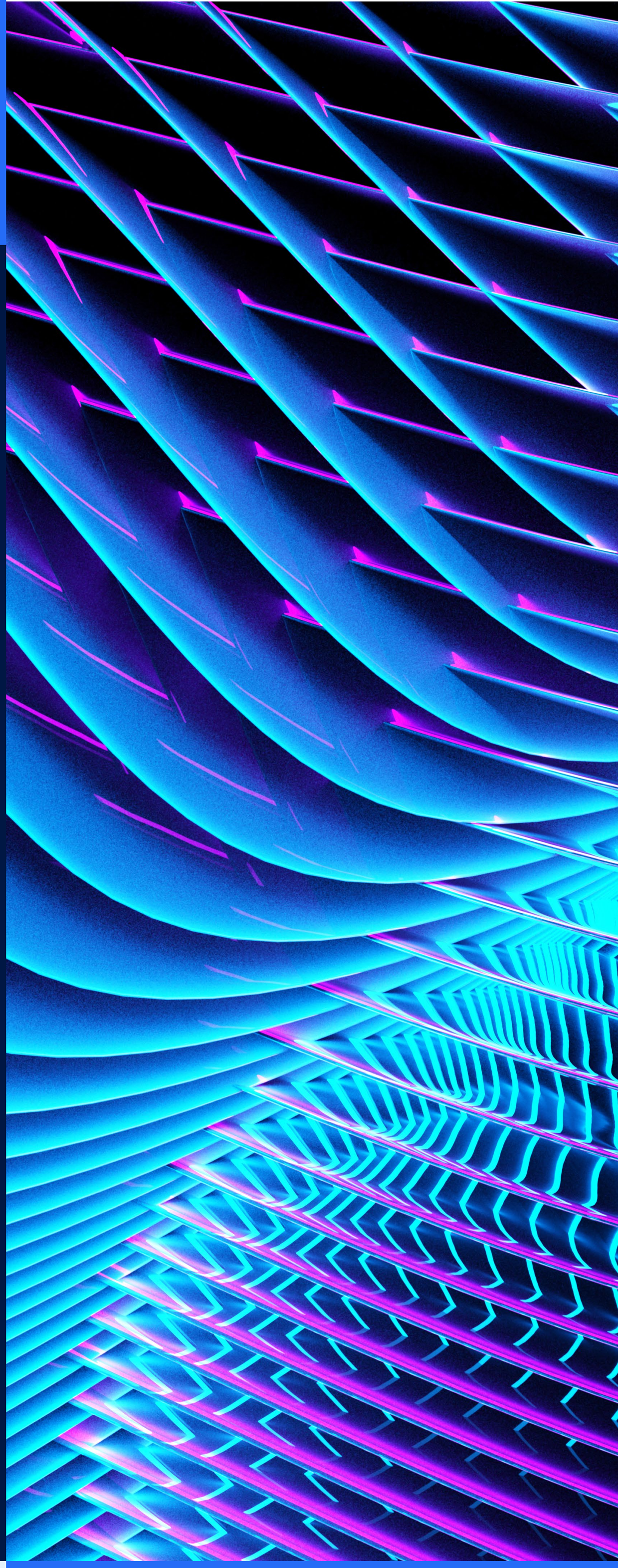
Navigating the EU AI Act:

Understanding Compliance and Opportunity in an age of Digital Transformation



WHITEPAPER

Introduction and Overview

Artificial intelligence (AI) has become a transformative force across industries, unlocking innovation while introducing new challenges. In response, the European Union (EU) has introduced the EU Artificial Intelligence Act (‘**EU AI Act**’), representing a significant regulatory development aimed at fostering trust, transparency, and accountability in the deployment of artificial intelligence systems (‘**AI systems**’) across various sectors, addressing potential risks associated with AI.

The AI Act was published in the Official Journal on 12th of July of 2024 and entered into force 20 days later. Its implementation and enforcement will follow a phased approach, concluding by the end of the year 2030.

This document outlines key provisions of the AI Act and how Zscaler is approaching the regulation.

Key Provisions of the Act

The AI Act contains several key provisions:

DEFINITION OF AI SYSTEM

In essence, Article 3(1) of the AI Act defines an AI system as a technology with a certain level of autonomy that, from the input it receives, can generate outputs such as content, predictions, recommendations, or decisions.

RISK-BASED CLASSIFICATION OF AI SYSTEMS

The AI Act adopts a risk-based approach, classifying AI systems into four risk levels, based on their potential to cause harm. This classification ensures that oversight is proportional to the potential impact of the AI system, focusing on safeguarding fundamental rights and public safety.

