

Strafford

---

*Presenting a live 90-minute webinar with interactive Q&A*

## **Contracting Pointers for AI Providers and Companies Incorporating AI in Their Products and Services**

Navigating Data Ownership and Licensing, IP Representations and Warranties, Regulatory Compliance, and Risk Allocation

---

TUESDAY, FEBRUARY 13, 2024

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

---

Today's faculty features:

Maureen E. Fulton, Partner, **Koley Jessen**, Omaha, NE

Jack Horgan, Shareholder, **Koley Jessen**, Omaha, NE

---

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 option 1.**

## *Continuing Education Credits*

FOR LIVE EVENT ONLY

---

In order for us to process your continuing education credit, you must confirm your participation in this webinar by responding to the attendance verification prompts and clicking the link to complete the Certification Process following the webinar.

If you don't click the link following the webinar, you will receive an email including a link to complete the Certification Process within 24 hours.

For any assistance completing the Certification Process, call 1-877-297-2901 or email [helpdesk@beaconlive.com](mailto:helpdesk@beaconlive.com). For additional information about continuing education, call us at 1-800-926-7926 option 2.

FOR LIVE EVENT ONLY

---

**Recording our programs is not permitted. However, today's participants can order a recorded version of this event at a special attendee price. Please call Customer Service at 800-926-7926 option 1 or visit Strafford's website at [www.straffordpub.com](http://www.straffordpub.com).**

---

**Strafford**

# Contracting Pointers for AI Providers

JACK HORGAN AND MAUREEN FULTON

February 13, 2024

KOLEY ■ JESSEN

ATTORNEYS

# Agenda

- Setting the Stage
- AI Provider Contract Issues
  - Review clauses that technology attorneys deal with every day, but in context of AI
- Privacy Legal Requirements in AI Contracts

# Setting the Stage

- What is AI?
  - For our purposes, typically refers to a computer system or software that uses machine learning
- What is machine learning?
  - A computer system or software that “learns” from massive amounts of data to perform certain tasks without being specifically programmed to do so
  - Classification, prediction (regression), etc.
  - Deep learning is a subset of ML that has many layers and nodes that are modeled after the human brain

# Setting the Stage

- What is generative AI?
  - This is the technology that is relatively new
  - Generates text, images, software code, music and other “creative” outputs, usually in response to a text prompt
- Why the recent AI explosion?
  - Internet + data + cloud deployment model + compute power (Moore’s law) + transformer architecture + user interfaces
  - All of this led to ChatGPT release on November 30, 2022

# Setting the Stage

- What is an AI provider?
  - Only a very small handful of companies have the resources and wherewithal to develop and train their own foundation models
  - Most are actually “AI deployers” that leverage a third-party foundation model in some manner
- So, most “AI Providers” are AI customers on one end (procurement side) and AI deployer on the other side (customer side)
- This presentation focuses on companies that leverage a third-party foundation model, rather than those that develop their own foundation models



# Setting the Stage

- Goal is to have very practical advice for contract issues
- Going to work through real-world provisions that are often negotiated
- This presentation assumes that the foundation model is deployed via –aaS model as opposed to on-premise license model

# AI Services Definition

2.1 Description of Services. Throughout the Term and at all times in connection with its actual or required performance under this Agreement, Provider shall, in accordance with all terms and conditions set forth in this Agreement and each applicable Service Order, provide to Customer and its Authorized Users the following services ("**Services**"):

- (a) Access, in accordance with **Section 2.2** of this Agreement, to the software-as-a-service offering(s) described in one or more sequentially numbered written service orders specifically referencing this Agreement, including all Specifications set forth in such service orders (the "**Subscription Services**"), which, upon their execution, will be attached as part of **Exhibit A** and by this reference are incorporated in and made a part of this Agreement (each, a "**Service Order**");
- (b) service maintenance and the Support Services as set forth in **Section 5** and in the Service Order; and
- (c) such other services as may be specified in the applicable Service Order.

# AI Provider Considerations

- Separate definition for AI functionality?
- A subset of Subscription Services definition or separate?
- Notice SLA type language – “throughout the Term and at all times...”

# Subscription Grant

▲ 2.1 Access and Use. Provider hereby grants to Customer and its Affiliates, exercisable by and through their Authorized Users, a non-exclusive, transferable (as permitted under Section 17.8), and sublicensable (pursuant to Section 2.2(e)), right to:

(a) access and use the Subscription Services, including in operation with other software, hardware, systems, networks, and services, for Customer's and its Affiliates' respective business purposes;

(b) generate, print, copy, upload, download, store, and otherwise Process all GUI, audio, visual, digital, and other output, displays, and content as may result from any access to or use of the Services;

(c) access and use the Services for all such non-production uses and applications as may be necessary or useful for the effective use of the Subscription Services hereunder, including for purposes of analysis, development, configuration, integration, testing, training, maintenance, support, and repair, which access and use will be without charge and not included for any purpose in any calculation of Customer's or its Authorized Users' use of the Services, including for purposes of assessing any Fees or other consideration payable to Provider or determining any excess use of the Subscription Services as described in Section 3.2; and

(d) perform, display, execute, reproduce, and modify (including to create improvements and derivative works of), and distribute and otherwise make available to Authorized Users, any Provider Materials solely to the extent necessary to access or use the Services in accordance with the terms and conditions of this Agreement.

