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.