King & Spalding

Client Alert

Technology Transactions and Sourcing

NOVEMBER 15, 2023

For more information, contact:

Amy Levin
+44 20 7551 7526
alevin@kslaw.com

Nicholas Maietta
+1 202 626 2954
nmaietta@kslaw.com

Alexa Christianson
+1 703 245 1049
achristianson@kslaw.com

King & Spalding

Chicago
110 N Wacker Drive
Suite 3800
Chicago, Illinois 60606
Tel. +1 312 995 6333

London
125 Old Broad Street
London, EC2N 1AR
United Kingdom
Tel. +44 20 7551 7500

Contracting for AI Technologies - Top Five Best Practices

Artificial intelligence ("AI"), including generative AI ("GAI")[1], has gained significant momentum in recent months due to its potential to transform how organizations create content, automate tasks, and provide personalized experiences. However, it is incumbent on legal counsel to carefully consider the associated risks posed by AI when negotiating and drafting contracts with third party vendors, including (i) contracts which govern an organization's direct purchase, use or license of AI technologies, and (ii) contracts which govern an organization's procurement of products and services from third party vendors which use and/or incorporate AI into their products and services.

Striking the right balance between enabling innovation and appropriately managing risk is key in determining the optimal contractual safeguards and protections to include when contracting for AI. To that end, this alert will provide (a) a brief overview of the key risks associated with the use of AI technologies, and (b) the top five (5) best practices which legal counsel should consider when negotiating and drafting contracts for the purchase and/or use of AI.

OVERVIEW OF KEY AI- RELATED RISKS

The use of AI presents a number of new and unique risks, ranging from legal risk (such as the loss of intellectual property rights), to business risk (such as business interruption or loss of revenue) to reputational risk (such as damage to an organization's brand) – each of which vary depending on the type of AI involved and how it is used. Thus, while a 'one size fits all' approach does not exist when evaluating AI risk, set forth below are the most prominent risks faced by our clients when contracting for AI technologies with third-party vendors:

- Risks related to the training data used to develop AIs, which may infringe a third party's intellectual property and/or data rights;
- Potential disputes over ownership of the AI's output;

- Confidentiality breaches and the unauthorized disclosure of data, particularly when sensitive data is shared with the AI model;
- Inaccurate output;
- Unintended and implicit biases in the training data or AI model which could lead to discriminatory, inappropriate, or harmful outputs; and
- Noncompliance with laws and regulations, particularly in highly-regulated industries such as healthcare and financial services.

TOP 5 BEST PRACTICES FOR AI CONTRACTING

To mitigate the risks associated with AI, legal counsel should consider the following five (5) best practices when contracting for AI technologies:

1. **Consider the Right Technology Framework**. Organizations need to carefully consider what they need from the AI technology and how the AI capabilities are best delivered, including determining whether to build or buy AI. Legal counsel should therefore encourage business input at the outset of any contract involving AI to ensure the right technology framework is being used. This requires identifying and assessing how the AI technology will be implemented into the organization's existing technology stack as well as how the AI will be integrated into existing offerings - each of which creates the potential for unanticipated risks and can be difficult to assess. When considering the implementation of any AI offering, the following factors at minimum should be considered to ensure the proper technology framework is deployed in the contract:
    a. **Training Data**: On what data was the AI trained? Does it appear the provider secured the appropriate rights to such data? Will the organization's own data be used in any way for training or improving the AI?
    b. **Dedicated Instance**: Is a dedicated instance of the AI available? What additional security and privacy safeguards are available for a dedicated instance? What hosting options are available for the AI technology?
    c. **Customization**: Will the organization's data be used to train or tune the AI models to a specific use-case? Are sufficient safeguards, representations, and warranties in place to address such uses of Company data? Is the additional cost worth the improved performance?
    d. **Safeguards**: What protections are in place to ensure that the output of the AI is not harmful and is aligned with expectations? Are such protections adequate for the use case? If not, what other protections can be implemented?
2. **Conduct AI-Specific Due Diligence on the Vendor**. Legal counsel should also conduct (or ensure that the business has conducted) the appropriate level of AI-specific due diligence by carefully assessing the following as it relates to the vendor: (a) data security and privacy practices; (b) training data (including associated data rights); (c) AI development practices; and (d) compliance with applicable laws and regulations. Organizations should provide vendors with risk questionnaires tailored to AI and the specific solution. Vendor responses can flag salient risks, such as how the AI will handle or store company data and whether the vendor utilizes secure software development practices. Early and proactive diligence reduces the likelihood that the parties discover, after significant time and resource investments are made, that they are misaligned on critical technical aspects of the vendor's offerings. Such proactive diligence is especially vital when AI technologies may be used as a component, or otherwise employed in the development of, the organization's own product or service offerings. Additionally, it is critical to establish sufficient audit rights to ensure ongoing compliance during the life of the contract.