# AI Provider Considerations

- Scope of use
  - Internal only?
  - Can customer commercialize output?
- Use restrictions are critical
- Need to create an Output definition
  - Many “typical” SaaS agreements do not contain an analogous definition

# OpenAI Business Terms

## 2. Restrictions

We own all right, title, and interest in and to the Services. You only receive rights to use the Services as explicitly granted in this Agreement. You will not, and will not permit End Users to:

- (a) use the Services or Customer Content (as defined below) in a manner that violates any applicable laws or OpenAI Policies;
- (b) use the Services or Customer Content in a manner that infringes, misappropriates, or otherwise violates any third party's rights;
- (c) send us any personal information of children under 13 or the applicable age of digital consent or allow minors to use our Services without consent from their parent or guardian;
- (d) reverse assemble, reverse compile, decompile, translate, engage in model extraction or stealing attacks, or otherwise attempt to discover the source code or underlying components of the Services, algorithms, and systems of the Services (except to the extent these restrictions are contrary to applicable law);
- (e) use Output (as defined below) to develop any artificial intelligence models that compete with our products and services. However, you can use Output to (i) develop artificial intelligence models primarily intended to categorize, classify, or organize data (e.g., embeddings or classifiers), as long as such models are not distributed or made commercially available to third parties and (ii) fine tune models provided as part of our Services;
- (f) use any method to extract data from the Services other than as permitted through the APIs; or
- (g) buy, sell, or transfer API keys from, to or with a third party.

# Compliance with Laws

2.5 Compliance with Laws. Provider shall comply with all applicable Laws as they concern this Agreement or the subject matter hereof, including by securing and maintaining all required and appropriate visas, work permits, business licenses, and other documentation and clearances necessary for performance of the Services.

▲ "**Law**" means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree, or other requirement of any federal, state, local, or foreign government or political subdivision thereof, or any arbitrator, court, or tribunal of competent jurisdiction.

# AI Provider Considerations

- Legal landscape is very dynamic
- New laws and regulations will be enacted
- Does the AI provider want to commit to comply with all laws that will be passed in the future?
- Does the AI provider want to commit to comply with all industry or sector specific laws that apply to its customers?
- Does the third-party foundation model provider make this same commitment to the AI provider?



# Subcontracting

2.4 Subcontracting. Provider shall not subcontract any Services, in whole or in part, without Customer's prior written consent, which consent may be given or withheld in Customer's sole discretion. Without limiting the foregoing:

- (a) Provider shall ensure each Provider subcontractor (including any subcontractor of a Provider subcontractor, each, a "**Subcontractor**") complies with all relevant terms of this Agreement;
- (b) Customer's consent to any such Subcontractor shall not relieve Provider of its representations, warranties, or obligations under this Agreement;
- (c) any noncompliance by any Subcontractor or its employees or agents with the provisions of this Agreement or any Service Order will constitute a breach by Provider; and
- (d) Provider shall enter into a written agreement with each Subcontractor that contains terms substantially similar to those set forth in this Agreement.

# AI Provider Considerations

- Third-party foundation model providers have extreme leverage
- AI providers will likely be unsuccessful in obtaining material contractual protections from foundation model providers
- Foundation model providers change their terms and standard practices frequently given the dynamic legal landscape and pace of innovation

# SLAs and Maintenance and Support

4.1 Availability Requirement. Provider shall make the Subscription Services Available, as measured over the course of each calendar month during the Term and any additional periods during which Provider does or is required to perform any Subscription Services (each such calendar month, a "**Service Period**"), at least 99.99% of the time, excluding only the time the Subscription Services are not Available solely as a result of one or more Exceptions (the "**Availability Requirement**").

5.1 Support Service Responsibilities. Provider shall:

(a) correct all Service Errors in accordance with the Support Service Level Requirements, including by providing defect repair, programming corrections, and remedial programming; and

(b) Respond to and Resolve Support Requests as specified in this Section 5.

# AI Provider Considerations

- Almost complete dependency on third-party foundation model provider
- AI feature may, or may not, be a core or mission critical feature
- Is AI provider able to remedy an error with third-party foundation model provider?
- Provider wants to avoid breach claims or service credits if AI feature is down for reasons outside of its control

# Data Security

## 6. Security.

6.1 Information Security. Throughout the Term and at all times in connection with its actual or required performance of the Services hereunder, Provider shall make the Services available in accordance with the data security requirements set out in **Exhibit C**.

