

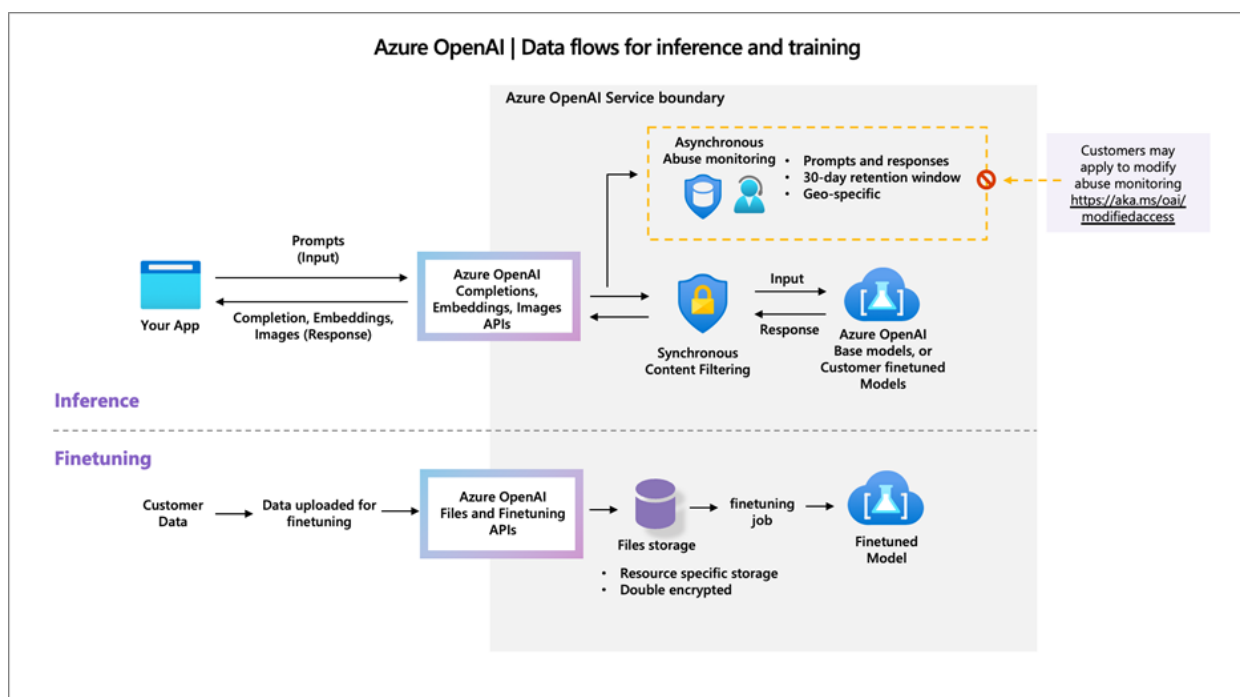
embeddings operations.

- **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.
- **Training & validation data.** You can provide your own training data consisting of prompt-completion pairs for the purposes of [fine-tuning an OpenAI model](#).

## How does the Azure OpenAI Service process data?

The diagram below illustrates how your data is processed. This diagram covers three different types of processing:

1. How the Azure OpenAI Service processes your prompts to generate content (including when additional data from a connected data source is added to a prompt using Azure OpenAI on your data).
2. How the Azure OpenAI Service creates a fine-tuned (custom) model with your training data.
3. How the Azure OpenAI 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



As depicted in the diagram above, managed customers may [apply to modify abuse monitoring](#) [↗](#).

