# FAQ: GenAI Risks / Solutions

IntelAgree, LLC
Legal and Information Security Teams

## A. INFORMATION SECURITY RISKS / SOLUTIONS

### 1. Is my data secure?

At IntelAgree, we use Microsoft Azure OpenAI (MS OAI) to power the generative AI features in Saige Assist. All the data processed by MS OAI is securely stored in Microsoft Azure datacenters in the US geography, which comply with a broad range of standards including ISO, HIPAA, HITRUST, GDPR, FINRA, NIST, SOC, and CCPA. IntelAgree can provide a comprehensive list on request. The short answer is, "yes, your data is secure."

### 2. Can other people/companies see my data when stored, processed, used on MS OAI?

Prompts (inputs) and completions (outputs), things you embed, and your training data:

a. are NOT available to other customers.
b. are NOT available to OpenAI.
c. are NOT used to improve OpenAI models.
d. are NOT used to improve any Microsoft or 3rd party products or services.
e. are NOT used for automatically improving Azure OpenAI models for your use in your resource (The models are stateless unless you explicitly fine-tune models with your training data).
f. In short, your fine-tuned Azure OpenAI models are available exclusively for your use.

### 3. What data does MS OAI process?

Azure OpenAI processes the following types of data:

a. Prompts and generated content. Prompts are submitted by the user, and content is generated by the service, via the completions, chat completions, images and embeddings operations.
b. Augmented data included with prompts. When using the "on your data" feature, the service retrieves relevant data from a configured data store and augments the prompt to produce generations that are grounded with your data.
c. Training & validation data. You can provide your own training data consisting of prompt-completion pairs for the purposes of fine-tuning an MS OAI model.

### 4. How is data processed by MS OAI?

Click on this link to see a diagram that shows how data is processed:
https://learn.microsoft.com/en-us/legal/cognitive-services/openai/media/flow.png

The diagram shows:

a. How the MS OAI Service processes your prompts to generate content (including when additional data from a connected data source is added to a prompt using MS OAI on your data).
b. How the MS OAI Service creates a fine-tuned (custom) model with your training data.
c. How the MS OAI Service and Microsoft personnel analyze prompts, completions and images for harmful content and for patterns suggesting the use of the service in a manner that violates the Code of Conduct or other applicable product terms.

### 5. Does MS OAI prevent abuse and harmful content generation?

To reduce the risk of harmful use of the MS OAI, the Azure OpenAI Service includes both content filtering and abuse monitoring features. To learn more about content filtering, ask IntelAgree to provide MS OAI Service content filtering details. To learn more about abuse monitoring, ask IntelAgree to provide more details.

Content filtering occurs synchronously as the service processes prompts to generate content as described above and here. No prompts or generated results are stored in the content classifier models, and prompts and results are not used to train, retrain, or improve the classifier models.

MS OAI abuse monitoring detects and mitigates instances of recurring content and/or behaviors that suggest use of the service in a manner that may violate the Code of Conduct for Azure OpenAI Service (details at this link: code of conduct) or other applicable product terms. To detect and mitigate abuse, MS OAI stores all prompts and generated content securely for up to thirty (30) days. (No prompts or completions are stored if the Microsoft customer is approved for and elects to configure abuse monitoring off, as described below – IntelAgree has been approved for and elected this Limited Access option so none of these inputs/outputs are retained by Microsoft and Microsoft employees cannot view any of this data)

## B. CONTRACTUAL RISKS / SOLUTIONS

### 1. What are IntelAgree's obligations, and Do I have a remedy if something goes wrong?

You have a Master Software as a Service Agreement (MSA) with IntelAgree, as well as either a Data Protection Agreement (DPA) or Business Associate Agreement (BAA) or both. All three of these documents contain one or more of the following:

a. Contractual obligations from IntelAgree to you regarding Confidential Information. Confidential information is defined in the MSA to include any Customer Data - which is information you upload to or create using the IntelAgree Systems. This provides a broad obligation for IntelAgree to protect your data including how that data is used for MS OAI features/functions.
b. Data breach obligations. DPAs and BAAs contain specific contractual obligations for IntelAgree when it comes to informing you of any breach of DPA and or BAA relevant data.

c. Contractual remedies for confidentiality breach. IntelAgree's standard MSA does not limit your remedy for a claim of confidentiality breach.

d. Data breach remedies. IntelAgree's standard MSA provide specific remedy/liability for IntelAgree for data breach as defined in the relevant DPA and or BAA. In addition, IntelAgree's

Standard MSA also provides a no-limit remedy to reimburse you for specific costs related to the typical data breach. The short answer is "yes, IntelAgree has obligations to protect your data, and you have remedies if we do not meet our obligations."

**2. Does IntelAgree evaluate its vendors and have recourse against them in contracts?**

a. Yes, we do evaluate our vendors.

IntelAgree has its own in-house Information Security Team. That team has already evaluated Microsoft and specifically the use of Microsoft Azure OpenAI. Just like IntelAgree itself, we have confirmed that our vendors with access to or use of your data are SOC, HIPAA and GDPR compliant. In addition, we have DPAs and BAAs in place with these key vendors.

b. Yes, we do have recourse when needed. In the master agreements in place with vendors, as well as the DPAs and or BAAs, we have obligations and remedies between IntelAgree and its vendors that are similar to those in place between your organization and IntelAgree.

**3. Are there specific contractual obligations related to Microsoft Azure OpenAi?**

a. Microsoft's Azure data center terms and conditions apply to IntelAgree's use of Microsoft data centers in general. https://azure.microsoft.com/en-us/support/legal/

b. It is key to note that Microsoft says, "Azure OpenAI Service is made available to customers under the terms governing their subscription to Microsoft Azure Services, including the Azure OpenAI section of the Microsoft Product Terms." Microsoft calls services like Azure OpenAI "Limited Access Services", and those services have additional terms, conditions and obligations for IntelAgree and Microsoft.

c. More detail about Limited Access Services and the terms, conditions and obligations – applicable to Microsoft and IntelAgree can be found here: https://www.microsoft.com/licensing/terms/productoffering/MicrosoftAzure/EAEAS