

Insights and Analysis

The EU AI Act and UK AI regulation: A product law perspective

19 October 2026

Regulation EU 2024/1689 (the **EU AI Act**) is widely regarded as a landmark piece of legislation. It introduces a dedicated legal framework for artificial intelligence (**AI**), adopts a risk-based approach to regulation, and places fundamental rights considerations at the heart of compliance.

While the EU has adopted a dedicated legislative framework for AI, the UK has, to date, favoured a more principles-based and sector-led approach, relying largely on existing regulatory frameworks. At first glance, that divergence may suggest that the compliance challenges facing businesses operating in the EU and UK are materially different.

For product lawyers, however, many of the concepts underpinning the EU AI Act are not entirely new. Many of its operational requirements, including risk management, post-market monitoring, incident investigation, regulatory notification, and corrective action, reflect concepts that have long featured in product regulation.

For decades, EU product laws have required manufacturers and other economic operators to monitor products through their lifecycle, assess risks, and take appropriate action where issues emerge.

Viewed through that lens, many of the EU AI Act's operational requirements, which appear to borrow

directly from the product safety playbook, will be familiar to organisations accustomed to product regulatory compliance.

A familiar approach to managing risk

One of the clearest parallels is that compliance obligations do not simply end once a product or system reaches the market.

Under EU product legislation, manufacturers are expected to continue monitoring products, gather information about real-world performance and respond when risks emerge. Increasingly, EU product regulation is built around lifecycle compliance rather than a one-off assessment undertaken before a product is placed on the market. This broader shift towards lifecycle regulation will be familiar to many businesses operating across both EU and UK product regulatory landscapes.

The EU AI Act adopts a similar philosophy. Providers of high-risk AI systems must establish post-market monitoring systems, collect information about the operation of their systems in practice and assess whether risks, incidents or non-conformities emerge after deployment. The objective is not simply to demonstrate compliance before a system reaches the market, but to continually assess whether that system continues to operate as intended.

Responding to risks and non-compliance

The similarities become even clearer when issues arise after products or systems have been placed on the market.

Under Regulation (EU) 2023/988 (the **EU General Product Safety Regulation** or **EU GPSR**), a manufacturer that considers, or has reason to believe, that a product is dangerous must act immediately. Depending on the circumstances, this may involve taking corrective measures, including withdrawal, or recall. Authorities must be notified and, where a recall is undertaken, consumers may also need to be informed.

Similar concepts can be found across the broader EU product regulatory framework. For example, under Directive 2011/65/EU (the **Restriction on Hazardous Materials Directive** or **RoHS Directive**), manufacturers that consider, or have reason to believe, that an in-scope product is non-compliant must take corrective measures and notify competent authorities.

The EU AI Act adopts both of these approaches:

- Where a provider considers, or has reason to believe, that a high-risk AI system is not in conformity, it must immediately take the necessary corrective action, which may involve bringing the system into conformity, withdrawing it, disabling it, or recalling it.
- Where a provider becomes aware that a high-risk AI system presents a risk to health, safety, or fundamental rights, it must immediately investigate the causes of the risk and inform market surveillance authorities (and, where applicable, the notified body) of the nature of the non-compliance and any corrective action taken.

Incident reporting: product safety thinking applied to AI

The parallels become even more apparent in the EU AI Act's serious incident reporting regime.

Providers of high-risk AI systems must report serious incidents to market surveillance authorities. Reports must generally be submitted immediately after the provider establishes, or reasonably suspects, a causal link between the AI system and the incident, and, in any event, no later than 15 days after becoming aware of the incident.

The regime also includes accelerated reporting deadlines in particularly serious circumstances:

- Widespread infringements, or incidents involving serious and irreversible disruption to critical infrastructure, must be reported immediately, and no later than 2 days after the provider (or deployer) becomes aware of that incident.

- Incidents involving death must be reported immediately after a causal relationship is established or suspected and, in any event, no later than 10 days after the provider (or deployer) becomes aware of the incident.

Reporting is only one element of the process. Following the report, providers of high-risk AI systems must also investigate the incident, conduct a risk assessment, cooperate with authorities, and implement any necessary corrective measures.

For organisations with established product safety procedures, many of these requirements will already be well understood. The practical questions are often the same: **what happened, is there a causal link, how serious is the risk, does the regulator need to be informed and what corrective action is required?**

Although these are classic product safety questions, they are increasingly becoming AI governance questions.

Fundamental rights: the key differentiator

However, there is one important difference.

Traditionally, product safety law has focused on protecting consumers against physical harms such as injury, death, or property damage.

The EU AI Act adopts a broader concept of risk. A serious incident may involve not only health and safety impacts, but also infringements of fundamental rights protected under EU law. For example, risks relating to discrimination, privacy, or freedom of expression may arise even where no physical harm occurs.

In that sense, the EU AI Act expands the categories of harms that must be monitored and managed. This means that, while many of the governance mechanisms found in the EU AI Act resemble those found elsewhere in product regulation, the nature of the risks that need to be assessed is

considerably broader.

What about the UK?

Although the UK has not adopted legislation equivalent to the EU AI Act, many of the same governance themes are beginning to emerge through existing regulatory frameworks and guidance. AI-related risks are increasingly being considered through the lens of established product safety, consumer protection, data protection and sector-specific regulation.

For example, organisations developing or deploying AI systems may already need to address AI-related risks under existing UK data protection requirements, while AI-enabled products remain subject to established product safety obligations.

For businesses operating across both jurisdictions, the EU AI Act may therefore have an influence extending beyond those activities that fall directly within its scope. The practical disciplines that it requires, including risk assessment, incident escalation, monitoring and governance, are likely to shape wider organisational practices, even where equivalent legal obligations do not currently exist under a standalone UK AI regime.

What does this mean for businesses?

The practical implication is that compliance with the EU AI Act may not require an entirely new approach to governance.

Many businesses already have established processes for monitoring products, investigating issues and engaging with regulators. For those organisations, the challenge may be less about building entirely new compliance structures and more about adapting existing governance frameworks to address AI-specific risks, including risks relating to fundamental rights.

This may be particularly true for businesses operating across both the UK and EU. Even where organisations are not subject to an equivalent standalone AI regime in the UK, compliance with the EU AI Act may influence governance standards across wider business operations.

Ultimately, while the EU AI Act introduces a novel regulatory framework for AI, businesses that already understand post-market monitoring, incident reporting, corrective action and regulatory engagement may be better placed than they expect to respond to its requirements. The challenge is likely to lie not in the underlying governance disciplines themselves, but in applying them to a new category of risks, including those relating to fundamental rights.

Authored by Valerie Kenyon, Eshana Subherwal, Vicki Kooner, and Magdalena Bakowska.

As AI, product safety, consumer protection and digital regulation continue to converge, businesses face an increasingly complex and interconnected compliance landscape. Our **Global Products Law team** supports clients across the full product lifecycle, from product design and market entry to post-market compliance, incident management and regulatory engagement. Through our horizon-scanning activities, we help businesses identify emerging regulatory risks and prepare for legal developments before they become enforcement priorities. To discuss any of the issues covered in this article, or their potential impact on your business, please get in touch.

Contacts



Valerie Kenyon

Partner

 London

 [Email me](#)



Vicki Kooner

Senior Associate

 London

 [Email me](#)



Christian Di Mauro

Partner

 Milan

 [Email me](#)



Eshana Subherwal

Senior Associate

 London

 [Email me](#)



Magdalena Bakowska

Senior Associate

 London

 [Email me](#)