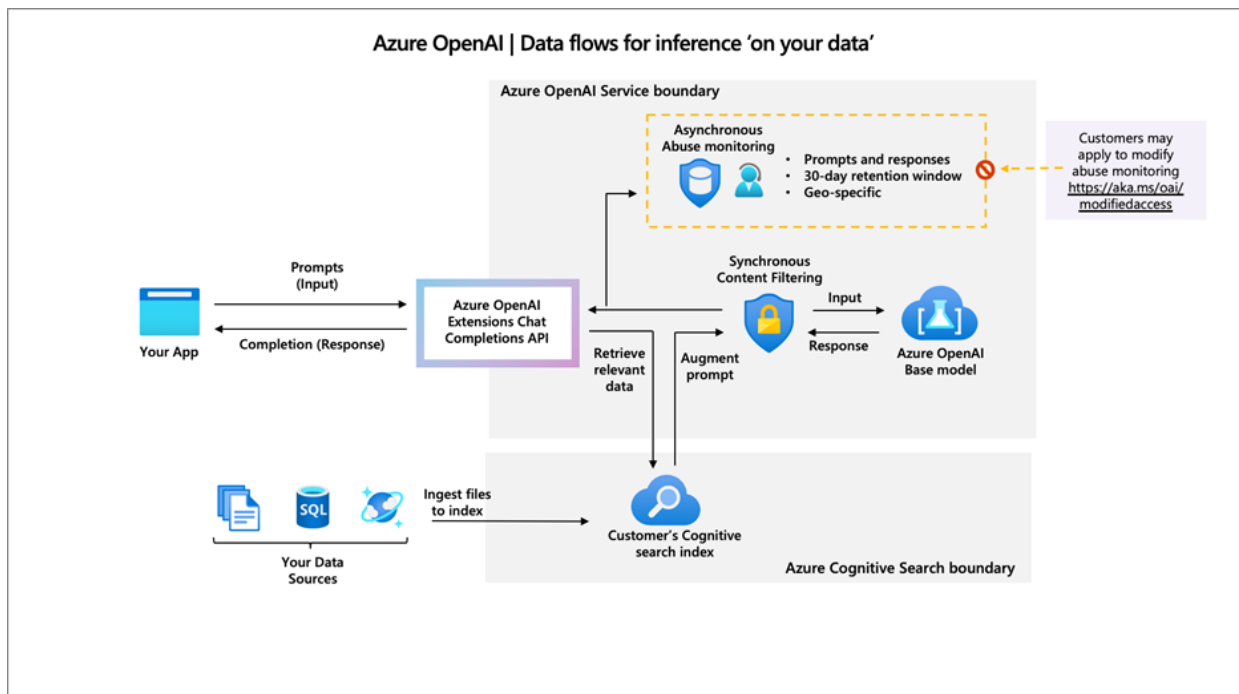
# Generating completions, images or embeddings

Models (base or fine-tuned) deployed in your resource process your input prompts and generate responses with text, images or embeddings. The service is configured to synchronously evaluate the prompt and completion data in real time to check for harmful content types and stops generating content that exceeds the configured thresholds. Learn more at [Azure OpenAI Service content filtering](#).

The models are stateless: no prompts or generations are stored in the model. Additionally, prompts and generations are not used to train, retrain, or improve the base models.

## Augmenting prompts with data retrieved from your data sources to "ground" the generated results

The Azure OpenAI "on your data" feature lets you connect data sources to ground the generated results with your data. The data remains stored in the data source and location you designate. **No data is copied into the Azure OpenAI service.** When a user prompt is received, the service retrieves relevant data from the connected data source and augments the prompt. The model processes this augmented prompt and the generated content is returned as described above.



As depicted in the diagram above, managed customers may apply to [modify abuse monitoring](#).

## Creating a customized (fine-tuned) model with your data:

Customers can upload their training data to the service to fine tune a model. Uploaded training data is stored in the Azure OpenAI resource in the customer's Azure tenant.

Training data and fine-tuned models:

- Are available exclusively for use by the customer.
- Are stored within the same region as the Azure OpenAI resource.
- Can be double [encrypted at rest](#) (by default with Microsoft's AES-256 encryption and optionally with a customer managed key).
- Can be deleted by the customer at any time.

Training data uploaded for fine-tuning is not used to train, retrain, or improve any Microsoft or 3rd party base models.

## Preventing abuse and harmful content generation

To reduce the risk of harmful use of the Azure OpenAI Service, the Azure OpenAI Service includes both content filtering and abuse monitoring features. To learn more about [content filtering](#), see Azure OpenAI Service content filtering. To learn more about abuse monitoring, see [abuse monitoring](#).

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.

Azure OpenAI 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](#) or other applicable product terms. To detect and mitigate abuse, Azure OpenAI stores all prompts and generated content securely for up to thirty (30) days. (No prompts or completions are stored if the customer is approved for and elects to configure abuse monitoring off, as described below.)

The data store where prompts and completions are stored is logically separated by customer resource (each request includes the resource ID of the customer's Azure OpenAI resource). A separate data store is located in each [region](#) [↗](#) in which the Azure OpenAI Service is available, and a customer's prompts and generated content are stored in the Azure region where the customer's Azure OpenAI service resource is deployed, within the Azure OpenAI service boundary. Human reviewers assessing potential abuse can access prompts and completions data only when that data has been flagged by the abuse monitoring system. The human reviewers are authorized Microsoft employees who access the data via point wise queries using request IDs, Secure Access Workstations (SAWs), and Just-In-Time (JIT) request approval granted by team managers. For Azure OpenAI Service deployed in the European Economic Area,

the authorized Microsoft employees are located in the European Economic Area.

## How can customers get an exemption from abuse monitoring and human review?

Some customers may want to use the Azure OpenAI Service for a use case that involves the processing of sensitive, highly confidential, or legally-regulated input data but where the likelihood of harmful outputs and/or misuse is low. These customers may conclude that they do not want or do not have the right to permit Microsoft to process such data for abuse detection, as described above, due to their internal policies or applicable legal regulations. To address these concerns, Microsoft allows customers who meet additional Limited Access eligibility criteria and attest to specific use cases to apply to modify the Azure OpenAI content management features by completing [this form](#).

