COSMOS
Navigate the Compliance Universe

CEP Magazine - May 2024

Ahmed Salim (asalim19@gmail.com) is a Chief Compliance Officer in Chicago, Illinois, USA.

Adrian Taylor (ataylor@premierhealth.com) is the Director of Diversity at Premier Health Partners in Dayton, Ohio, USA.

Nakis Urfi (linkedin.com/in/nurfi/) is Senior Manager, Provider Relations & Regulatory Compliance at Abbott based in Dallas, Texas, USA.

The EU AI Act: A comprehensive guide for organizations

By Ahmed Salim, Adrian Taylor, and Nakis Urfi

The EU recently introduced the AI Act, landmark legislation aimed at regulating artificial intelligence (AI) technologies. This article provides an in-depth overview of the EU AI Act, its implications for organizations, and detailed guidance on how compliance professionals can prepare and build programs around its requirements.[1] Additionally, we will explore how organizations can effectively prepare for the implementation of the AI Act.

Summary of the EU AI Act

The EU AI Act is a comprehensive regulatory framework designed to ensure the ethical and responsible development, deployment, and use of AI technologies within the EU. It covers a wide range of AI systems, including both high-risk and non-high-risk applications. The act aims to strike a balance between fostering innovation and protecting fundamental rights, such as privacy, nondiscrimination, and transparency.[2]

Implications for organizations

The EU AI Act has significant implications for organizations operating within the EU or providing AI technologies to EU markets. Compliance with the act will be mandatory, and noncompliance may result in substantial fines and reputational damage. Organizations must carefully assess their AI systems to determine whether they fall under the act's high-risk category and take appropriate measures to ensure compliance.

Preparing compliance professionals

Compliance professionals play a crucial role in helping organizations navigate the complexities of the EU AI Act. To prepare for this new regulatory landscape, compliance professionals should do the following.

Understand the act

Compliance professionals must thoroughly familiarize themselves with the provisions, requirements, and obligations outlined in the EU AI Act. This includes studying the act's definitions, risk assessment criteria, and

compliance procedures. They should also stay updated on any guidance or clarifications provided by regulatory authorities. The act applies to organizations outside the EU, so multinational companies should actively participate in industry forums, attend relevant conferences, and engage with regulatory bodies to gain insights and share best practices.

Conduct risk assessments

Compliance professionals should work closely with relevant stakeholders—including AI developers, data scientists, and legal teams—to identify and assess AI systems based on risk. Compliance professionals should ensure that the company's AI is not a prohibited AI risk use case and identify whether their AI falls under the act's extensive requirements for providers and users in the high-risk AI category. High-risk AI includes medical devices, vehicles, job recruitment, influencing elections, access to services such as insurance and benefits, critical infrastructures, biometric identification, and law enforcement. This involves evaluating potential risks related to safety, fundamental rights, and legal compliance. Risk assessments should consider factors such as the system's intended purpose, its potential impact on individuals and society, and its autonomy level. Compliance professionals should document the risk assessment process, including the identified risks, mitigating measures, and ongoing monitoring plans.

Develop compliance programs

Compliance professionals should develop comprehensive compliance programs tailored to their organization's specific AI systems. These programs should include policies, procedures, and controls to ensure adherence to the act's requirements. Compliance programs should address areas such as data protection, transparency, accountability, human oversight, and algorithmic bias mitigation. They should also establish mechanisms for ongoing monitoring, reporting, and auditing of AI systems, including using secure software development lifecycles. Compliance professionals should collaborate with technology teams to ensure compliance programs align with existing data protection and cybersecurity frameworks. High-risk AI systems have additional requirements, including impact assessments, registration in the public EU database, implementation of quality management system, certain levels of data governance, transparency with technical documentation and instructions for use, and human oversight.

Collaborate with stakeholders

Compliance professionals should collaborate with various stakeholders within the organization, including technology, legal, and data protection teams, to ensure a holistic approach to compliance. They should actively engage with AI developers and data scientists to understand the technical aspects of AI systems and identify potential compliance challenges. Collaboration with external experts and industry associations can also provide valuable insights and best practices. Compliance professionals should establish clear communication channels to facilitate information exchange and ensure that compliance requirements are integrated into the organization's AI development lifecycle.

Preparing organizations for implementation

To effectively prepare for the implementation of the EU AI Act, organizations should consider the following steps.

