

AI Guardrail Considerations For Legal Transaction Teams

By **Michal Berkner, Alexander Gee and Nikki Bradford** (September 30, 2026)

On Aug. 17, the Solicitors Regulation Authority issued a guidance note for solicitors and law firms, warning about the misuse of artificial intelligence and raising concerns that both free-to-use and paid-for AI tools may not provide the contractual and technical safeguards needed to maintain client confidentiality.[1]

This article explores the risks that the use of AI tools in corporate transactions poses to confidential information. We consider whether traditional contractual protections restricting public disclosure of such information adequately address those risks. We also highlight some key considerations for transaction teams seeking to ensure that their nondisclosure agreements, or NDAs, are fit for purpose in an AI-enabled deal environment.

Public AI Versus Private AI

AI tools and systems used in the context of transactions can be divided, broadly, into two categories:

- Open or public AI — these systems are typically free to use and publicly accessible. Prompts, inputs and outputs may be used to train, improve or otherwise develop the underlying model, and there are limited controls over how data is accessed, retained or reused.
- Closed or private AI — these systems are typically paid for and operate within a secure, controlled environment where prompts, inputs and outputs are not used to train the underlying model. Strict controls are maintained over data access and usage.



Michal Berkner



Alexander Gee



Nikki Bradford

The use of AI and the risks associated with it must be considered from the outset of any transaction and throughout its life cycle. While the efficiencies and opportunities of AI are clear for all to see, the absence of adequate guardrails in NDAs and other contractual frameworks may leave confidential information exposed, regardless of whether the AI tools used are open or closed.

Why the System Distinction Is Important

In *Munir, R (on the Application of) v. Secretary of State for the Home Department*, heard in October and November 2025, the Upper Tribunal likened uploading confidential information into an open or public AI tool to placing the information on the internet in the public domain.[2]

The SRA has gone further, warning that the use of closed or private AI may in itself be insufficient and that users must ensure that appropriate protections are in place within the applicable contractual framework, including the relevant terms of use or service

contracts.[3]

The risk is particularly concerning for clients operating in industries where proprietary data holds significant value or provides a competitive advantage, such as the healthcare and life sciences sector, where the unauthorized exposure of clinical trial datasets, trade secrets or other sensitive information through AI tools could have far-reaching commercial and regulatory consequences.

NDA's

Given these risks, transaction teams need to consider whether their existing contractual frameworks, and in particular their NDAs, adequately address the use of AI by all parties to the transaction, and, critically, the restrictions on use.

Deal teams and their legal advisers should be scrutinizing how all recipients of confidential information, in particular those acting for the buy-side in transactions and their in-house teams, investment bankers and other external deal advisers, intend to use AI tools to process that information.

Most sophisticated law firms have negotiated terms with their AI service providers to include protections for client data. This is to prevent confidential information from being exposed to unauthorized parties, and restrictions on the training of the underlying AI models using client and law firm data. However, law firms are not the only parties involved in the collection, handling and review of confidential information during a transaction.

For example, if a recipient of confidential information proposes to manage the due diligence process in-house using AI tools to reduce costs, there is a real risk that the individuals involved may not fully appreciate the consequences of uploading confidential information to open or public tools, including the potential for inadvertent disclosure to unauthorized parties, the loss of privilege or the impact of allowing proprietary data to be used to train the underlying AI models.

Many existing NDAs were drafted well before AI-assisted working became commonplace in transactions, and have historically only included express terms on AI usage in a small fraction of cases.

While typical confidentiality and permitted-use restrictions may extend to the use of AI tools in principle, they rarely address what happens when confidential information is included in a prompt, processed by an AI system or reflected in an output and are unlikely to impose restrictions on the training of the underlying AI model.

Transaction teams should not assume that an NDA drafted without AI-specific provisions adequately deals with the associated risks — and should consider whether supplementary provisions are advisable.

No One-Size-Fits-All Approach

When advising on M&A-related NDAs, set clear expectations around AI usage during the course of the transaction. When acting for the disclosing party, draw a clear distinction between open or public and closed or private AI tools and to restrict expressly the use of open or public AI.

The use of closed or private AI tools can typically be permitted, but only where appropriate

safeguards are in place to prevent confidential information from being disclosed to third parties or used to train or improve the underlying model, and to ensure that the information can be deleted or destroyed when required.

There is, however, no one-size-fits-all approach; the precise parameters will depend on the nature of the transaction, the industry sector and the sensitivity of the information involved.

Transaction teams should therefore consider whether their NDAs provide sufficient clarity on which AI tools may be used to process confidential information and whether they are open or public, or closed or private, as well as what contractual and technical safeguards should apply to that use.

Teams should also assess whether information submitted to the AI tool can be accessed, retained or reused beyond the transaction or used to train or improve the AI model. They should also consider whether there is a risk that any input or AI-generated output could be accessed or reviewed by third parties, including human reviewers or developers, who are not subject to the terms of the NDA.

In addition, consideration should be given to whether return and destruction obligations capture prompts, outputs and other AI-generated materials derived from the confidential information, whether equivalent protections are applied where advisers, consultants or other representatives use AI tools, and which party should bear the risk of the misuse of AI in due diligence.

Conclusion

The AI landscape is fast-moving, and the risks are real. NDAs must be updated and a new market standard set as a matter of priority to ensure that NDAs are fit for purpose in an AI-enabled deal environment.

Failing to address what kind of AI tools counterparties are permitted to use as part of any transaction risks leaving companies' most valuable assets — proprietary know-how, trade secrets and commercially sensitive data — unnecessarily exposed. The question is no longer whether to address AI in your NDAs, but whether you can afford not to.

Michal Berkner and Alexander Gee are partners, and Nikki Bradford is an associate, at Baker McKenzie.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] <https://www.sra.org.uk/solicitors/guidance/misuse-ai/>.

[2] *Munir, R (On the Application Of) v Secretary of State for the Home Department (AI hallucinations; supervision; Hamid)* [2026] UKUT 81 (IAC).

[3] SRA, 'Misuse of AI - Warning notice' (August 2026), 'Our concerns' section available at: <https://www.sra.org.uk/solicitors/guidance/misuse-ai/>.