6.2 Data Breach Procedures. Provider maintains a data breach plan in accordance with the criteria set forth in **Exhibit C** and shall implement the procedures required under such data breach plan on the occurrence of a data breach (as defined in such plan).

6.3 Provider Systems. Provider shall be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems), and networks used by or for Provider to access the Customer Systems or otherwise in connection with the Services ("**Provider Systems**") and shall prevent unauthorized access to the Customer Systems through the Provider Systems.

6.4 Material Breach of Security Provisions. Any failure of the Services to meet the requirements of this Agreement with respect to the security of any Customer Data or other Confidential Information of Customer, including any related backup, disaster recovery, or other policies, practices, or procedures, is a material breach of this Agreement for which Customer, at its option, may terminate this Agreement immediately on written notice to Provider without any notice or cure period, and Provider shall promptly reimburse to Customer any Fees prepaid by Customer prorated to the date of such termination.

# AI Provider Considerations

- Almost complete dependency on third-party foundation model provider
- Is AI provider able to remedy a data incident that occurs on foundation model providers systems?
- AI provider should not commit to any security term or condition that is stronger or broader than it receives from its third-party providers

# Fees

8.2 Fees During Renewal Terms. Provider's Fees are fixed during the Initial Term. Provider may increase Fees for any Renewal Term by providing written notice to Customer at least 60 calendar days prior to the commencement of such Renewal Term.

8.3 Responsibility for Costs. Provider shall be responsible for all costs and expenses incurred in or incidental to the performance of Services, including all costs of any materials supplied by Provider, all fees, fines, licenses, bonds, or taxes required of or imposed against Provider, and all other of Provider's costs of doing business.

# AI Provider Considerations

- Almost complete dependency on third-party foundation model provider
- Foundation model provider may change fees
- AI provider may be locked in to provide AI services on the customer side under a fixed price while fees/expenses on the procurement side are increasing



# Term and Termination

14.3 Termination for Cause. Either party may terminate by written notice of termination to the other party effective as of the date specified in such notice: (i) this Agreement, if the other party materially breaches this Agreement; or (ii) any Service Order, if the other party materially breaches that Service Order, in each case (clause (i) and (ii)) provided that such breach (A) cannot be cured; or (B) being capable of cure, remains uncured thirty (30) days after the breaching party receives written notice thereof; and

# AI Provider Considerations

- AI provider needs to consider term and termination in context of foundation model provider's termination rights and rights to amend commercial terms
- AI provider may be locked in to provide AI services on the customer side while the foundation model provider may amend the commercial terms on the procurement side

# OpenAI Business Terms

## 14. Modifications to these Business Terms and the OpenAI Policies

**14.1 Updates.** We may update these Business Terms or the OpenAI Policies by providing you with reasonable notice, including by posting the update on our website. If, in our sole judgment, an update materially impacts your rights or obligations, we will provide at least 30 days' notice before the update goes into effect, unless the update is necessary for us to comply with applicable law, in which case we will provide you with as much notice as reasonably possible. Any other updates will be effective on the date we post the updated Business Terms or OpenAI Policies. Your continued use of, or access to, the Services after an update goes into effect will constitute acceptance of the update. If you do not agree with an update, you may stop using the Services or terminate this Agreement under Section 8.2 (Termination).

**14.2 Exceptions to Updates.** Except for an update to comply with applicable law, updates to these Business Terms or the OpenAI Policies will not apply to: (a) Disputes between you and OpenAI arising prior to the update; or (b) Order Forms signed by you and OpenAI (as opposed to an automated ordering page) prior to us notifying you of the update. However, to the extent an update relates to a Service or feature launched after an Order Form is signed it will be effective upon your first use of such Service

# Confidentiality

**"Confidential Information"** means information in any form or medium (whether oral, written, electronic, or other) that the Disclosing Party considers confidential or proprietary, including information consisting of or relating to the Disclosing Party's technology, trade secrets, know-how, business operations, plans, strategies, customers, and pricing, and information with respect to which the Disclosing Party has contractual or other confidentiality obligations, in each case whether or not marked, designated, or otherwise identified as "confidential".

# AI Provider Considerations

- Are inputs customer's confidential information?
- Are outputs confidential information?
  - If yes, customer's or provider's?
- Are AI models improved with input confidential information?
  - If yes, customer's or provider's?
- How do non-use, non-disclosure and protection terms typically found in confidentiality sections apply to inputs and outputs?
- Consider application of post-termination return and destruction requirements

# OpenAI Business Terms

## 4. Confidentiality

**4.1 Use and Nondisclosure.** “Confidential Information” means any business, technical or financial information, materials, or other subject matter disclosed by one party (“Discloser”) to the other party (“Recipient”) that is identified as confidential at the time of disclosure or should be reasonably understood by Recipient to be confidential under the circumstances. For the avoidance of doubt, Confidential Information includes Customer Content. Recipient agrees it will: (a) only use Discloser’s Confidential Information to exercise its rights and fulfill its obligations under this Agreement, (b) take reasonable measures to protect the Confidential Information, and (c) not disclose the Confidential Information to any third party except as expressly permitted in this Agreement.

