

# SOME ATTENTION TO LEGAL IS ALL YOU NEED: A Legal Checklist for AI Customers

This is a high-level, non-exhaustive checklist for customers of AI solutions that will use the solution and output strictly for internal use cases and not use the solution or any output as part of its products or services or for any other external use case. Subsequent checklists will address issues relating to companies' use of AI with its products and services or other external use cases. This checklist was last updated on January 4, 2024 and will be periodically updated as the AI legal landscape changes.\*

## Company-wide Strategic Considerations

Designate an individual or committee within your company that oversees the procurement and use of AI solutions and manages the risks associated with procurement and use of AI solutions.

Draft and implement an internal AI Policy for your company.

Address the following topics in your AI Policy:

- The individuals to which the policy applies;

- Permitted uses of AI solutions;

- Prohibited uses of AI solutions;

- Uses of AI solutions that require specific approvals;

- Prohibited AI providers;

- Approved AI providers;

- AI providers that require specific approvals;

- Approval processes for AI use cases and AI providers;

- Requirements to run AI solutions in a test environment before deployment in a live production environment;

Requirements for human review of outputs and human involvement in decisions assisted by AI;

Reporting obligations with respect to use of AI solutions;

Recordkeeping with respect to use of AI solutions; and

Relation of the policy to other company policies.

Educate your employees on the AI Policy, and, if necessary, provide AI training to your employees.

Establish a system of metrics, reports and audits to confirm your company's compliance with the AI Policy.

---

## Pre-Contract Diligence

Perform due diligence on the AI provider to obtain information on the following:

Nature of the data used by the provider to train the base AI model;

Whether such data includes data scraped from the Internet without third-party consent;

Whether such data includes personal information;

AI provider's use of your fine-tuning training data and inputs (including inputs used during testing);

AI provider's use of outputs generated from your fine-tuning training data and inputs;

To what extent other data is created as a result of your use of the AI solution (ex. "derived data") and the AI provider's use of such data;

AI provider's use of the AI model that is improved with your fine-tuning training data, inputs and outputs;

AI provider's business continuity, disaster recovery, security and privacy practices;

AI provider's legal compliance program; and

AI provider's use of open source software.

Request a 'model card' from the AI provider that sets forth: (i) the training data used to train the base AI model; (ii) the AI model's performance; and (iii) known issues or limitations of the AI model.

Consider whether or not intellectual property protection of outputs is important to you for the particular internal use case. If yes, consider non-AI methods to develop the outputs, if practicable.

---

## Contract Issues

Ensure there is a written contract governing the AI provider's provision of AI solutions. Such contracts may take the form of "click-through" terms of service.

Ask the AI provider if better contract terms are available for an "enterprise" version of the AI solution.

Review and understand the contract to ensure it addresses the issues set forth in this checklist.

Consider the deployment model of the AI solutions.

If the service is deployed as an AI-as-a-service where the AI model will be retained by the provider and you interact with it via an Internet-based user interface, then many traditional software-as-a-service contract issues should be considered.

If the AI model and algorithms are delivered to you to be ran on your infrastructure, then many traditional software license contract issues should be considered.

If the AI solution will be embodied in a physical good or robot, then many traditional sale of goods or lease contract issues should be considered.

Some traditional software-as-a-service and software license contract issues to consider are:

Term of the contract;

Termination rights of the parties;

Provider's post-term transition assistance obligations;

Provider's rights to change the features or functionalities of the service or software;

Restrictions on your access to and use of the service or software;

Your affiliates' rights to use the service or software

Price and payment terms;

Provider's ability to increase prices;

Provider's implementation obligations;

Your acceptance testing rights;

Provider's right to subcontract its obligations;

Provider's business continuity, disaster recovery, data security and privacy contractual commitments;

SLAs regarding uptime, problem response time and problem resolution time;

Risk allocation provisions, including liability caps, waiver of certain types of damages, representations, warranties and indemnities;

Provider's obligations to carry certain insurance policies;

Your ability to assign the contract in the event of a corporate transaction;

Your rights in the event the provider declares bankruptcy;

Governing law and jurisdiction for disputes; and


Provider's ability to unilaterally change the contract terms.

