OTTAVIO

Data security and privacy

How Ottavio works with your company's information



Ottavio is an AI teammate that lives in your Slack, Teams, Discord, or WhatsApp and connects to your tools. To do its job well it needs to see company information. This document explains **what it sees, what it doesn't, where it's stored, who can access it, and how you stay in control** at all times.

1. The principle: your data stays yours

- **I query, I don't copy.** I ask your tools when I need something (a figure, an alert) and keep only what I produce: the daily report, alerts and answers. I don't keep replicas of your CRM or your database.
- **Read-only, least privilege.** Every connection has read-only permissions and covers only what the agreed task requires.
- **You decide and you can revoke.** Any access can be removed in one click from your own tool, without depending on us.

2. How I connect to your tools

- **SaaS tools** (HubSpot, Salesforce, Notion, Asana, Google Workspace…): through OAuth with read-only permissions. You authorize, you revoke.
- **Your own databases:** through a read-only user that only sees a few **views** prepared by your team, with figures and without sensitive columns (no emails, phone numbers or ID documents). You choose what I see.
- **Meetings:** I read the notes and transcripts of the meetings you choose to share with me.
- **No passwords in chat.** Credentials are authorized through OAuth or configured securely, never typed into a conversation.

3. Personal data: the bare minimum

- Your customers' personal data **never appears in a channel**. If an authorized person needs it, they receive it privately through a **temporary link** that expires and logs who opens it.
- When nobody needs to be identified, I work with **aggregated figures** or **pseudonymized** data before sending anything to the AI model.
- Everyone sees only what **their role** allows.

4. What I keep and for how long

- **Default retention: 90 days.** The conversations, reports and alerts I produce are deleted automatically after that period. You can shorten it to 30 days or set whatever you need.
- **Configuration:** what you've taught me (people, alerts, tone, rules) is kept for as long as the service runs, so I can keep working.
- **When the service ends** we delete all your information and give you a **certificate of deletion**. Before that, we export it for you on request.

5. Who can access your information

- **Encrypted credentials** in a separate store, isolated per customer.
- **Nobody on the Ottavio team reads your content by default.** If it is ever needed for support, it happens only with your explicit permission and is logged.
- **Audit log:** a record of what I queried, when and for whom. You can request it at any time.
- **Isolation:** each customer's data is kept separate from everyone else's.

6. Inside your chat

- **A person approves** what matters before it's published (for example, the daily report).
- **Every figure is checked** against its source before it goes out. If it doesn't add up, it doesn't go out.
- **I only answer authorised users** in your company and ignore third-party instructions that try to manipulate me.
- **Rules that can't be switched off:** no personal data in channels, no invented figures, no investment advice.

7. The artificial intelligence model

- I run on **Claude by Anthropic**, through its **enterprise API**. By contract, data sent through the API is **not used to train models**.
- For companies that need it, I can use Claude **through Amazon Web Services in a European region** (AWS Bedrock), so processing stays within AWS infrastructure in Europe.

8. Three ways to install me

Tier	Where I run	Who it's for
Cloud	Ottavio servers in the European Union, with each customer isolated.	Teams that want to get started quickly.
Dedicated	A server just for your company, in the European Union.	Companies with stricter security requirements.
In your cloud	Inside your own infrastructure (AWS, Azure, Google Cloud…). Your data never leaves the building.	Regulated sectors: finance, health, public sector.

9. Compliance and contracts

- **GDPR.** You are the data controller and Ottavio acts as **data processor** (Art. 28), under a signed **data processing agreement (DPA)**.
- **List of sub-processors** (hosting, AI model provider) available and kept up to date; we notify you before any change.
- **Non-disclosure agreement (NDA)** on request.
- **Incidents:** should any security incident affect you, we notify you **without undue delay** so you can meet your own obligations.

More questions? Write to **hola@ottavio.bot** or ask Ottavio at **ottavio.bot**.