Assess current AI systems

Organizations must conduct a thorough assessment of their existing AI systems to determine their risk level and compliance obligations under the act. This assessment should include an AI inventory of where AI is used in the

organization, data collection, processing, and decision-making processes. It should also consider the potential impact on individuals' rights, safety, and well-being.[3] Organizations should document the results of these assessments and identify any necessary remedial actions. Compliance professionals should collaborate with AI developers and data scientists to ensure the assessment process is comprehensive and accurate. If organizations are using generative AI, individuals must be informed when interacting with AI, and the AI content must be labeled and detectable.[4]

Implement ethical guidelines

Organizations should establish clear ethical guidelines for developing and using AI technologies. These guidelines should align with the act's transparency, fairness, and accountability principles. They should address issues such as explainability, fairness in decision-making, and the prevention of AI systems being used for harmful purposes. Ethical guidelines should be communicated to all relevant stakeholders and integrated into the organization's AI development processes. Compliance professionals should work with senior management to ensure ethical guidelines are effectively implemented and enforced.

Enhance data governance

Organizations must strengthen their data governance practices to comply with the act's data protection, privacy, and security requirements. This may involve implementing robust data management systems, conducting data protection impact assessments, and establishing mechanisms for obtaining informed consent.[5] Organizations should also consider adopting privacy-enhancing technologies and implementing privacy-by-design principles to minimize risks associated with AI systems. Compliance professionals should collaborate with data protection officers and technology teams to develop and implement data governance frameworks that align with the act's requirements.

Train employees

Organizations should provide comprehensive training programs to educate employees about the EU AI Act, its implications, and their roles in ensuring compliance. Training should cover topics such as the ethical use of AI, data protection, bias mitigation, and the importance of human oversight. It should be tailored to different roles within the organization, including AI developers, data scientists, compliance professionals, and senior management. Regular training updates should be provided to keep employees informed about any changes or updates to the act. Compliance professionals should collaborate with human resource departments to develop training materials and ensure that training programs are effectively delivered.

Conclusion

The EU AI Act represents a significant step toward regulating AI technologies within the EU. The penalties and enforcement can be severe once the act is in effect, where organizations could pay fines up to 35 million euros or 7% of global annual turnover for prohibited AI violations.[6] Organizations must understand its provisions, assess their AI systems, and develop robust compliance programs to ensure adherence. Compliance professionals play a vital role in guiding organizations through this process; however, organizations themselves must also proactively prepare for the act's implementation by assessing their systems, implementing ethical guidelines, enhancing data governance, and training employees. By embracing the EU AI Act, organizations can demonstrate their commitment to responsible AI development and contribute to a trustworthy and ethical AI ecosystem. Compliance professionals should continuously monitor regulatory developments and adapt compliance programs accordingly to ensure ongoing compliance with the evolving requirements of the EU AI Act.

Takeaways

- The EU recently introduced the AI Act, landmark legislation aimed at regulating artificial intelligence (AI) technologies.
- Compliance professionals play a crucial role in helping organizations navigate the complexities of the EU AI Act and should prepare for this new regulatory landscape.
- The EU AI Act has significant implications for organizations operating in or providing AI technologies to EU markets.
- Compliance professionals should understand the act thoroughly, conduct risk assessments, develop compliance programs tailored to their organization's AI systems, and collaborate with various stakeholders within and outside the organization.
- Compliance professionals play a vital role in guiding organizations through this process. Ongoing monitoring of regulatory developments is essential to adapt compliance programs to evolving requirements, demonstrating a commitment to responsible AI development and contributing to a trustworthy and ethical AI ecosystem.

1 European Parliament, "Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI," news release, December 9, 2023, https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.
2 European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts," Brussels, April 21, 2021, COM(2021) 206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.
3 Hadrien Pouget and Ranj Zuhdi, "AI and Product Safety Standards Under the EU AI Act," Carnegie Foundation for International Peace, March 5, 2024, https://carnegieendowment.org/2024/03/05/ai-and-product-safety-standards-under-eu-ai-act-pub-91870#:~:text=The%20AI%20Act%20extends%20risk,for%20private%20life%2C%20and%20nondiscrimination
4 McDermott Will & Emery, "The AI Act: The EU's Bid to Set the Global Standard for AI Regulation," JD Supra, March 13, 2024, https://www.jdsupra.com/legalnews/the-ai-act-the-eu-s-bid-to-set-the-5379690/.
5 Conor Hogan and Matthew Goodbun, "International: Navigating generative AI and compliance," OneTrust Data Guidance, February 2024, https://www.dataguidance.com/opinion/international-navigating-generative-ai-and.
6 McDermott Will & Emery, "The AI Act: The EU's Bid to Set the Global Standard for AI Regulation."