3. **Include an AI Governance Framework**. Legal counsel should also consider including a comprehensive and well-defined AI governance framework in the contract. Including a governance framework will establish clear guidelines and standards for vendors and ensure that they adhere to ethical, technical, data security, and legal principles when using AI. Essential components of an effective AI governance plan or framework include:
   a. requiring counterparties to provide transparent documentation of their AI models and data sources, as such transparency will foster accountability and enables organizations to better assess the reliability of the AI technology;
   b. regular monitoring of AI outputs to ensure alignment with defined technical benchmarks and to identify the potential need to retrain the AI model; and
   c. periodic audits to confirm compliance with data security requirements.
4. **Address the Evolving AI Regulatory Requirements**. In light of the evolving global regulatory landscape in the area of AI, legal counsel should also include robust compliance with laws' provisions in the contract, which should capture the vendor's (and its subcontractors') compliance with all AI-related laws, rules and regulations in the applicable jurisdictions involved, as well as non-binding legislation such as voluntary guidelines and best practices for the development and use of AI and GAI. As of the date of this client alert, notable regulatory actions in the US concerning AI include:
   a. Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence: Calls upon agencies to develop new AI safety and security standards.
   b. The Blueprint for an AI Bill of Rights: Establishes key, but non-binding, principles: (1) safe and effective systems; (2) algorithmic discrimination protections; (3) data privacy; (4) notice and explanation; and (5) human alternative, consideration and fallback.
   c. Voluntary AI Commitments offered to the White House: Leading AI companies made voluntary commitments to the White House to move toward safe, transparent and secure development of AI technology.
   d. NIST's AI Risk Management Framework: Establishes best practices for managing risk associated with AI.

Therefore, when contracting for AI, it is critical that legal counsel include contractual mechanisms which adequately address the vendor's (and its sub-contractors') compliance with the applicable regulatory framework, including: (i) properly defining the scope of applicable laws to include (in addition to the typical definition of laws and regulations) non-binding legislation, as well as new legislation which is enacted at a future date; and (ii) indemnities, representations and warranties, annual vendor certifications, and periodic (and/or triggered) audit rights.

5. **Include AI-Specific Terms, Rights, and Remedies**. Finally, in light of the unique risks presented by the use of AI, legal counsel should also evaluate whether the following AI-specific elements should be included in the contract:
   a. Data use terms tailored for AI that include specifically addressing the use of company data, company inputs to the AI, and outputs of the AI model, and how such data can be used;
   b. Definitions (e.g., data incident, service levels) that encompass AI-specific issues and risks, such as model drift, privacy attacks, or adversarial inputs;
   c. Uncapped vendor-indemnification for data incidents;
   d. Uncapped vendor-indemnification for infringement of third-party intellectual property and data rights;

e. Uncapped damages for the organization's reputational harm due to a data incident or similar failure of the AI model;

f. Incorporation of AI-specific information security and privacy requirements, such as handling data subject requests;

g. Termination rights triggered by the misuse of company data, data incidents, regulatory investigation or enforcement, challenges to the IP rights surrounding training data, and/or an issuance of a temporary restraining order on the counterparty.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,300 lawyers in 23 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE
ATLANTA	CHICAGO	GENEVA	MIAMI	RIYADH	TOKYO
AUSTIN	DENVER	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
BRUSSELS	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	

[1] GAI refers to a class of AI models that use machine learning ("**ML**") techniques trained on large datasets to produce content, such as text, images, or music. The large data sets and ML techniques generally allow the GAI to identify sophisticated and detailed patterns and produce improved content. Large Language Models ("**LLM**") are a category of GAI that used for generating human-like text, with OpenAI's GPT-4 being one of the most recognizable LLM, which serves as the foundational technology behind GAI-powered chatbots like ChatGPT.