Require the AI provider to represent and warrant that it obtained and will obtain all consents, permissions, rights and licenses necessary to use the training data that the provider used and will use to train the AI model and to provide AI solutions.

Carefully review representations and warranties provided by you that relate to fine-tuning training data and input to ensure that you can comply with such representations and warranties and that they are not overly broad.

Review and understand any use restrictions contained in the contract that impact your use of the AI solutions and the outputs.

Ensure the applicable contract contains terms that restrict the AI provider's use and disclosure of your fine-tuning training data and input for purposes of providing you (and only you) the AI solutions.



Ensure the applicable contract contains terms that provide that you retain all rights, title and interest in and to your fine-tuning training data and input.

Consider how contractual confidentiality terms apply to your fine-tuning training data, inputs, outputs and the AI model that has been fine-tuned by you and/or improved as a result of your inputs.

Consider whether or not the AI provider can use your fine-tuning training data, inputs and outputs to train its AI models that will benefit the provider's other customers.

Ensure that the AI provider is obligated to return to you or destroy (at your direction) all of your fine-tuning training data, your inputs, your outputs and (if applicable) the model that has been fine-tuned or trained with your fine-tuning training data or inputs.

Ensure that you have all required rights and licenses from the provider to use the outputs after the termination or expiration of the contract.

Ensure that, to the extent the AI provider has any intellectual property rights covering the output, such intellectual property rights are assigned to you. (Note: it is unlikely in most current use cases that the provider has any intellectual property rights in the output to assign to you.)

If the AI provider is not willing to provide an assignment of intellectual property rights covering output, ensure that the contract contains a license from the AI provider that is broad enough to cover all of your intended uses of the output.

Consider whether the AI provider should assign to you the intellectual property rights covering the AI model that has been fine-tuned by you and/or improved as a result of your inputs.

Carefully review all provisions in the contract addressing aggregate liability caps and waiver of certain types of damages to ensure that you have the opportunity to recover meaningful amounts from the AI provider in the event you need to make a claim against the AI provider.

Determine whether or not the contract should contain representations, warranties or obligations from the provider with respect to the accuracy, completeness, etc. of the output.

Ensure that the contract requires the AI provider to comply with all applicable laws and regulations, including new laws and regulations that are passed after the effective date of the contract.

Ensure the contract contains security terms and addresses the AI provider's obligations related to data security incidents.

Require the AI provider to defend and indemnify you from third-party claims alleging that the AI provider's AI solution itself, or your mere use of the AI solution itself as contemplated by the parties, infringes third-party intellectual property rights.

Consider whether or not the AI provider should defend and indemnify you from third-party claims arising from your reliance on the AI solution or its output, especially if the AI solution or output does not conform to agreed upon specifications in the contract.

Consider whether or not the AI provider should defend and indemnify you from third-party claims alleging the output infringes third-party intellectual property rights or publicity rights.

Consider whether or not the AI provider should defend and indemnify you from third-party claims alleging the output contains tortious material (material that is biased, defamatory, discriminatory, etc.).

Ensure that the AI provider has a requirement to provide information and assistance to you (subject to reasonable limitations) in connection with any requirement for you to disclose use of AI (ex. required disclosures to regulators).

Consider whether or not you should have the right to audit the AI provider (subject to reasonable limitations).

If the contract takes the form of “standard terms and conditions,” ensure that the AI provider does not have the right to unilaterally change the terms and conditions.

---

## Data Rights Clearance, Data Privacy, and Data Security

Establish and implement proper policies within your company to address access to and use of your fine-tuning training data, inputs, the AI solutions and output.

Establish and implement proper policies within your company to respond to security events relating to your fine-tuning training data, inputs, the AI solutions and output.

Review NIST’s AI Risk Management Framework for best AI security practices.

Request the AI provider to disclose any applicable open source licenses or third-party contracts that impact your use of the AI solutions or output.

Conduct an AI impact assessment prior to deployment of the AI solutions.

Perform a detailed data assessment to determine the nature of all data that will be disclosed to the AI provider or the AI solution for training or as input.

Ensure that you have all necessary consents, permissions, rights and licenses to use your fine-tuning training data and inputs with AI solutions and to disclose your fine-tuning training data and inputs to the AI provider for the purposes of training and using the AI solution.