**4.2 Exceptions.** The obligations in Section 4.1 do not apply to any information that (a) is or becomes generally available to the public through no fault of Recipient, (b) was in Recipient’s possession or known by it prior to receipt from Discloser, (c) was rightfully disclosed to Recipient without restriction by a third party, or (d) was independently developed without use of Discloser’s Confidential Information. Recipient may disclose Confidential Information only to its employees, contractors, and agents who have a need to know and who are bound by confidentiality obligations at least as restrictive as those of this Agreement. Recipient will be responsible for any breach of this Section 4 by its employees, contractors, and agents. Recipient may disclose Confidential Information to the extent required by law, provided that Recipient uses reasonable efforts to notify Discloser in advance.

## Intellectual Property Right Ownership and Licensing

- Note that title of slide is misleading for several of the following sets of data and materials.
  - Data and AI generated materials generally are not protectable by intellectual property rights in US (trade secret may be an exception).
  - Contractual restrictions become much more important.

# Intellectual Property Right Ownership and Licensing

- Foundation model training data (usually not addressed)
- Customer fine-tuning data, inputs and prompts
  - Create precise definitions
  - Are these items “Confidential Information” and “Customer Data”?
  - What will provider do with these sets of data?
  - Ensure customer provides all required rights and licenses
  - “Ownership” typically not critical for provider



# Intellectual Property Right Ownership and Licensing

- Outputs
  - Create a precise definition
  - Is Output “Confidential Information” and “Customer Data”?
  - What will provider do with Outputs, if anything?
  - What restrictions need to be imposed upon customer’s use of Outputs?
  - Likely not subject to intellectual property right protection under current US law
  - If provider assigns intellectual property rights to customer, ensure such assignment is “quitclaim” style

# Intellectual Property Right Ownership and Licensing

- Improved AI model
  - Important to remember ownership of improved AI model if provider further trains its models on customer inputs and resulting outputs
  - Provider wants to avoid situation where customer claims it owns the improvements to the model or provider is prohibited from using improved model with other customers

# OpenAI Business Terms

3.1 *Customer Content.* You and End Users may provide input to the Services (“Input”), and receive output from the Services based on the Input (“Output”). We call Input and Output together “Customer Content.” As between you and OpenAI, and to the extent permitted by applicable law, you (a) retain all ownership rights in Input and (b) own all Output. We hereby assign to you all our right, title, and interest, if any, in and to Output.

3.2 *Our Obligations for Customer Content.* We will process and store Customer Content in accordance with our Enterprise privacy commitments. We will only use Customer Content as necessary to provide you with the Services, comply with applicable law, and enforce OpenAI Policies. We will not use Customer Content to develop or improve the Services.

# Representations and Warranties

11.2 Additional Provider Warranties. Provider represents and warrants to Customer that:

▲ (a) Provider has, and throughout the Term and any additional periods during which Provider does or is required to perform the Services will have, the unconditional and irrevocable right, power, and authority, including all permits and licenses required, to provide the Services and grant and perform all rights and licenses granted or required to be granted by it under this Agreement;

(b) neither Provider's grant of the rights or licenses hereunder nor its performance of any Services or other obligations under this Agreement does or at any time will: (i) conflict with or violate any applicable Law, including any Law relating to data privacy, data security, or Personal Information; (ii) require the consent, approval, or authorization of any governmental or regulatory authority or other third party; or (iii) require the provision of any payment or other consideration by Customer or any Authorized User to any third party, and Provider shall promptly notify Customer in writing if it becomes aware of any change in any applicable Law that would preclude Provider's performance of its obligations hereunder;

(c) as accessed and used by Customer or any Authorized User in accordance with this Agreement and the Specifications, the Subscription Services, Documentation, and all other Services and materials provided by Provider under this Agreement will not infringe, misappropriate, or otherwise violate any Intellectual Property Right or other right of any third party;

# AI Provider Considerations

- Little to no control over outputs
- Outputs are dependent upon inputs
- Outputs can infringe upon third-party intellectual property rights and third-party publicity rights
- Providers do not want to subject themselves to breach of contract claims and damages

# OpenAI Business Terms

## 9. Warranties; Disclaimer

**9.1 Warranties.** We warrant that, during the Term, when used in accordance with this Agreement, the Services will conform in all material respects with the documentation we provide to you or otherwise make publicly available.

**9.2 Disclaimer.** Except for the warranties in this Section 9, the Services are provided “as is” and we and our affiliates and licensors hereby disclaim all warranties, express or implied, including all implied warranties of merchantability, fitness for a particular purpose and title, noninfringement, or quiet enjoyment, and any warranties arising out of course of dealing or trade usage. Despite anything to the contrary, we make no representations or warranties (a) that use of the Services will be uninterrupted, error free, or secure, (b) that defects will be corrected, (c) that Customer Content will be accurate, or (d) with respect to Third Party Offerings.