If Microsoft approves a customer's request to modify abuse monitoring, then Microsoft does not store any prompts and completions associated with the approved Azure subscription for which abuse monitoring is configured off. In this case, because no prompts and completions are stored at rest in the Service Results Store, the human review process is not possible and is not performed. See [Abuse monitoring](#) for more information.

## How can a customer verify if data storage for abuse monitoring is off?

There are two ways for customers, once approved to turn off abuse monitoring, to verify that data storage for abuse monitoring has been turned off in their approved Azure subscription:

- Using the Azure portal, or
- Azure CLI (or any management API).

### ⓘ Note

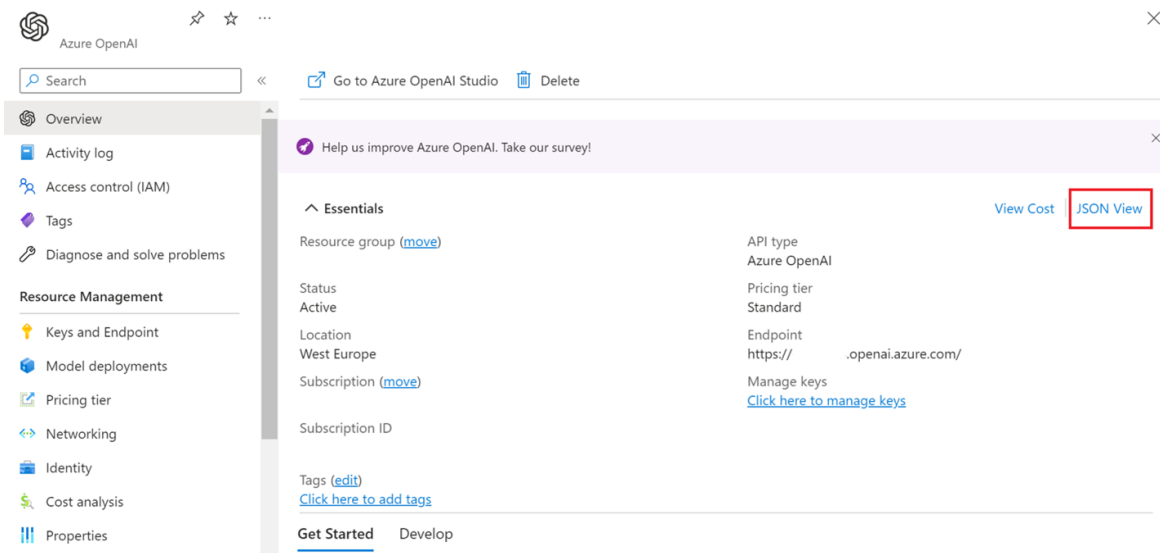
The value of "false" for the "ContentLogging" attribute appears only if data storage for abuse monitoring is turned off. Otherwise, this property will not appear in either Azure portal or Azure CLI's output.

## Prerequisites

1. Sign into Azure
2. Select the Azure Subscription which hosts the Azure OpenAI Service resource.
3. Navigate to the **Overview** page of the Azure OpenAI Service resource.

### Logging status verification using the Azure portal:

1. Go to the resource Overview page
2. Click on the **JSON view** link on the top right corner as shown in the image below.



There will be a value in the Capabilities list called "ContentLogging" which will appear and be set to FALSE when logging for abuse monitoring is off.

JSON

```
{
  "name": "ContentLogging",
  "value": "false"
}
```

### Logging status verification using the Azure CLI (or other management API):

Execute the following command in Azure CLI to see the same JSON data as shown in the Azure portal above.

Azure CLI

```
az cognitiveservices account show -n resource\_name -g resource \_group
```

To learn more about Microsoft's privacy and security commitments see the [Microsoft Trust Center](#).

# Change log

Date	Changes
23 June 2023	Added information about data processing for new Azure on your data feature; removed information about abuse monitoring which is now available at <a href="#">Azure OpenAI Service abuse monitoring</a> . Added summary note. Updated and streamlined content and updated diagrams for additional clarity. added change log

## See also

- [Limited access to Azure OpenAI Service](#)
- [Code of conduct for Azure OpenAI Service integrations](#)
- [Transparency note and use cases for Azure OpenAI Service](#)
- [Characteristics and limitations for Azure OpenAI Service](#)
- Report abuse of Azure OpenAI Service through the [Report Abuse Portal](#) ↗
- Report problematic content to [cscraireport@microsoft.com](mailto:cscraireport@microsoft.com)

