Zap

Zap AI

CUSTOMER BRIEF · DATA SECURITY AND DATA SOVEREIGNTY

Data security and data sovereignty

This document explains how Zap AI handles your data, where that data is stored and processed, who can access it, and the controls available to you. It is written for prospects and customers evaluating Zap AI, and for their security and procurement teams.

How Zap AI works

01 · HOW ZAP AI WORKS

Zap AI works with the Zap Data Hub platform, adding analysis, recommendations, and reporting help. It does not receive a continuous feed of your data. Instead, when a user prompts the AI, Zap sends the AI provider the data needed to answer that prompt, typically the results of a specific report or query. Zap currently uses OpenAI as its sole AI provider, under a signed Data Processing Addendum.

Prompts can come from a user in Zap's own interfaces or, when MCP access is released, from your own AI assistant connected to Zap over MCP. Both follow the same path. When you connect your own assistant, it submits prompts to Zap AI on your behalf, and those prompts are processed through OpenAI in the same way. Connecting your own AI does not change the provider on our side. Section 04 covers this in detail.

Two points matter for how you assess this. First, the AI only receives data after an administrator has enabled data access in the platform. Second, the data sent is a narrow slice per prompt, but it can contain real, sensitive data, because the purpose of the feature is to answer questions about your data.

02 · WHERE YOUR DATA IS STORED AND PROCESSED

There are three locations to understand, and we are direct about each one:

AT REST

Your data stays at rest in the Microsoft Azure region in which your instance is provisioned.

The Zap Data Hub warehouse and reporting model that hold your data remain hosted in the Microsoft Azure region in which your instance is provisioned, for example the United Kingdom or the United States.

PER-PROMPT PROCESSING

Data sent with each prompt is processed in the United States by default.

When a user prompts the AI, the data needed to answer that prompt, typically the results of a specific report or query, is sent to our AI provider for processing and a response is returned. By default, processing takes place in the United States. That data can include personal information and commercially sensitive figures.

RETENTION

AI prompts and responses are retained in Australia.

Zap keeps a copy of AI prompts and responses, including the data sent to the AI and prompts submitted by an AI assistant you connect over MCP, in its central data warehouse in Australia. This is used to operate, support, monitor, and improve the AI features, and to measure usage for billing.

We state this plainly because it matters for data sovereignty assessments. When you use Zap AI with data access enabled, the data sent with each prompt is processed by default in the United States, and retained by Zap in Australia. Your core warehouse data, at rest, stays in the Microsoft Azure region in which your instance is provisioned. Your data is not used to train the provider's general-purpose models. That is a contractual commitment. The provider may retain prompts and results for up to 30 days for abuse monitoring.

03 · WHO CAN ACCESS YOUR DATA, AND FROM WHERE

Authorised Zap personnel whose role includes querying customer usage may access the retained AI prompts and responses, including the query results. This access is role-based and spans Zap's operating locations, which currently include Australia, the United Kingdom, the United States, and South Africa, and may extend to other locations as Zap grows. We disclose this broadly on purpose, so there is no gap between what we say and what our people can do.

Where access from one country reaches data held in another, that cross-border access is covered by Standard Contractual Clauses where required, and all access is subject to confidentiality obligations and Zap's ISO 27001 certified information security management system.

04 · WHEN YOU BRING YOUR OWN AI

When MCP access is released, you will be able to connect your own AI assistant, for example Claude, ChatGPT or Copilot, to Zap over MCP. Your assistant then submits prompts to Zap AI on your behalf, within the signed-in user's permissions. MCP access will be enabled with Zap per customer rather than self-service.

On our side, nothing changes. A connected assistant follows the same path as a user in our chat: the same administrator data access controls, the same OpenAI processing under our Data Processing Addendum, and the same operational record retained in Australia. Connecting your own AI does not add a provider on our side and does not bypass any control. If this surprises you, it is worth saying directly: even when you bring your own AI, the prompts it submits to Zap are processed by OpenAI under our agreement, exactly as if you had typed them in our chat yourself.

What changes is on your side. The responses returned to your assistant are then held by your AI provider under your agreement with them. Our agreements cover the path up to the response being returned. What your assistant and its provider do with it after that point is governed by your terms with that provider, not ours.

05 · YOUR CONTROLS

You decide whether the AI gets access to your data at all:

- **Documentation-only mode.** If an administrator does not enable data access, the AI answers from product documentation only. In this mode no customer data is sent to the AI provider or leaves your environment. The same applies to an assistant connected over MCP: with data access disabled, it receives documentation-only answers.
- **Disable AI entirely.** The AI module is optional. You can run the core Zap platform without it, and disable it at any time if your data handling requirements change.