# Indemnification

12. Indemnification. Provider (the "**Indemnifying Party**") shall indemnify, defend, and hold harmless Customer and each of Customer's Affiliates, and its and their respective officers, directors, employees, agents, successors, and assigns (each of the foregoing Persons, a "**Customer Indemnitee**" from and against any and all Losses resulting from any Action by a third party that arise out of or result from, or are alleged to arise out of or result from: (a) breach of any representation, warranty, covenant, or obligation of Provider under this Agreement; (b) Provider's violation of any Law; or (c) any claim that the Subscription Services, or Customer's use thereof, infringes any right of any third party.)

# AI Provider Considerations

- Outputs can infringe intellectual property rights
- Outputs can infringe publicity rights
- Outputs may contain third-party materials
- Outputs may be biased or inaccurate
- Significant litigation between content owners and foundation model developers
  - No guarantee that deployers and users will not be eventual targets of litigation



# OpenAI Business Terms

## 10. Indemnification

10.1 *By Us.* We agree to defend and indemnify you for any damages finally awarded by a court of competent jurisdiction and any settlement amounts payable to a third party arising out of a third party claim alleging that the Services (including training data we use to train a model that powers the Services) infringe any third party intellectual property right. This excludes claims to the extent arising from: (a) combination of any Services with products, services, or software not provided by us or on our behalf, (b) fine-tuning, customization, or modification of the Services by any party other than us, (c) the Input or any training data you provide to us, (d) your failure to comply with this Agreement or laws, regulations, or industry standards applicable to you, or (e) Customer Applications (if the claim would not have arisen but for your Customer Application). If we reasonably believes that all or any portion of the Services is likely to become the subject of any infringement claim, we (x) will procure, at our expense, the right for you to continue using the Services in accordance with this Agreement, (y) will replace or modify the allegedly infringing Service so it is non-infringing, or (z), if (x) and (y) are not commercially practicable, we may, in our sole discretion, terminate this Agreement upon written notice to you and refund any prepaid amounts for unused Services. You will promptly comply with all reasonable instructions we provide you with respect to (x) through (y) above, including any instruction to replace, modify, or cease use of an impacted Service.

10.2 *By Customer.* You agree to indemnify, defend, and hold us and our affiliates and licensors harmless against any liabilities, damages, and costs (including reasonable attorneys' fees) payable to a third party arising out of a third party claim related to (a) use of the Services in violation of this Agreement (including violation of OpenAI Policies), (b) Customer Applications (if any), or (c) Input.

# How Privacy Legal Requirements Can Be Incorporated Into AI Contracts

# General Privacy Issues Arising with AI



- Privacy Notice Consents
- Right to withdraw consent
- Data minimization requirements
- Data Protection Impact Assessments
- Vendor Management
- Sensitive data collection opt-in requirements

# When we think about AI and privacy, consider:



How is data flowing into the artificial intelligence?  
How is data flowing out of the artificial intelligence?



What will the AI user provide to the AI when licensing an AI product?

# Privacy Laws that address AI

- GDPR
- CCPA
- Virginia, Colorado, Connecticut privacy laws
- Florida, Texas, Montana, Tennessee, Indiana privacy laws
- Sector-specific laws, such as the New York law regulating Automated Employment Decision Tools



# GDPR Article 22

---

- GDPR includes specific requirements for automated decision-making that has legal or similarly significant effects on data subjects
- Permitted only where the decision is
  - Necessary for the performance of a contract,
  - Authorized by domestic law applicable to the controller, or
  - Where the data subject has provided explicit consent

# GDPR

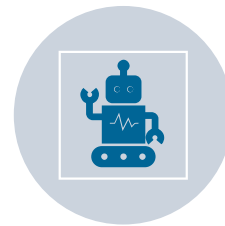
## Article 22

- If processing activities fall under Article 22, must
  - Determine which of the three bases for processing applies
  - Conduct a data protection impact assessment to identify risks and determine how they will be mitigated
  - Provide data subjects with information about the processing, including the personal data used, why it is used, and what the effects might be
  - Establish a mechanism for data subjects to request reconsideration of an automated decision

# Types of AI Data that May Include Personal Data



**Foundational Training Data:** an extremely large data set



**Training Data:** Make your AI tool specialized for you



**Input Data:** Information/prompts from you to the AI that the AI needs in order to respond to your specific experiences



**Output Data:** Something that did not exist beforehand that comes out of the AI

All need to be considered when drafting privacy provisions



# **Data Processing Addendums: How is AI Data Implicated?**

## Key Definitions: Sample Provision

*Personal Data:* Any information relating to an identified or identifiable natural person (*Data Subject*)

*Services:* Processing services provided by the Processor to the Controller and described under subject matter of the processing in Annex 1 of this DPA

*Processing:* Any operation performed on personal data, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Training data

Input data

Output data

## Key Definitions: How is AI Data Implicated?

- **Training data:** Can the model be trained using only anonymized, pseudonymized, or aggregated data?
- **Input data:** Can personal data be excluded from the input data, or minimized where feasible?
- **Output data:** If the input data included personal data, the output data will likely include personal data as well. Consider also that inferences derived from personal data are considered personal data under CCPA.

