WHITEPAPER

The 6 principles of AI and data protection: how the AI act ensures data is safe

imprivata®

In today's rapidly evolving technological landscape, the responsible development and deployment of artificial intelligence (AI) systems are paramount. Recently, regulations have been developing in an attempt to identify, assess, and provide guidance on how to mitigate the potential risks of AI systems, specifically generative AI and large language models (LLM). In the United States, the White House released the AI Bill of Rights and an executive order to help outline best practices for creating and using AI systems. The biggest move has come from the European Union's proposed AI Act, which aims to establish a comprehensive framework of ethical and legal standards to govern the use of AI.

This whitepaper examines the Six Key Principles of AI utilized by the AI Act, and Imprivata's commitment to adhering to these principles for governing the privacy and security of data.

Background of the AI Act

AI has brought a new era of possibilities to the world. However, with this progress comes the need to ensure that AI systems operate within a framework of ethical and legal standards. The most definitive and comprehensive attempt to legislate these standards can be seen in Europe's AI Act, which is very close to becoming law.

The AI Act itself represents a general framework for the future of AI, emphasizing the importance of human oversight, accountability, and the need for rigorous testing and validation of AI systems to minimize risks and ensure reliability. The Act includes six principles that providers and consumers of AI systems should follow, with privacy and data governance being the central pillars. As a response to growing concerns about how personal data is handled, the AI Act outlines measures to protect individuals' privacy, ensuring that AI systems process data lawfully, fairly, and transparently.

01

HUMAN OVERSIGHT AND ACCOUNTABILITY

The first principle is rooted in the recognition that AI systems should assist human capabilities rather than replace them. To achieve this, AI systems must be designed to allow humans to make informed decisions and intervene when necessary. AI systems must be transparent and understandable, providing clear explanations for their actions and recommendations.

Accountability mechanisms are crucial for ensuring that AI systems are developed and used responsibly. This includes holding individuals and organizations accountable for the actions of AI systems under their control.

02

TECHNICAL ROBUSTNESS AND SAFETY

To help maintain the reliability and trustworthiness of AI systems, providers and developers must design systems to be generally reliable, predictable, and safe to use. This requires the adoption of robust testing and validation methodologies, a proactive approach to identifying and mitigating risks, and assurance that AI systems perform as intended, eliminating or posing little harm to individuals or society.

03

PRIVACY AND DATA GOVERNANCE

The privacy and data governance standards of this principle reflect growing concerns with how organizations that use AI systems handle personal data. The AI Act mandates strict measures to protect individuals' privacy, with guidelines around processing data lawfully, fairly, and transparently.

One of the key requirements is that AI systems must be designed with privacy by design and by default — a fundamental tenant **introduced by the GDPR**. Essentially, privacy considerations must be integrated into AI systems from the start.

Under data governance, there are specific provisions on data security, retention, and subject rights. These provisions are designed to safeguard personal data from unauthorized access, use, or disclosure, and give individuals the right to access, correct, and/or delete their data.

04

TRANSPARENCY

AI systems need to be transparent, with providers giving clear insight into:

- The purpose of an AI system
- The data processed by the system
- The decisions made by the system

Organizations need to provide clear and accessible information about data processing practices, such as the legal basis for processing, the categories of data involved, and the recipients of that data.

05

DIVERSITY, NON-DISCRIMINATION, AND FAIRNESS

Ethical development and deployment of AI rest upon three pillars: diversity, non-discrimination, and fairness. These serve as the foundation for ensuring that AI technologies benefit all individuals and society.

- Diversity in AI development teams brings a range of perspectives, experiences, and backgrounds to foster ideas and approaches that may have otherwise gone unnoticed.
- Non-discrimination means organizations must actively work to prevent their AI models from being discriminatory.
- Fairness is establishing robust policies and procedures to ensure that AI systems are used in a fair and unbiased manner.

06

SOCIAL AND ENVIRONMENTAL WELL-BEING

The sixth principle rests on the belief that AI systems should be designed and used in a way that contributes to sustainable and inclusive growth, social progress, respect for the environment, and sustainable development. Organizations must develop and deploy AI systems in a responsible manner, considering potential risks, and contributing positively to society.

How Imprivata adheres to these principles

Your patient data is of the utmost importance to us, and we understand the importance of trusting our organization as a business partner. We have woven the principle of privacy and security by design and default into the enterprise, from product design to third-party risk management.

Our compliance program has cross-functional leadership that gives equal weight to privacy and security. We have interdisciplinary committees that meet regularly to discuss developments, needs, and actions within these spaces, one of which is our AI Committee. This committee includes strategic members across product design, data science, research and development, engineering, security, privacy, compliance, procurement, and other stakeholders, all tasked with responsible AI governance based on the core principles.

While our compliance program is enterprise-wide, we also apply specific standards to our products. Imprivata Digital Identity Intelligence (formerly FairWarning) is designed as a governance and compliance enabler, with HIPAA as the North star. With our proactive approach to privacy and security, we have invested in third-party certifications and assessments of the enterprise as a whole, and Imprivata Digital Identity Intelligence, specifically, including:

- SOC 2 Type 2
- ISO 27001
- ISO 27701
- HIPAA Risk Assessments
- ONC CEHRT

We have also engaged with specialized AI experts to help plan long-term infrastructure, transparency, and other governance and compliance actions related to the Imprivata Digital Identity Intelligence solution. This independent review of our AI model aligns to HIPAA standards, which are some of the most stringent standards for the anonymization of data.

Our organization has always taken data protection seriously. In fact, our compliance efforts already aligned with the Six AI Principles before the AI Act was introduced. As AI continues to develop more capabilities, Imprivata will stay current with ongoing regulations to ensure our systems uphold current standards, and fully protect the privacy of individuals.

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organisations solve complex workflow,security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organisations in over 45 countries to fully manage andsecure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at +1 781 674 2700
or visit us online at **www.imprivata.com**