AGENTIC AI: NAVIGATING LEGAL RISK

August 2025

James Hutchinson and Jonathan Booton

Artificial intelligence is evolving rapidly, with innovative technologies emerging on a regular basis. One of the most significant developments is agentic AI. Unlike traditional AI tools that operate within defined parameters, agentic AI systems can pursue goals, make autonomous decisions and interact dynamically with the world.

Below are several practical examples of how agentic AI could be used in the construction industry:

- **Project management and supply chain optimisation** – Agentic AI could help manage material orders, predict shortages, automate logistics and ensure timely delivery. For example, if a materials shipment is delayed, the system could identify the issue and automatically reorganise the work schedule to minimise downtime.
- **Health and safety monitoring** – Agentic AI could analyse video fees to identify risks such as missing personal protective equipment or overcrowded sites. If a hazard is detected, the system might log the issue, adjust schedules or resources to avoid accidents or delays and escalate persistent problems to a safety officer for on-site intervention or training.
- **BIM** – Agentic AI could review BIM models for compliance issues and propose design changes, streamlining the design and construction process.

While the opportunities are substantial, agentic AI also raises complex legal risks and uncertainty. These systems challenge traditional approaches to accountability, data protection, regulation and legal principles of agency. We set out below the English law position and key risks to consider.

Legal position under English law

There is currently no dedicated legal framework for AI under English law. The Government's approach is pro-innovation and principles based, favouring the adaptation of existing laws over creating a new regulatory regime.

Key risks

1. **Scale of automation –** Agentic AI can operate continuously and at scale, which increases the potential impact of errors or misaligned decisions. A single faulty decision could affect multiple projects or result in a wide-reaching data breach involving many data subjects.
2. **Accountability and liability –** Traditional liability models assume a human decision-maker. Agentic AI disrupts this principle. Legal responsibility for its actions is uncertain and organisations using agentic AI may find themselves strictly liable. Contractual protections may also be limited, as AI providers typically seek to exclude liability for their system's behaviour.

3. **Roles under data protection legislation** – Agentic AI raises questions about data controller and data processor roles under the UK GDPR. To avoid an AI system being treated as a data controller, there must be dynamic human oversight. Clear allocation of responsibility between developers and deployers is essential.

4. **Transparency and explainability** – UK GDPR requires individuals to be informed about how their data is used. This is especially challenging with agentic AI, which may make unexpected decisions, hallucinate or rely on biased data. Decisions may also be highly technical and difficult to explain. Organisations will need to implement systems to trace, assess and explain how a decision has been made.

5. **Automated decision-making** – The Data (Use and Access) Act 2025 relaxes some restrictions on automated decision making. However, decisions must still be fair, transparent, explainable and free from bias. Where agentic AI is used in sensitive areas, such as employment or insurance, organisations must ensure appropriate human oversight and the ability to justify decisions.

6. **Data minimisation and purpose limitation** – Agentic AI can process large volumes of personal data, increasing the risk of misuse, leaks or unauthorised profiling. Organisations must apply strict data minimisation principles and purpose limitation rules under UK GDPR.

7. **Testing AI systems** – Traditional testing methods may not be sufficient for agentic AI. Innovative approaches are needed to test these systems over time in real worlds environments, to identify risks such as bias, discrimination or incorrect outputs.

8. **Intellectual property considerations** – Agentic AI can create original content, but English law does not yet clearly address IP ownership where there is no human author. There are also risks around copyright infringement if training data or outputs use protected works. Organisations should adopt policies to address ownership, third party rights and use of confidential material. Meaningful human input is essential.

Next steps

Adopting agent AI brings both opportunities and risks. To prepare, organisations should:

- **Assess exposure** – Conduct an AI risk audit of current or planned deployment.

- **Insurance** – Consider insurance policies and ensure that the organisation has adequate cover where AI is being deployed, particularly where there has been automated decision making.

- **Update contracts** – Consider adding AI specific clauses related to autonomy, liability, data use and compliance (where applicable).

- **Establish ethical guardrails** – Establish good AI governance and create and update policies that ensure ethical and legal oversight. See our recent article on why AI policies are important here.

- **Monitor the regulatory Landscape** – Keep an eye out for changes to legislation such as the EU AI Act and the Data (Use and Access) Act 2025. See our recent articles on:

- prohibited AI practices which are now in force here; and

- the changes resulting from the introduction of the Data (Use and Access) Act 2025 [here](#).

How we can help

To learn more about how we can support your organisation in managing the legal risks of agentic AI, please contact:

- James Hutchinson – j.hutchinson@beale-law.com – +44 (0) 20 7469 0408
- Jonathan Booton – j.booton@beale-law.com – +44 (0) 20 7469 0403

James Hutchinson - j.hutchinson@beale-law.com - +44 (0) 20 7469 0408
Jonathan Booton - j.booton@beale-law.com - +44 (0) 20 7469 0403