# Sensitive Data Collection

- GDPR prohibits the use of automated decision-making technologies to process special categories of personal data unless the data subject has provided consent, or the processing is necessary for reasons of substantial public interest under EU or Member State law.
- Colorado Privacy Act Regulations require controllers to describe in their privacy notice the impact of the use of sensitive data for profiling.
- Some U.S. laws require opt-in consent for the processing of sensitive data generally

# Sensitive Data Collection: Sample Provision

In addition to all other requirements applicable to Personal Information, if Supplier processes any “Sensitive Personal Data” or “Sensitive Data” as defined under the Data Protection Laws, Supplier will comply with all additional instructions relating to such Sensitive Personal Data that may be provided by Customer to Supplier, and agrees to timely carry out any requests to limit use and disclosure of Sensitive Personal Data that may be made to Customer by consumers.

Input data

Output data

# Sensitive Data Collection: How is AI Data Implicated?

- **Input data:** If GDPR applies, do you have a lawful basis for the use of AI tools to process special categories of data? If applicable, do you have consent from the data subject for the processing of sensitive data?
- **Output data:** Does your privacy notice describe how the output from sensitive data processing will be used?

# Consumer Rights Requests

- Right to know, Right to opt out, Right to delete, Right to object among rights that could be implicated
- Most of the current U.S. state privacy laws provide individuals an opportunity to opt out of profiling in connection with decisions related to insurance, lending services, housing, or other similarly impactful decisions.

# Consumer Rights Requests: Sample Provision

Data Subject requests. Supplier shall promptly:  
notify Company if it receives a request from a data subject under Data Protection Laws in respect of Personal Data (including full details and copies of the complaint, communication or request), as well as data correction, deletion, blocking and/or Processing and provide full cooperation, assistance, and support to Company, consistent with the functionality of services or applications provided under the Contract, to comply with any data subject requests to exercise their rights under applicable Data Protection Laws. The Supplier shall not respond to the request itself, unless authorized to do so by Company;  
assist Company by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Company's obligation to respond to requests for exercising the data subject's rights.

Training data

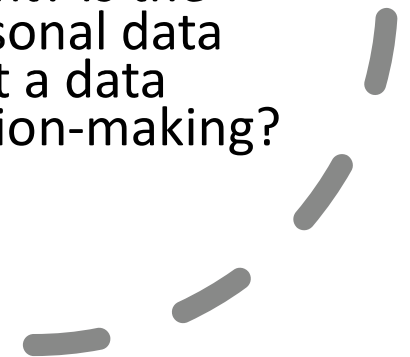
Input data

Output data



# Consumer Rights Requests: How is AI Data Implicated?

- **Training data:** Was personal data used as part of the training data? Is training data able to be extracted and then deleted or corrected after it is provided to the model for training? Is the service provider able to provide a copy of personal data used to train the model in the event of a consumer rights request?
- **Input data:** Was personal data used as part of the input data? Is input data able to be extracted and then deleted or corrected after it is inputted into the AI model? Can you access records of inputs to provide in connection with a data subject access request where relevant? Is the service provider able to remove personal data from the input data in the event that a data subject opts out of automated decision-making?



# Consumer Rights Requests: How is AI Data Implicated?

- **Output data:** When outputs are generated, is personal data included as part of the output? Is input data able to be extracted and then deleted or corrected after it is received from the AI? Do you have processes in place to stop the processing of personal data using AI tools in the event a data subject opts out of automated decision-making?



## Records of Processing Activities: Sample Provision

If applicable, Supplier shall maintain a record of its Processing activities conducted for and on behalf of Company. Such a record shall contain: (i) the categories of Processing carried out on behalf of Company; (ii) details of EU/EEA Restricted Transfers or UK Restricted Transfers of Personal Data including the identification of the country or international organization that the Personal Data is transferred to and record of the safeguards the Supplier has put in place to ensure that the transfer will be in accordance with Data Protection Laws. The Supplier shall make this record available to Company within 48 hours of receiving such a request.

