educational institutions
- Social scoring based on social behavior or personal characteristics
- AI systems that manipulate human behavior to circumvent their free will
- AI used to exploit the vulnerabilities of people (due to their age, disability, social or economic situation)

Failure to comply with the rules can lead to fines ranging from 35 million euros or 7% of global turnover to 7.5 million euros or 1.5 % of turnover, depending on the infringement and size of the company.

Potential benefits

Implementing the requirements of the AI Act is intended to develop benefits for EU member nations, businesses, individuals and other entities, for example:

- **Protection of individuals’ fundamental rights**: The AI Act protects the fundamental rights of individuals from AI-related risks, such as privacy concerns, data extraction, discrimination and bias.
- **Enabling responsible innovation**: Innovation is supported by regulatory sandboxes allowing the AI community to experiment with new and cutting-edge technologies without the fear of immediate regulatory consequences.

- **Risk-based approach**: The AI Act introduces the concept of a risk-based approach shifting the focus to risk avoidance as the primary motivator.
- **Market harmonization**: The AI Act promotes consistency for developing a single market for AI that brings forth trustworthy and responsible AI as a competitive advantage.
- **Alignment in governance and oversight**: A European Artificial Intelligence Board will be established to ensure consistent application of the regulation across the EU.
- **Supervisory authorities**: National supervisory authorities will be designated in each member state.
- **Transparency and explainability**:
  - AI systems that interact with humans or generate or manipulate image, audio or video content must disclose that they are AI-generated. This includes chatbots and deepfake technologies. Users must be clearly informed when they are interacting with an AI system.
  - Explainability becomes a binding principle in the AI lifecycle to understand and interpret the decisions and predictions made by AI systems to build trust, ensure fairness and enable easier adoption.

Potential challenges

Although the proposed framework includes much-needed guidance, organizations will still be faced with challenges that will complicate implementation, for example:

- **Transparency requirements**: Questions remain concerning how to create appropriate technical documentation, comply with EU copyright law and disseminate detailed summaries about the content used for training.
- **Generative AI**: Organizations will need to determine how to identify copyright infringement and violations as well as how responsibilities are split between providers and users of such systems.
- **Non-compliance and penalties**: Organizations need to understand the potential for fines and reputational damage that can be posed by violations or misinterpretation of requirements.

- **Labeling**: Organizations must incorporate labels for deepfakes, chatbot interactions and AI-generated content (must be identified and revealed to users).
- **Compliance costs**: Organizations might face increased costs and complexity in ensuring compliance with the EU AI Act, especially if their AI systems fall under the high-risk category. This involves adapting AI systems to meet the stringent requirements for data governance, transparency and human oversight set out in the Act.
- **Operational adjustments**: Companies may need to make significant adjustments to their AI systems, especially in terms of data governance and transparency. This could mean re-engineering AI models, altering data collection and management processes, and implementing new oversight mechanisms.
- **Data privacy and cross-border data flows**: The Act's alignment with GDPR means organizations must ensure strict data privacy measures are in place, complicating data management and potentially impacting cross-border data flows.
- **Management and maintenance of AI programs**: Organizations will need to build overarching and multidisciplinary programs to ensure the ongoing management of responsible and trustworthy AI initiatives.
- **Potential disgorgement of existing models**: Organizations should be aware of the fact that the existing AI models in place can be deleted or revoked due to the non-compliant practices violating the AI Act's requirements.

One of the biggest challenges may come in the form of the "unknown" – driven by "additional binding obligations" that will be "operationalized through codes of practices developed by industry, the scientific community, civil society, and other stakeholders together with the [European] Commission."

What businesses can do to prepare for the AI Act

Due to the complexity and the variety of the obligations prescribed by the EU AI Act, affected businesses are advised to start preparing now for the profound impact the legislation is bound to have. Following are some suggested steps organizations should take, though this list should not be viewed as exhaustive:

Business context

- Form a uniform understanding of the term "AI" within the organization.
- Educate staff on the potentials and risks associated with AI.
- Determine whether the organization is contemplating or already deploying AI.
- Identify jurisdictional scope of your AI initiatives.
- Identify the potential roles of your organization in AI (user, developer or deployer) governance.
- Identify the teams/business units/regions dealing with, developing and monitoring AI.
- Formalize a steering committee composed of a cross section/region of stakeholders.
- Ensure regional ownership and accountability for enforcement.
- Ensure management level/C-suite sponsorship.

Operations

- Review and identify the existing data and information lifecycle management capabilities of the organization.
- Identify the third-party ecosystem in relation to AI initiatives.
- Identify the existing technical measures for security, privacy, data quality, robustness and bias management.

Compliance and risk management

- Identify already existing related risk assessments (e.g., data protection impact assessments, information security assessments, third party due diligence).
- Identify current/potentially applicable use cases and preliminary risk classification.
- Centralize the inventory for the AI ecosystem including models, algorithms and components (similar to records of processing).
- Identify the responsible parties for leading the communication and interaction with related EU regulatory bodies.

- Identify how AI strategy and initiatives come together with the existing risk management and data strategy.
- Start building an AI-specific risk management program.
- Incorporate the financial risks and monetary fines into your overall compliance risks.

In closing

The EU AI Act paves the way for more legislation impacting AI, and other nations, organizations and groups are sure to follow with additional legislation. AI, by its self-evolving nature, has been on the radar of governments and policymakers. The United States is taking some initial steps in this regard with the Biden administration's first executive order on AI, which directs various U.S. government agencies to identify the risks of the technology as well as harness the benefits.

The first international agreement was signed in Bletchley in November between 28 countries, including the United States, China, EU and UK, to mark the collaborative commitment to ensure the responsible development of AI. And now, the EU delivered its final Act to enforce the first multi-regional binding law.

The EU AI Act marks a significant step toward a regulated AI landscape, impacting all organizations and stakeholders "placing on the market or putting into service AI systems in the [European] Union, irrespective of whether those providers are established within the Union or in a third country" (Article 2/a). The scope of the Act is wide enough to cover the parties located in the third country "where the output produced by the system is used in the Union" (Article 2/c). For this reason, the Act's implications ripple beyond the EU. All organizations face a complex compliance landscape, necessitating adjustments in AI operations and strategies to meet the EU standards. This situation underscores the need for a global perspective on AI governance, as the Act could potentially harmonize or diverge AI regulations across different regions.

Overall, the EU AI Act is not just a regional regulation but a catalyst for global AI policy evolution. It prompts organizations worldwide to prioritize ethical AI practices, adapt to evolving regulatory landscapes, and contribute to a global dialogue on responsible AI development and use. This global perspective is essential for fostering innovation that respects fundamental rights and ethical principles in AI applications.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2023 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®