- **Unacceptable risk:** AI practices that pose an unacceptable risk are prohibited (Article 5 of the AI Act – 'Prohibited AI Practices').
- **High-risk AI systems:** certain AI systems are considered high-risk and must meet specific legal requirements (Article 6 of the AI Act – 'Classification Rules for High-Risk AI Systems' and Annex III).
- **Limited-risk AI:** AI systems with lower risk are subject to lighter obligations (Article 50 of the AI Act – 'Transparency Obligations for Providers and Deployers of Certain AI Systems').
- **Minimal-risk AI:** Unregulated AI systems (including the majority of AI applications currently available on the EU single market, such as AI enabled video games and spam filters).

REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

High-risk AI systems must meet strict requirements to ensure reliability, transparency, and accountability. These requirements aim to create a framework that promotes responsible AI deployment.

- **Risk management:** Organizations should develop and execute a comprehensive risk assessment process to identify and mitigate risks throughout the AI lifecycle, when developing or leveraging AI systems deemed high-risk.
- **Data governance:** Organizations should ensure training datasets are free from bias and of high quality.
- **Transparency and documentation:** Architectural design documents should be developed and maintained by organizations developing or leveraging high-risk AI systems, ensuring transparency on the systems functioning and intended purpose.
- **Human oversight:** Mechanisms should be put into place to prevent harm by enabling human intervention when needed.

Roles and Responsibilities

There are various actors involved in the lifecycle of AI systems. These responsibilities ensure accountability, compliance with regulations, and the safe and ethical deployment of AI technologies. The EU AI Act has defined a set of key responsibilities, divided among the primary stakeholders of the AI lifecycle.

PROVIDERS (DEVELOPERS):

Entities that develop, place on the market, or put AI systems into service.

DEPLOYERS:

A natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

IMPORTERS:

Bring AI systems into the EU market from third-party countries.

DISTRIBUTORS:

Make AI systems available on the EU market, their responsibilities are similar to those of importers but focus on the supply chain within the EU.

AUTHORIZED REPRESENTATIVES:

For non-EU providers, authorized representatives act as their legal representative within the EU.

NATIONAL AUTHORITIES AND THE EUROPEAN AI BOARD:

Regulatory authorities that oversee and enforce compliance against the regulation.

Governance and Compliance

The EU AI Act establishes a governance structure to oversee compliance, including the creation of national supervisory authorities and a European Artificial Intelligence Board. Organizations developing or deploying AI must ensure conformity through audits and detailed architectural documentation. Non-compliance can lead to fines up to €35M or 7% of annual turnover, whichever is higher. In addition, individual Member States will have the ability to establish rules on penalties and other enforcement measures, which may include warnings and non-monetary measures.

Zscaler's Organizational Philosophy on AI

Mission and Vision

Zscaler recognizes the potential of AI in driving innovation, enhancing operational efficiency, and delivering unparalleled customer value. Leveraging AI effectively can unlock significant competitive advantages, from automating routine tasks to uncovering insights in vast datasets. However, alongside this enthusiasm for AI capabilities comes the critical responsibility to deploy these technologies securely, ethically, and in alignment with evolving societal expectations and regulatory frameworks. In an effort to achieve this balance, Zscaler is determined to embed transparency into their AI strategies and mitigate potential harm.

AI in Zscaler Services

Zscaler is leveraging the power of AI to deliver smarter, faster, and more proactive protection against cyberattacks. By integrating various types of AI, such as machine learning, natural language processing, and behavior analytics, Zscaler can detect and respond to threats in near real-time, minimizing vulnerabilities, and enhancing user experiences. AI allows Zscaler to analyze vast amounts of data, identify patterns, and predict potential risks, empowering Zscaler customers to stay one step ahead of adversaries. As the field of AI continues to evolve, Zscaler will remain at the forefront of leveraging these technologies for the betterment of its customers, while ensuring data privacy and compliance.

AI Evaluation and Governance

To further enhance the governance over AI systems, Zscaler has implemented an internal AI risk assessment process as part of its product due diligence to evaluate the risks posed by potential AI systems, ensuring that they comply with applicable regulatory requirements, and appropriate mitigation measures are identified.

Wrap Up

As a leader in cybersecurity, Zscaler is committed to adhering to the EU AI Act by evaluating its AI systems and their impact. Zscaler assesses its AI systems to mitigate risks and ensure compliance with emerging regulatory standards early in the AI system development lifecycle.

Zscaler's flagship zero trust architecture coupled with AI-enabled services empowers customers to combat AI-driven threats effectively by delivering advanced solutions. By leveraging AI responsibly, Zscaler helps organizations embrace AI through security and data protection guardrails, maintain regulatory compliance, and build resilient security strategies for the future. Through innovation and accountability, Zscaler aims to support its customers in navigating the complexities of the modern threat landscape with confidence and trust.

DISCLAIMER:

The information contained herein should not be construed as legal advice. Customers are responsible for making their own independent assessments of the information in this white paper and conducting their own due diligence. Information and views expressed in this white paper, including URLs and other internet website references, may be revised without notice.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Zero Trust Everywhere