Input data

Output data

# Records of Processing Activities: How is AI Data Implicated?

- **Input data:** If input data contains personal data, the details of processing should be included in Article 30 records
- **Output data:** If the output data is considered Article 22 profiling with legal or similar effects, the basis for processing should also be documented in records

# Data Retention: Sample Provision

Return of Personal Data and Termination. Supplier shall, within thirty (30) days of termination of the Contract, or if requested during the term of the Contract, cease all Processing of Personal Data and return to Company all copies of Personal Data. In lieu of returning copies, Company may, at its sole discretion, require Supplier to destroy all copies of Personal Data, using agreed upon methods to ensure such Personal Data is not recoverable, and certify to such destruction. Supplier may continue to retain Personal Data beyond the period prescribed in this section above where required by law, or in accordance with the Contract and/or applicable regulatory or industry standards, provided that (i) Supplier notifies Company prior to the Contract's termination or expiration of the obligation, including the specific reasons for such retention; (ii) Supplier has a documented retention period and secure deletion procedure for such copies, with back-up copies retained only to the end of their legally required retention period; (iii) following such period, all copies and back-up copies are deleted in such a manner that they are not recoverable; (iv) Supplier performs no Processing of Personal Data other than that necessitated by retaining or deleting the relevant copies; and (v) Supplier continues to comply with all the requirements of this DPA in relation to any such retained Personal Data until the same is securely deleted. Termination or expiration of the Contract for any reason shall not relieve the Supplier from obligations to continue to protect Personal Data in accordance with the terms of the Contract, this DPA and applicable law.

Training data

Input data

Output data

# Data Retention: How is AI Data Implicated?

- **Training data:** Can personal data be deleted once training is complete? If it is not feasible to delete immediately, can a periodic review process for deletion be implemented?
- **Input data:** Can personal data be deleted promptly after the input data is processed? If it is not feasible to delete immediately, can a periodic review process for deletion be implemented?
- **Output data:** Can output data be deleted after the processing purposes is achieved? If the processing involves long-term use, such as profiling, can a periodic review process for deletion be implemented?

# Data Protection Impact Assessments

- Article 35 of GDPR requires a DPIA “where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.”
- Many U.S. state laws also require a DPIA when the processing activities will include “profiling” that leads to a reasonably foreseeable risk of harm.

# Data Protection Impact Assessments: Sample Provision

The Processor shall assist the Controller with any Data Protection Impact Assessment as required by Art. 35 of the GDPR that relates to the Services provided by the Processor to the Controller and the Personal Data processed by the Processor on behalf of the Controller.

Input data



# Data Protection Impact Assessments: How is AI Data Implicated?

- **Input data:** Before processing, determine whether the intended use triggers a requirement to conduct a DPIA under applicable law

# Privacy Notice Requirement

- Article 13 of GDPR requires information on the processing to be provided to the data subject, including the purposes of the processing for which the personal data are intended, the legal basis for the processing, and the existence of automated decision-making, including profiling, that produces legal effects for the data subject and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

## Privacy Notice Requirement: Sample Provision

Controller will provide data subjects with appropriate notice of the processing in accordance with Data Protection Laws, including the use of automated decision-making technologies (“ADMT”), information about the logic of the ADMT, and the potential effect of the processing on the data subject.

Training data

Input data

Output data

# Privacy Notice: How is AI Data Implicated?

- **Training data**: Does your privacy notice describe how personal data is used to train the AI model?
- **Input data**: Does your privacy notice describe how personal data is used as input data?
- **Output data**: Does your privacy notice describe how the resulting output data will be used?

# Requirement for Cross- Border Transfer Mechanism: Sample Provision

- **Controller to Processor:**
  - To the extent Controller Transfers Personal Data from the European Economic Area, Supplier commits to enter into the EU Standard Contractual Clauses. To the extent applicable, the executed EU Standard Contractual Clauses form part of the terms and conditions of the Contract and this DPA and is entered between Controller and Processor. Where the Transfer to Processor is covered by Processor's BCR and/or the Data Privacy Framework (DPF) Program, Processor warrants that it shall (i) maintain it in good standing for the duration of the services provided under the Contract, (ii) promptly notify Controller of any subsequent material changes in such authorization/certification, and (iii) enter into an appropriate onward transfer agreement with any such sub-processor, or by entering into SCCs, in each case providing the same or more protection than the terms in this DPA."
  - Processor agrees to provide additional information as it may be required by applicable Data Protection Law and execute the data transfer impact assessment during its on-boarding process. Processor agrees and acknowledges that the data transfer impact assessment questionnaire completed during its on-boarding process is deemed incorporated in this DPA or other applicable country-specific cross-border data transfer agreements executed between the parties.

Training data

Input data

Output data

# Requirement for Cross- Border Transfer Mechanism: Sample Provision


Onward Transfers by Processor: To the extent that Processor engages third parties in an arrangement that involves an EU/EEA Restricted Transfer, Switzerland Restricted Transfer or a UK Restricted Transfer, Processor shall ensure that an adequate safeguard is in place between the Processor and the third party to protect the transferred Personal Data in compliance with Data Protection Laws. Processor shall make available evidence of such safeguard to Controller on reasonable request.”

