AI ACT

WHITE PAPER

April 2024
VERSION: 1.0

TABLE OF CONTENTS

Introduction

This white paper explores the contrasting regulatory frameworks for artificial intelligence (AI) in the European Union and the United Kingdom. It aims to illuminate their implications for AI system creators and provide a guide for navigating these diverse legal landscapes.

Background

The dawn of Artificial Intelligence (AI) has not only heralded unprecedented technological progress, it has also raised pressing ethical, privacy, and security questions that challenge our traditional regulatory paradigms. As we stand at this critical juncture, this white paper provides a detailed exploration of the divergent paths taken by the European Union (EU) and the United Kingdom (UK) in framing regulations to govern the burgeoning field of AI.

The EU's AI Act represents a pioneering attempt to create a holistic legal structure that meticulously categorises AI applications into different risk tiers, mandating rigorous compliance protocols for those deemed high-risk, to safeguard fundamental human rights and societal values. In contrast, the UK's strategy eschews prescriptive rules in favour of a more dynamic, principles-based framework that emphasises flexibility, fostering an environment conducive to innovation while still upholding ethical standards and public trust.

This paper provides an insightful comparison of these approaches, offering guidance for AI system creators on navigating the regulatory landscapes.

The EU Approach

The EU's AI Act is a landmark piece of legislation that categorises AI systems into four risk levels: **Unacceptable**, **High**, **Limited**, and **Minimal**. It focuses on imposing obligations on high-risk AI applications, including comprehensive risk management systems, stringent data governance, transparency measures and adherence to ethical standards. The Act emphasises the protection of fundamental rights and safety, with significant fines for non-compliance.

In the EU, creators of AI systems, especially those classified as high-risk, will need to ensure compliance with strict regulations outlined in the AI Act. This includes conducting thorough risk assessments, implementing robust data governance protocols, ensuring transparency and traceability of AI systems, and adhering to specific technical standards and documentation requirements. Creators must also register high-risk AI systems in an EU database.

EU Act Risk Levels

The risk levels are broadly defined as follows:

Unacceptable: The use of technologies in the unacceptable risk category is prohibited with little exception, including real-time facial and biometric identification systems in public spaces, China-like systems of social scoring, subliminal techniques to distort behaviour and technologies that exploit vulnerabilities of certain populations.

High-risk: Critical infrastructure, employment and management of workers, law enforcement and democratic processes. These are only some examples please refer to the Act itself for a broader list.

Limited Risk: These pose a lower risk but have some transparency obligations. For example requiring that individuals must be informed if they are engaging with a chatbot.

Minimal Risk The examples given are AI-enabled video games or spam filters. These make up the majority of AI systems currently in use within the EU.

In the EU, non-compliance with the AI Act can result in fines of up to €30 million or 6% of the total worldwide annual turnover for companies, depending on the severity of the infringement.

The UK Approach

In contract, the UK's regulatory framework for AI is characterised by its adaptability and emphasis on fostering innovation. It promotes a principles-based approach, focusing on the safety, transparency, fairness, accountability, and contestability of AI systems. The UK aims to create a regulatory environment that supports growth and innovation while addressing the ethical and societal impacts of AI technologies.

In the UK, the approach is more principles-based, focusing on safety, transparency, fairness, and accountability. Creators are encouraged to adopt AI in a way that aligns with these principles, fostering innovation while also ensuring public trust. The UK government emphasises the importance of ethical AI development, offering guidance and frameworks to support creators in implementing these principles effectively. Regulators will be the ones to enforce measures to ensure AI systems function correctly and are technically secure throughout their lifecycle.

The principles cover five main areas outlined as follows:

Safety, security and robustness

- AI systems should be reliable, secure and safe throughout their entire lifespan. Risks associated with their use should be identified, evaluated and controlled continuously.

- Regulators may need to enforce certain measures on the entities they regulate to ensure AI systems function correctly and are technically secure and reliable throughout their lifecycle.

Appropriate transparency and explainability

- AI systems must be transparent and explainable at an appropriate level. This means providing relevant information about the AI system to relevant parties, including details on its purpose, usage and timing. Explainability means relevant parties can access, interpret and understand the decision-making processes of an AI system. The degree of transparency and explainability required should be proportional to the risks associated with the AI system.

- Regulators may need to encourage and support relevant actors throughout the AI lifecycle to implement appropriate transparency measures, such as product labelling. This is to ensure parties directly affected by the use of the AI system are able to enforce their rights.

Fairness

- AI systems should not violate the legal rights of individuals or organisations, exhibit unfair discrimination towards individuals or lead to unjust market outcomes. All parties involved in the AI lifecycle should determine the appropriate standards of fairness that align with the specific purpose, results and relevant laws of the system.

- Regulators may need to create and publish guidelines and examples of fairness thatapply to AI systems within their regulatory jurisdiction and develop instructions that consider pertinent laws, regulations, technical standards and assurance techniques.

Accountability and governance

- Effective measures of governance must be implemented to oversee the supply and use of AI systems. There needs to be unambiguous accountability established throughout the AI lifecycle.

- Regulators will be expected to explore strategies to guarantee that clear standards for regulatory compliance and best practices are placed on relevant actors in the AI supply chain. Additionally, they may need to foster the implementation of governance processes that ensure these standards are consistently met.

Contestability and redress

- Where appropriate, users, impacted third parties and actors in the AI lifecycle should be able to contest an AI decision or outcome that is harmful or creates material risk of harm.

- Regulators will be expected to clarify existing routes to contestability and redress and implement proportionate measures to ensure that the outcomes of AI use are contestable where appropriate.

The UK's approach to enforcement will rely on regulators with additional monitoring functions as support from the central government.

ICO Intervention

The Information Commissioner's Office (ICO) will play a significant role in data protection and privacy matters. Therefore, penalties in the UK can also be substantial, aligning with GDPR , which allow for fines up to £17.5 million or 4% of annual global turnover, whichever is greater, for serious breaches.

Implications for AI Creators and Businesses

AI system creators operating within the EU will need to navigate a more structured regulatory environment, especially for high-risk applications. This includes compliance with specific requirements such as risk assessments, data governance protocols, and transparency obligations. In the UK, creators are encouraged to adopt a flexible approach, aligning with principles that ensure the safe and ethical development of AI technologies.

For the most current and detailed information regarding AI regulations in the EU and UK, please visit the following official websites:

- EU AI Act:
  https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

- UK government whitepaper on AI including annex information
  https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach

Further reading

- UK ICO AI Guidance:
  https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

- UK Government National AI Strategy including a 10-year plan:
  https://www.gov.uk/government/publications/national-ai-strategy

- EU AI Act Infographic of features and requirements:
  https://iapp.org/resources/article/eu-ai-act-cheat-sheet/