Questback IQ

Compliance and Security

Contents

Azure OpenAI Service is designed to comply with the General Data Protection Regulation (GDPR), ensuring that data is handled securely and in accordance with privacy laws. Here's how this compliance is maintained.

Data Processing and Storage

Data Handling

Azure OpenAI processes user inputs (prompts, queries) and outputs (responses) to provide the service, monitor for abuse, and improve the quality of Azure's Responsible AI systems.
https://learn.microsoft.com/en-us/answers/questions/1192849/azure-openai-data-restrictions

Data Storage

Some features, such as the Assistants API and Stored completions, may store data within the service. This data is stored at rest in the customer's Azure tenant, within the same geography as the Azure OpenAI resource.
https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy?tabs=azure-portal

Data Processing Agreement("DPA")

Questback and Microsoft DPA agreement

According to official communication from Microsoft support, Microsoft does not enter into individually signed Data Processing Agreements with customers. Instead, Microsoft has adopted a standardized Data Protection Addendum, which forms an integral part of its general contractual framework, such as the Microsoft Customer Agreement and the Online Services Terms (OST).
This standardized DPA is publicly available on Microsoft's official website and is legally binding upon Microsoft and its customers once services are consumed. The public availability of the DPA ensures transparency and allows customers to verify its authenticity and terms. No additional signature is required for the DPA to be valid and enforceable.
https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Sub-proccesor and Data Storage

See Questback Trust center for specification:
https://www.questback.com/trust-center/questback-essentials-list-of-sub-processors/

Data Retention Policies

Retention Duration

Data stored for Azure OpenAI Service features is stored at rest in the Azure OpenAI resource in the customer's Azure tenant, within the same geography as the Azure OpenAI resource.
learn.microsoft.com
https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy?tabs=azure-portal

Deletion

Customers can delete their stored data at any time.
https://www.dreaminforce.com/openai-data-policies-data-usage-retention/

Default Retention

To detect and mitigate abuse, Azure OpenAI may store prompts and generated content securely for up to 30 days. This data is encrypted both in transit and at rest and is not accessible to other customers or OpenAI.
https://learn.microsoft.com/en-us/answers/questions/2181252/azure-openai-data-retention-privacy-2025

Data Usage

Model Training

By default, data submitted through Azure OpenAI is not used to train OpenAI models.
https://openai.com/enterprise-privacy/

Security Measures

Encryption

Data is encrypted at rest and in transit to protect against unauthorized access.
https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy?tabs=azure-portal

Access Controls

Strict access controls are in place to ensure that only authorized personnel can access data.

Content abuse Monitoring

Content abuse monitoring is automatically enabled to monitoring and detect misuse (e.g., generating harmful or illegal content).

Geographical Storage

Questback ensures that prompts and completions (data) processed through Azure OpenAI are transient and not persistently stored by Microsoft. Microsoft does not store, share, or utilize customer data, including fine-tuning data, outside of Questback's subscription environment. Additionally, Diagnostic Settings capable of capturing prompts and completions are disabled, reinforcing our commitment to data confidentiality and compliance.

Data Residency

Geographical Storage

Data is stored within the same geography as the Azure OpenAI resource, ensuring compliance with regional data residency requirements.

By adhering to these practices, Azure OpenAI Service ensures compliance with GDPR, providing customers with confidence that their data is handled securely and in accordance with applicable privacy laws.

https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy?tabs=azure-portal