Training data

Input data

Output data

## Requirement for Cross- Border Transfer Mechanism: How is AI Data Implicated?

- **Training data:** Will training of the model involve any international transfers of personal data?
  - **Input data:** Where is the service provider located? Will the service provider make any onward transfers of personal data to subprocessors?
  - **Output data:** Will the use of the output data involve any international transfers of personal data?
- 

## Vendor Management: Sample Provision

Processor shall implement and maintain policies and programs ensuring that its employees, agents, contractors, and permitted sub-contractors that have access to Controller Personal Data receive regular security, privacy and data classification awareness and training. Processor's training and awareness program shall contain training on how to implement and comply with its enterprise IT cybersecurity and privacy programs and how to protect Controller's Personal Data. Cybersecurity training, including new threats and vulnerabilities, shall be required for all Processor developer and system administration staff supporting Processor systems Processing Controller Personal Data. All development staff should be trained on secure coding principles and best practices.

Processor shall implement appropriate measure to ensure that its employees, agents, contractors and permitted sub-contractors that have access to Controller Personal Data are bound by the terms of a written confidentiality or non-disclosure agreement that commits such parties to adhere to security requirements no less protective than those set forth in the Contract and this DPA. Such confidentiality or non-disclosure agreement shall in no way limit Processor's liability for the disclosure, use, or misuse of any Controller Personal Data by any such employees, agents, contractors and permitted sub-contractors.

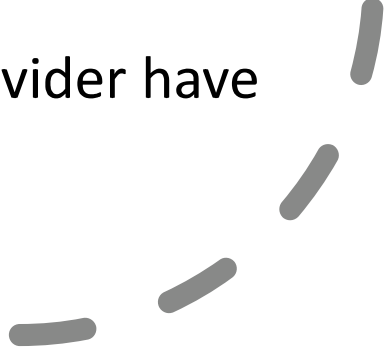
Training data

Input data

Output data



## Vendor Management: How is AI Data Implicated?

- **Training data:** Will third parties have access to training data? Will training data be accessible to other customers?
  - **Input data:** Does the service provider reasonably limit internal access to input data? Will input data be accessible to other customers?
  - **Output data:** Will the service provider have unlimited access to output data?
- 

## Requirement to Identify Lawful Basis of Processing: Sample Provision

Controller agrees to (i) determine the means and purposes of Processor's Processing of Controller Personal Data in accordance with the Agreement and this DPA; and (ii) maintain responsibility for accuracy, quality, and legality of Controller Personal Data and the means by which Controller acquired Controller Personal Data. Controller shall have sole responsibility for obtaining any and all relevant agreements, authorizations, consents, instructions or permissions for the Processing of Controller Personal Data from Data Subjects for Processor to process Controller Personal Data on Controller's behalf. Controller shall have sole responsibility for the accuracy, completeness, format, and legality of Controller Personal Data.

Training data

Input data

# Requirement to identify lawful basis of processing: How is AI Data Implicated?

- **Training data:** Have you identified a lawful basis for using personal data to train the model?
- **Input data:** Have you identified a lawful basis for processing the data using the AI tool? If GDPR Article 22 applies, have you identified a basis for the use of automated decision-making with legal or similar effects?

## **Limitation of Liability (DPAs): Sample Provision**

Any liability arising out of or in connection with this DPA shall follow, and be exclusively governed by, the liability provisions set forth in, or otherwise applicable to, the Services Agreement. Therefore, and for the purpose of calculating liability caps and/or determining the application of other limitations on liability, any liability occurring under this DPA shall be deemed to occur under the Services Agreement.

## **Limitation of Liability (DPAs): Sample Provision**

In addition to any exceptions to any limitations of liability in the Contract, such exceptions shall be amended to add the following: Notwithstanding anything to the contrary in the Contract, any limitation on Processor's liability will not apply to (a) Processor's indemnification obligations under this DPA, (b) Processor's gross negligence or willful misconduct, (c) claims and incurred costs relating to Processor's breach of its obligations of confidentiality hereunder, or (d) any fines, fees or assessments imposed on Controller by a third party or governmental authority as a result of Processor's actions or inactions with respect to Processor's obligations under this DPA.

# Questions?



**Maureen E. Fulton**

Shareholder

*Maureen.Fulton@koleyjessen.com*

Omaha  
402.343.3753



**Jack D.  
Horgan**

Shareholder

*Jack.Horgan@koleyjessen.com*

Omaha  
402.343.3848

# Q&A

You may use the Chat function to ask questions or email questions to [lawquestion@straffordpub.com](mailto:lawquestion@straffordpub.com).

Group Listening Code: **TLKGJD**

*Please watch for the Certification Process link to appear on your screen to complete the survey and request your certificate(s).*



*Not a Passholder Yet?*

## *Try the CLE Individual Annual Pass*

- Attend unlimited live webinars in any of our legal practice areas – we produce over 750+ advanced live CLE webinars each year
- Get unlimited access to hundreds of recorded webinars
- Get all your CLE credits for one price

**Simply respond** to the email you will receive after the program and we will rebate the cost of this webinar from the pass price!

---

Did you know that Strafford offers **volume discounts**? Add additional attendees to your next webinar order at 35% off (40% off for 5 or more).