

# Lawyer Insights

## Understanding the Current AI Compliance Issues and Data Privacy Risks in the Metaverse

Organizations should focus on designing and operating AI systems used in the metaverse in accordance with new legislation in the EU, the UK and beyond.

By Sarah Pearce

Published in Law.com | April 10, 2023



Last month, Hunton Andrews Kurth released a client alert briefly discussing the challenges in the metaverse and new legal, regulatory and technical issues that may not have been addressed or even contemplated in existing legislation to ensure compliance. In this article, we further discuss these compliance issues, with a focus on AI and in particular, on the forthcoming EU Artificial Intelligence Regulation and approach in the EU and UK.

### About the EU Artificial Intelligence Regulation

Among the most advanced legislation for the regulation of the use of AI in the metaverse, the EU Artificial Intelligence Regulation (EU Regulation) identifies different levels of regulation depending on the perceived risks posed by the various forms and uses of AI. Some uses of AI technologies in the metaverse may well fall into the unacceptable, high-risk and high-regulation bracket. These will likely include any use of AI technologies for biometric identification, education and training, or employment. Similarly, any use of AI technology that amounts to subliminal, manipulative or exploitative techniques that cause harm, or any use that involves automated face recognition will also be classified as high risk and subject to strict requirements before getting to market. Such requirements include implementing a risk management system, providing usable training, validation and testing data sets, maintaining technical documentation and records, and finally, ensuring human oversight.

AI systems with specific transparency obligations are likely to be classified as “limited risk” under the EU Regulation. However, it will require operators to ensure users faced with AI-enabled chatbots or AI-enabled video and computer games, for example, be made aware that they are interacting with a machine, so they can make an informed decision to continue or refrain. Data privacy requirements must also be considered of course in the context of transparency. The EU Regulation includes future-proofing provisions and requires operators of AI systems to remain trustworthy even after they have been placed on the market, with AI technology providers being required to demonstrate ongoing quality and risk management.

### AI Compliance in the UK

The EU Regulation is likely just the first of many similar such steps towards regulation globally. The UK Government also set out its proposals for new AI legislation in the summer of last year and just recently, on 29 March 2023 it launched a White Paper to guide the use of AI in the UK. The White Paper sets out

## **Understanding the Current AI Compliance Issues and Data Privacy Risks in the Metaverse**

By Sarah Pearce

Published in Law.com | April 10, 2023

a so-called “new” approach to regulating AI that aims to “build public trust in cutting edge technologies and make it easier for businesses to innovate, grow and create jobs.”

In its White Paper, the UK Government takes a more flexible approach compared to that of the EU. Rather than setting out a series of requirements, the UK approach is based on five core principles:

- safety, security and robustness: applications of AI should function in a secure, safe and robust way where risks are carefully managed
- transparency and explainability: organizations developing and deploying AI should be able to communicate when and how it is used and explain a system’s decision-making process in an appropriate level of detail that matches the risks posed by the use of AI
- fairness: AI should be used in a way which complies with the UK’s existing laws, for example the Equality Act 2010 or UK GDPR, and must not discriminate against individuals or create unfair commercial outcomes
- accountability and governance: measures are needed to ensure there is appropriate oversight of the way AI is being used and clear accountability for the outcomes
- contestability and redress: people need to have clear routes to dispute harmful outcomes or decisions generated by AI

Furthermore, instead of appointing one regulator as responsible for AI governance and enforcing compliance with these principles, the UK Government plans to grant powers to existing regulators including the Information Commissioner’s Office and the Competition and Markets Authority to develop “tailored, context-specific approaches” that are appropriate to the use of AI in their respective fields. The White Paper talks of legislation further down the line to “ensure consistency” of approach but it is clearly not imminent and in the meantime, the designated regulators will be tasked with developing guidance for organizations developing and using AI technologies and with monitoring AI implementation.

There is ongoing debate around similar regulations outside of the UK and Europe, including various US initiatives contemplating federal regulation of AI.

### **Establishing an AI Risk-Management Program for Compliance**

At Hunton Andrews Kurth, we continue to monitor the development of AI legislation globally, including the adoption process of the EU Regulation. Organizations should focus on designing and operating AI systems used in the metaverse in accordance with the new legislation. Developers and providers of AI technologies operating in the metaverse should establish a comprehensive AI risk-management program integrated within their business operations. The program should include:

- an inventory of all AI systems used by the organization;
- a risk-classification system;
- risk-mitigation measures;

## Understanding the Current AI Compliance Issues and Data Privacy Risks in the Metaverse

By Sarah Pearce

Published in Law.com | April 10, 2023

- independent audits;
- data-risk-management processes; and
- an AI governance structure.

It is important to think about compliance by design and a framework that could address various issues while remaining flexible enough to accommodate the differences in regional and national legislation.

*Sarah Pearce is a partner in the firm's Global Technology, Outsourcing & Privacy group in the firm's London office. Sarah's practice covers a broad range of data privacy and data security issues in the UK and across Europe. She can be reached at [+44 \(0\)20 7220 5722](tel:+442072205722) or [spearce@HuntonAK.com](mailto:spearce@HuntonAK.com).*

*Reprinted with permission from the April 10, 2023 issue of Law.com. © 2023 ALM Media Properties, LLC. Further duplication without permission is prohibited. All rights reserved.*