Adopting Generative AI? Key Contract Considerations for Healthy Due Diligence

Devin Bates
dbates@mwlaw.com
(501) 688.8864

08/26/2024

As generative AI continues to be a hot topic in board rooms and an unavoidable reality on the front lines of business, leaders must make informed decisions when choosing AI vendors. The integration of AI into your operations can offer substantial benefits, but it also introduces unique risks and challenges. To protect your business interests, it's essential to ask questions of AI vendors upfront. Below, we explore some of these key points to help you navigate the adoption of generative AI.

1. Understanding the AI Tools: What type of AI is being used by the vendor? Before entering a contract, ensure you have a clear understanding of the specific AI tools the vendor will use to analyze or modify your data. Determine whether these tools are proprietary or third-party solutions, and ask for detailed descriptions of their functionality. This knowledge will help you assess the tools' compatibility with your business needs and identify any potential risks.

2. Incident Response Expertise: was AI development guided by professionals? AI tools should be developed with input from experienced incident response professionals. These experts bring valuable insights into risk management and security, ensuring the AI tools are equipped to handle potential data breaches and other security incidents. Confirm with the vendor that such professionals were involved in the AI's development.

3. AI vs. Traditional Analysis: how much is AI-driven? Understand the extent to which the vendor's solutions rely on AI versus traditional analysis methods. Understanding this balance is crucial, as it impacts the reliability, accuracy, and legal defensibility of the results. Ask the vendor to specify which aspects of their solutions are AI-driven and which are based on traditional methodologies.

4. Data Sources and Training: what fueled the AI'S development? The performance of an AI tool is significantly influenced by the quality and scope of the data used for its training. Inquire about the sources of data the vendor used to develop their AI tools and the extent of these datasets. This information helps you gauge the AI's ability to handle various scenarios, its potential biases, and overall reliability.

5. Compliance with Privacy Laws: is data sharing legal? Ensure that sharing your data with the AI vendor complies with all applicable privacy laws and confidentiality obligations. These can evolve quickly, especially as state and federal agencies churn out new laws and regulations at a quick pace. Non-compliance can lead to severe legal and financial consequences, so it is important to clarify how your data will be used and confirm that its use is legally permissible under relevant regulations.

6. Data Use Restrictions: what are the limits on vendor use? Clearly define the restrictions on the vendor's ability to use or further utilize your data. These restrictions should be explicitly outlined in your

contract. Understand whether the vendor can use your data for purposes beyond the agreed scope, such as refining their AI tools, and ensure your rights over the data are preserved.

7. Protecting Confidential Information: can it be kept out of AI tools? Your organization's confidential information, trade secrets, intellectual property, and all other types of sensitive data must be protected from being inadvertently incorporated into the vendor's AI tools. Ask the vendor about the measures in place to prevent this. If such protection cannot be guaranteed, consider the implications of sharing specific data with the vendor.

8. Data Security Measures: what protections are in place? If your sensitive data will be processed by the AI tool, it is vital to understand the security measures the vendor has implemented. These could include encryption, access controls, and incident response protocols. Robust security measures are essential to prevent unauthorized access and data breaches.

9. Ownership Rights: who owns the AI-generated output? Define the ownership rights of any AI-generated output, especially if it includes outputs derived from your data. Your contract should clearly state that your business retains control over critical outputs. This is crucial to protect your proprietary information, trade secrets, and other intellectual property.

10. Accuracy and Verification: How Are AI Results Verified? Ensure that the AI-generated results are accurate and complete. Inquire about the methods the vendor uses to verify the outputs produced by their AI tools. This might include human oversight, cross-checking with traditional methods, or other validation techniques. Reliable verification processes are key to trusting the AI's outputs.

It can also be wise to address training and support, because once implemented of course you will want your internal users to understand how the AI tool works and how they can use it properly. Ensuring a healthy dose of understanding will ensure that your team can manage the AI's integration into your business processes effectively, leading to potential disruptions or inefficiencies.

Adopting generative AI offers significant and transformative advantages but also requires careful consideration and thorough vetting of AI vendors. By addressing the points outlined above in your contracts, you can ensure that your business is protected, compliant, and positioned to leverage AI effectively. As always, seeking legal counsel to navigate these complex issues can provide additional safeguards and peace of mind.

This content was generated in part by, and prepared for publication with the assistance of, ChatGPT.