

The Dos and Don'ts of AI in Contracting

Posted in Alert on November 5, 2025

As artificial intelligence (AI) technologies increasingly integrate into legal practice, contract drafting has become a prominent area of innovation. AI models promise enhanced efficiency, consistency, and cost-savings, but the use of AI models may also introduce legal, regulatory, and practical risks. This article outlines high-level dos and don'ts for businesses deploying AI in contract drafting and processing.

The Dos:

1. Keep Human Oversight Involved

Do use generative AI models approved by your company's IT team to modify drafts of standard agreement templates, provide summaries, or compare variations of contract clauses; however, before implementation, AI generated agreements should always be reviewed by a legal professional for legal requirements (for example, jurisdiction-specific regulations) and for legal contextual understanding (for example, identification and allocation of risk and liability).

2. Ensure Data Security

Companies are responsible for ensuring that the AI vendors and tools they contract with or otherwise use are in compliance with federal and state data protection laws. Do work with your internal IT team to ensure your company's AI tools have proper data security certifications (for example, SOC 2 Type II or ISO 27001). Do ensure that AI models utilized by the company (particularly open-source platforms) do not share or train on confidential or protected information. Do have written Data Processing Agreements in place with AI vendors (drafted by legal counsel, not AI) and monitor for downstream liability in the case of noncompliance.

3. Keep Records of AI Use

Do maintain documentation of how and when AI was used in contract drafting workstream. The goal of this documentation is not just to create a log but to actively demonstrate a commitment to quality control and reasonable oversight. In the event of dispute over a contract, being able to produce an audit trail showing a consistent process of AI-assisted drafting followed by competent human review can help rebut potential claims and resolve disputes.

4. Leverage AI for Executory Contracts

Do take advantage of AI's review and summary capacities for contract intake, e.g. flagging incomplete forms and other gaps, summarizing typical customers and markets for operational strategy, and identifying potential sales leads for additional upselling opportunities and add-on products and services. Of course, this is subject to data security and consumer protection requirements where applicable.

The Don'ts:

1. Don't Input Sensitive Data into AI Models

Personal data, trade secrets, and confidential information should only be analyzed with AI tools that have been validated and approved by a company's internal IT team. Providing confidential materials to an unvetted or public-facing AI model may make the information accessible to the AI software company for its own business purposes. The most significant risk is that the AI model will "train" on the confidential material, which means the AI platform is essentially absorbing the information to improve itself. If this happens, your confidential material could be incorporated into the output the AI model delivers to other users, potentially exposing your trade secrets to a competitor or the public. Inputting confidential information into a public AI model is the digital equivalent of publishing it, resulting in an irreversible loss of trade secret protection and a potential waiver of legal privilege.

2. Don't Rely on AI for Compliance Assurance

Don't rely on generative AI to ensure comprehensive legal compliance. Although AI can sometimes assist in risk identification, it has critical limitations which make it unreliable as an authority on legal compliance. Additionally, because industry-specific laws and regulations change frequently and vary across jurisdictions, AI systems trained on obsolete data could generate legally incorrect responses, or even "hallucinate" by citing non-existent laws or cases or by creating fictitious regulatory standards.

3. Don't Use Unvetted Output

Don't copy-paste AI-generated text directly into contracts without professional review, as it often contains subtle but critical flaws, including legally unenforceable language, outdated legal references, or terms misaligned with your commercial objectives. AI models should only be implemented in legal contract workflows with professional human oversight, including both a legal and internal compliance review.

In sum, generative AI is a powerful tool for accelerating the contracting process, but the current generation of AI platforms are not a viable replacement for competent legal counsel (yet). While AI can help automate routine tasks, provide excellent summaries and comparisons, or highlight risks, it has no understanding of a business's risk tolerance, no strategic insight into negotiating position, and zero accountability for the outcome. Before integrating generative AI into their contract drafting workflows, companies should properly vet AI tools, mandate qualified human supervision, and validate all AI-generated documents for legal and regulatory compliance.

We Can Help

At Miller & Martin, PLLC, our attorneys represent companies and business owners of all kinds in connection with contract drafting and processing. If you need help with such a matter, please feel free to contact [T. J. Gentle](#), [Jason McCarter](#) or [Livia Campos](#).

[Read article published on JD Supra](#)