

LEGAL SURGERY

agentbase
THE UK SALES AGENT REGISTER

Implications of AI agents for agency agreements

Salesforce UK Limited is currently advertising Agentforce with the strapline “What AI Was Meant To Be”.

An AI agent can be described as a software programme that can interact with its environment, collect data, and use the data to perform self-determined tasks to meet pre-determined goals. This raises the question whether principles can require their agents – whether individuals, partnerships, or companies – to use AI agents.

Can principals require that their agents use AI agents?

The starting point under both the Commercial Agents Regulations and at common law is that an agent must comply with the reasonable requests of their principal.

This was illustrated some years ago in a case concerning an agent who refused to use new technology introduced by their principal. The manner of the refusal was such as to breach the necessary personal relationship of trust that must exist between principal and agent (in the same way as it is necessary to exist between employer and employee).

This was followed more recently in a case where the agent had resisted the changes introduced by the principal to move to a paperless email communication system. In that case, the principal was able to snatch victory from the jaws of defeat as a result of the way in which the agent behaved.

The key takeaway from both judgments is that the courts will not stand in the way of a principal introducing technological change into their business so far as their agents are concerned provided that the principal goes about requesting their agent's adoption of the technological change in a reasonable way.

It follows that in principle, principals can require the use by the agents of AI agents.

Can principals require that their agents do not use AI agents?

Although the question may seem counterintuitive, it follows from the cases mentioned above, that in principle, principals can require that their agents do not use AI agents.

Failure to act in accordance with a principal's reasonable requests

An agent who fails to act in accordance with their

principal's reasonable requests is in danger of the principal claiming that such failure amounts to a serious breach by the agent of the agency agreement which the principal can accept. The result is that the principal claims that it was the agent who brought the agency agreement to an end and, as a consequence, the agent has lost the right to claim compensation or indemnity under the Commercial Agents Regulations.

Risks of using AI agents at a principal's request

Where an agent uses AI at the request of their principal, it is important to consider confidentiality. The main issues include:

- **Data access:** To function effectively AI agents often require access to large datasets. Such datasets can include confidential information but when processed by an AI system, there is the risk that such information is compromised if there are insufficient security controls.
- **Cloud storage:** Many AI agents operate using cloud-based services. This means that data is transmitted over the internet and stored in external servers. In turn, this introduces additional vulnerability as a result of the possibility of data breaches during transmission or attacks on cloud infrastructure.
- **Sharing information:** A particular way in which an AI agent is similar to an agent is that an AI agent is not immune to sharing information inadvertently! This could occur where an AI agent is integrated into multiple systems or applications resulting in the unintentional sharing of confidential information across the systems.
- **Data protection:** It is also possible that the principal's data protection strategy is insufficient.

Agents, AI agents, and data protection

The relationship between the principal and agent, particularly concerning data sharing and control, varies on a case-by-case basis.

Establishing the facts about the data flow and use between the parties is important in determining whether, under UK data protection laws, the agent is acting as a processor (for the principal) or as a separate controller.

AI agents add an additional layer of complexity as they may need to process personal data submitted by the agent as a third party service. The agent should clarify its status, and obligations, under data protection laws in respect of its use of the AI agent. This may include the agent being required to ensure that the AI agent

is subject to the GDPR-mandated contractual data processing obligations for processors.

If the agent acts as a controller, any processing of personal data must comply with the GDPR principles, including lawfulness, fairness, transparency, data minimization, storage limitation and security.

The agent will also need to be in a position where it can facilitate any data rights requests made by end-customers.

These will all need to be considered in the context of using an AI agent. There will also be additional international transfer requirements to consider if the AI agent is processing personal data outside the UK and EEA.

Failure to comply with applicable data protection laws could expose both the agent and the principal to regulatory sanctions, including fines. Therefore, establishing the facts from the outset is essential to ensure that the necessary measures, as between agent, principal and AI agent, are duly put in place.

Implications of AI agents in agency law: key takeaway

When an agent is requested by their principal to use an AI agent, it is crucial to carefully consider the terms of the request and the intended use of the AI agent, as this can significantly impact the responsibilities and obligations of both principal and agent.

Steve Sidkin is a Head of Commerce and Technology at Fox Williams LLP, Solicitors

fox williams
Good sense in the City

10 Finsbury Square
London, EC2A 1AF
Tel: 020 7615 2505
SISidkin@foxwilliams.com
www.foxwilliams.com



Disclaimer: This article does not contain legal advice and is for general guidance only. AgentBase, the firm of solicitors and the writer accept no liability in connection with the general guidance given.

Please ensure that you obtain legal advice before acting in reliance upon anything in the article. For example please be clear that the information and views given in this column may not cover all possible angles, aspects, relevant considerations and/or points of law and so that all or any information which is given above needs in every instance to be referred for legal advice for clarification and amplification, before being relied