If your fine-tuning training data or input will contain any personal information:

Ensure that, at the time the data was collected, the individual consented to your use and disclosure of the data in connection with the AI solution;

Consider whether you have a lawful basis for disclosing and processing the data in connection with the AI solution other than consent;

Determine the appropriate role for each party under applicable data privacy laws (ex. data controller, data processor, etc.);

Ensure that the applicable contract contains all contract provisions that are required under applicable laws and regulations (ex. Data Processing Agreement, Business Associate Agreement, etc.); and

Develop and implement a policy to comply with individual data right requests.

Do not use any of your trade secrets or particularly sensitive confidential information as fine-tuning training data or inputs with the AI solution.

Do not use confidential information of a third-party that you are contractually obligated to protect and keep confidential as fine-tuning training data or inputs with the AI solution.

Consider the AI provider's positions and practices with respect to data minimization, data governance, transparency and explainability as it related to the AI provider's use of data and its AI solutions.

---

## Legal Compliance and Risk

Ensure that your disclosure and use of your fine-tuning training data and input in connection with the AI solution does not violate any applicable laws or regulations.

Test the AI solution with your fine-tuning training data and inputs prior to deployment to ensure that the AI solution does not produce biased or discriminatory outputs.

Implement measures to reduce risk of using output that infringes third-party intellectual property rights by using software programs that scan for infringing material and open source code.

Consider what level of human review is required for the particular output and internal use case.

Ensure that you are able to understand and explain the rationale behind the outputs used to make any business decision.

Continuously monitor updates to existing laws and regulations and passages of new laws and regulations that apply to your use of the AI solutions, input and output.

Designate an individual or committee that is responsible for monitoring and reporting on updates to existing laws and regulations and passages of new laws and regulations that apply to your use of the AI solutions, the related data and output.

Some AI internal use cases that require particular attention to applicable laws and regulations are:

Any use of AI by a company in a heavily regulated industry (healthcare, financial services, insurance, etc.)

Use of AI in the workplace, including hiring processes, employee monitoring and automated robots on your premises; and

Use of AI to profile individuals or make automated decisions without human involvement.

Create and implement record-keeping policies that document your use of the AI solutions.

Discuss your company's use of AI with your insurance provider to determine whether any new AI-specific risks are insurable.

Discuss your company's use of AI with your insurance provider to ensure that such use does not risk coverage under current policies.

Consider whether your company's use of the AI solution or decision-making based on the output raises any antitrust concerns. This risk is heightened if you use AI to automatically set pricing.

Consider whether the AI solution will create new recordings of information (that are discoverable in litigation) that were never previously recorded. This is especially true for "meeting assistant" solutions that record and summarize meetings.

*\* Please note that this checklist is for informational purposes only. Use of or reliance upon this checklist does not create an attorney - client relationship. Each company has unique characteristics and circumstances, so please seek professional legal advice before relying on any information contained in this checklist.*



# ARTIFICIAL INTELLIGENCE PRACTICE GROUP

## KEY CONTACTS



### Jack D. Horgan

402.343.3848

[jack.horgan@koleyjessen.com](mailto:jack.horgan@koleyjessen.com)

Jack Horgan counsels clients in the technology industry and works with them on their most critical technology functions and agreements. Evaluating and mitigating risks in complex technology transactions is what he does best. Advising clients on both the provider-side and procurement-side of technology transactions, Jack frequently manages transactions that involve: artificial intelligence, software licensing, software distribution, software development, SaaS, PaaS, IaaS, cloud computing, outsourcing, ERP solutions, IoT, co-location arrangements, database licensing, NFTs, blockchain, mobile applications, patent and technology licensing, joint development arrangements, and IT professional services.



### Roberta L. Christensen

402.343.3712

[roberta.christensen@koleyjessen.com](mailto:roberta.christensen@koleyjessen.com)



### Maureen E. Fulton

402.343.3753

[maureen.fulton@koleyjessen.com](mailto:maureen.fulton@koleyjessen.com)



### Matthew J. Speiker

402.343.3861

[matthew.speiker@koleyjessen.com](mailto:matthew.speiker@koleyjessen.com)