COSMOS
Navigate the Compliance Universe

Ethikos Volume 37, Number 1. January 02, 2023
Artificial Intelligence Act: A European approach

By Patrick Wellens, CCEP-I, CIA, CFE, CRMA, MBA

Patrick Wellens (patrickwellens@hotmail.com) is currently a Compliance Manager for a division of a multinational pharma company based in Zurich, Switzerland. He is a Board Member of Ethics and Compliance Switzerland and co-chair of the Working Group Life Sciences.

Artificial intelligence (AI) is a technology that mimics human intelligence to perform tasks and can iteratively improve itself based on the information it collects.[1] AI is used widely in many technologies and industries; some may notice, others may not. These include (but are by no means limited to): self-driving cars (automotive industry), making the diagnosis of certain diseases more accurate (healthcare industry), product search recommendations (e-commerce & marketing), chatbots (customer service), robotics process automation (manufacturing), facial recognition (defense industry), and talent acquisition (corporations).

AI optimizes operations and resource allocation and improves the prediction and analysis of large datasets. At the same time, AI can also create new risks or negative consequences for individuals and society. AI technology can be misused and provide powerful tools for manipulative, exploitative, or social control practices. Therefore, the European Union (EU) Artificial Intelligence Act defined a risk-based framework that differentiates AI systems with unacceptable risk, high risk, or low or minimal risk, and defined minimum standards that AI systems should comply with.[2]

Common principles for the use of AI

The Artificial Intelligence Act is based on several principles.

- The use of AI technology must be in line with EU values and fundamental rights.[3] The charter of fundamental rights of the EU defines the universal values of human dignity, freedom, equality, and solidarity based on the principles of democracy and the rule of law. This contains principles on nondiscrimination and gender equality.
- AI technology must comply with existing General Data Protection Regulation (GDPR), the EU Data Governance Act,[4] the EU strategy for data,[5] and AI Liability Directive.[6]
- The Artificial Intelligence Act applies a risk-based approach by defining AI services that create unacceptable risk, high risk, and low or minimal risks.
- Transparency obligation for AI systems—i.e., AI systems shall be designed and developed in such a way that their operation is sufficiently transparent to enable users to interpret the systems' output.
- AI systems shall have human oversight—high-risk AI systems shall be designed and developed in such a way that natural persons can effectively oversee them during the period in which the AI system is in use, intending to prevent or minimize the risks to health, safety, or fundamental rights.

Scope of the AI Directive

The Directive applies to AI systems placed on, put into service, or used in the European market. Therefore, the AI Directive also applies to producers and users that are established in a third country (outside the EU) to the extent that the output produced by AI systems are used in the EU.

AI systems exclusively used developed or used for military purposes are excluded from the scope of the Directive.

Prohibited AI services

The following AI services are forbidden:

- Those which materially distort a person's behavior in a manner that causes or is likely to cause that person or another person physical and/or psychological harm.
- Those which exploit vulnerabilities of a specific group of people due to their age or physical or mental disability.
- Those which evaluate or classify the trustworthiness of real people over time based on social behavior or personality characteristics. This includes the social score leading to detrimental treatment of those people or groups in ways unrelated to the context in which the data was collected or unjustified or disproportionate to social behavior.
- Those systems that use real-time remote biometric identification in publicly accessible spaces for law enforcement, unless they are targeted to search for potential victims of crime (including missing children), are in prevention of a specific, substantial, and imminent threat to the life (such as a terrorist attack), or are for the detection, localization, identification, or prosecution of suspect of criminal offense.
- Those which use real-time remote biometric identification in publicly accessible spaces for law enforcement need prior authorization by judicial authority.

High-risk AI services

AI systems identified as high risk are those that:

- Have significant harmful impact on health, safety, and fundamental rights of persons in the EU.
- Are safety components of products or systems.
- Are intended for remote biometric identification of natural persons (technical inaccuracies could lead to biased results and discriminatory effects regarding age, ethnicity, sex, or disabilities).
- Are to be used as safety components in management and operation of critical infrastructure (operation of road traffic, supply of water/gas, electricity, etc.).
- Are used for credit scoring or credit worthiness.
- Are used in employment (recruitment and selection of persons, for making decisions on promotions).
- Are used in migration, asylum, border control, or affect vulnerable people. The accuracy, nondiscriminatory nature, and transparency are important.

Purchase Login