How your data flows

ZAP AI · HOW YOUR DATA FLOWS

Canonical reference. The data security one-pager and the Privacy Policy both describe what is shown here.

Your environment · the Microsoft Azure region in which your instance is provisioned

Your data is stored at rest in the Microsoft Azure region in which your instance is provisioned. It stays here unless you use AI features with data access enabled.

Source databases
Your ERP and business systems

→

Data warehouse
Data pulled in and transformed

→

Reporting model
The semantic layer your reports are built from

↓

An admin must enable AI data access

No data is sent to the AI until an administrator allows it through the platform. This applies equally to an assistant you connect over MCP.

Documentation-only mode

No data access. No customer data leaves region.

↓

When a user prompts the AI

1. The user asks a question or asks the AI to do something, or your own AI assistant, connected over MCP, submits a prompt on the user's behalf.
2. The AI requests the data needed to answer that prompt, typically the results of a specific report or query.
3. Zap sends that data, a narrow slice each time, but containing real data.

The results can include personal data and commercially sensitive figures, because the AI answers questions about your data.

↓ ENCRYPTED IN TRANSIT (TLS)

AI processing · OpenAI, United States by default

OpenAI processes the request and returns a response. Zap currently uses OpenAI as its sole AI provider, under a signed Data Processing Addendum with EU Standard Contractual Clauses and the UK addendum.

Not used to train general-purpose models • Not made public • Not shared with other customers

Encrypted in transit and at rest.
Prompts and results may be retained up to 30 days for abuse monitoring.

Where your own AI is connected · your provider, your terms

The response returns to your assistant. From that point it is held by your AI provider, for example Anthropic, OpenAI or Microsoft, under your agreement with them. Zap's agreements cover the path up to this box.

↓ RESPONSE RETURNED TO THE USER OR TO YOUR CONNECTED ASSISTANT

Retained by Zap · Australia

A copy of AI prompts and responses, including the data sent to the AI, is retained in Zap's central data warehouse in Australia. It is used to operate, support, monitor and improve the AI features, and to measure usage.

Who can access it

Authorised Zap personnel whose role includes querying customer usage may access this data.

Access is role-based across Zap's operating locations, which may change over time.

Cross-border access covered by Standard Contractual Clauses (SCCs) where required.

Your controls

Run AI in documentation-only mode, so no customer data is sent anywhere.

Or disable the AI module entirely and use the core Zap platform on its own.

When released, connecting your own AI over MCP is enabled with Zap, per customer. The same data access controls apply to it.

You decide whether AI gets data access at all.

This reference describes Zap AI at general availability. What the AI can request depends on what your administrator enables.

Common questions

06 · COMMON QUESTIONS

QUESTION	ANSWER
What data does the AI actually receive?	The data needed to answer each prompt, typically the results of a specific report or query. Not a bulk feed of your warehouse. That data can contain real, sensitive information.
Is data encrypted in transit and at rest?	Yes. Data sent to and from the AI provider is encrypted in transit using TLS. Data at rest in the Zap warehouse and in the AI provider environment is encrypted.
Is my data made public?	No. Data sent through the AI provider is not public, and is not shared with other Zap customers or other organisations.
Is my data used to train general-purpose AI models?	No. Under OpenAI's API terms and the Data Processing Addendum Zap has signed, data submitted through the API is not used to train OpenAI's general-purpose models. This is a contractual commitment.
Can I use AI without sending it my data?	Yes. In documentation-only mode the AI answers from product documentation and receives no customer data. An administrator controls whether data access is enabled.
What contracts and safeguards are in place?	A signed Data Processing Addendum with OpenAI that includes the EU Standard Contractual Clauses and, where applicable, the UK International Data Transfer Addendum.
If I connect my own AI (Claude, ChatGPT or Copilot), does OpenAI still process my data?	Yes. Your assistant submits prompts to Zap AI, and Zap AI processes them through OpenAI under our agreement, exactly as if you typed the prompt in our chat yourself. We say this directly because it is the part most people do not expect.
Whose terms cover the data once it is back with my assistant?	Yours. Our agreements cover the path up to the response being returned to your assistant. What your assistant and its provider retain or do with it after that is governed by your agreement with that provider.

For specific security or data protection questions, your Zap account manager can arrange a more detailed response from our team.