TWD TalkWithData

The AI that knows your company.

Presentation, Privacy and Data Protection Policy and Terms of Use

Edition of November 18, 2026
Version of the legal texts: v42
KGPX Serviços Administrativos LTDA · CNPJ 23.543.381/0001-50
talkwithdata.ai

LETTER FROM THE FOUNDER

The AI that knows your company.

This document brings together, in a dated edition, what TalkWithData is and the rules by which it treats the data of the people who use it.

I built TalkWithData so that a company can talk to its own data without losing control of it. Each person reads only what the organization decided they may read, and what the company teaches the agent stays with the company.

The Privacy and Data Protection Policy and the Terms of Use that follow are the texts in force on this date. They say what we do with data and what we never do with it. The version that applies is always the one published at talkwithdata.ai, and this copy records the date it was issued.

Questions about privacy reach me at contact@talkwithdata.ai.

Guilherme Favaron

Guilherme Favaron
Founder and Data Protection Officer
KGPX Serviços Administrativos LTDA (TalkWithData)
Campinas, November 18, 2026

Contents

Part I. The product

Part II. Privacy and Data Protection Policy

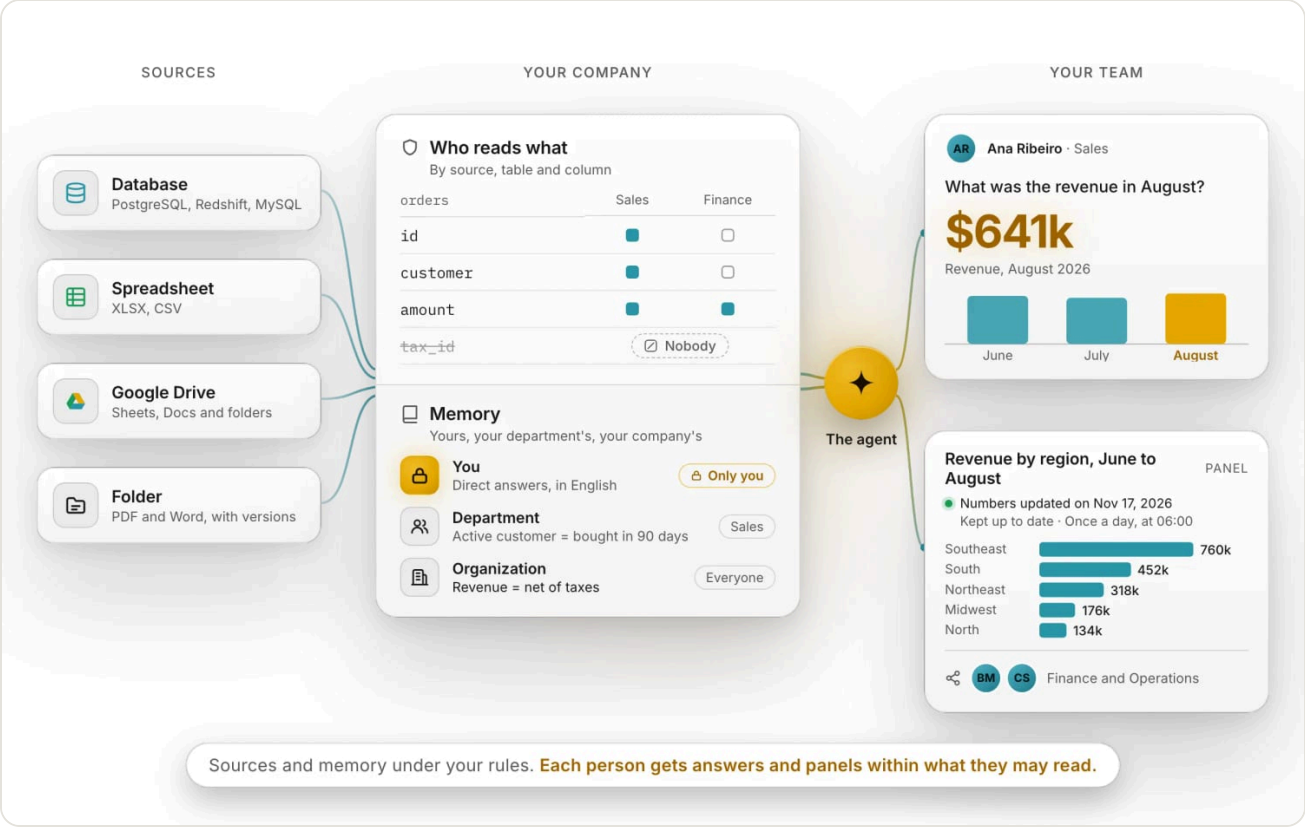
Part III. Terms of Use

Part IV. Subprocessors on the date of this edition

The AI that knows your company.

Data, documents and memory, each person reading only what they may.

Connect databases, spreadsheets, documents and Google Drive, and ask in plain language. Answers arrive as charts and panels that follow your company's rules and knowledge.

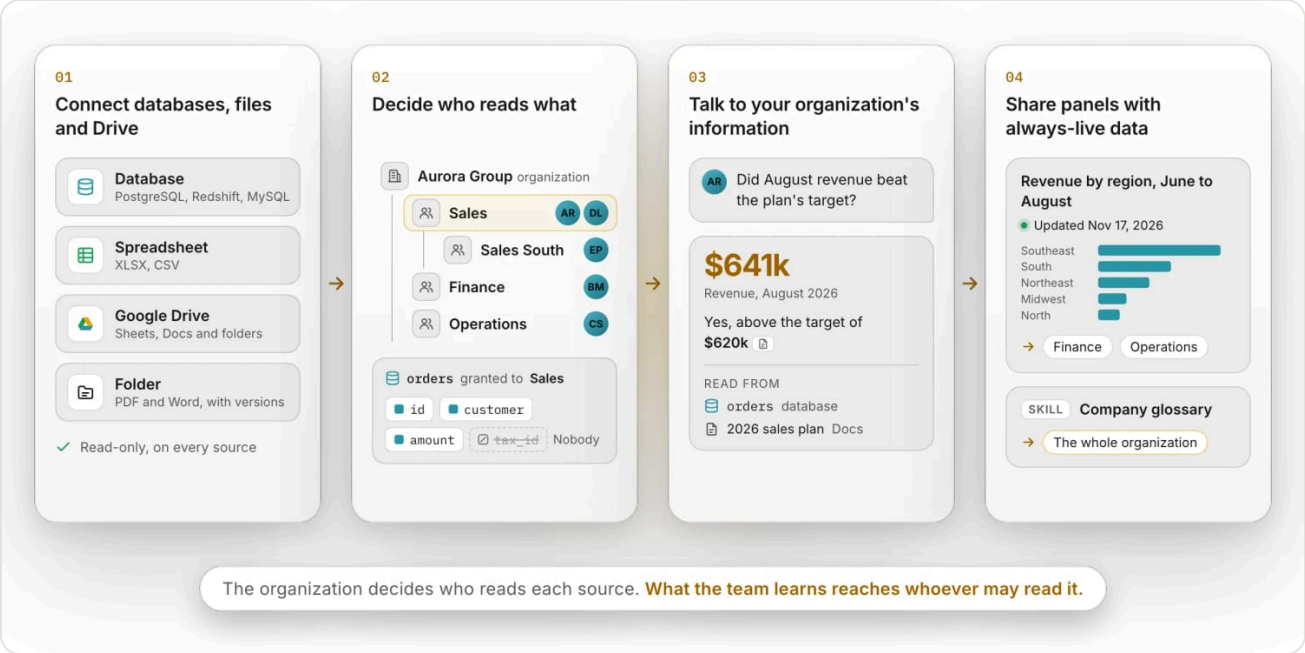


This presentation is informative and is not part of the Terms of Use.

HOW IT WORKS

From your data to your team in four steps

1. Connect databases, files and Drive
2. Decide who reads what
3. Talk to your organization's information
4. Share panels with always-live data

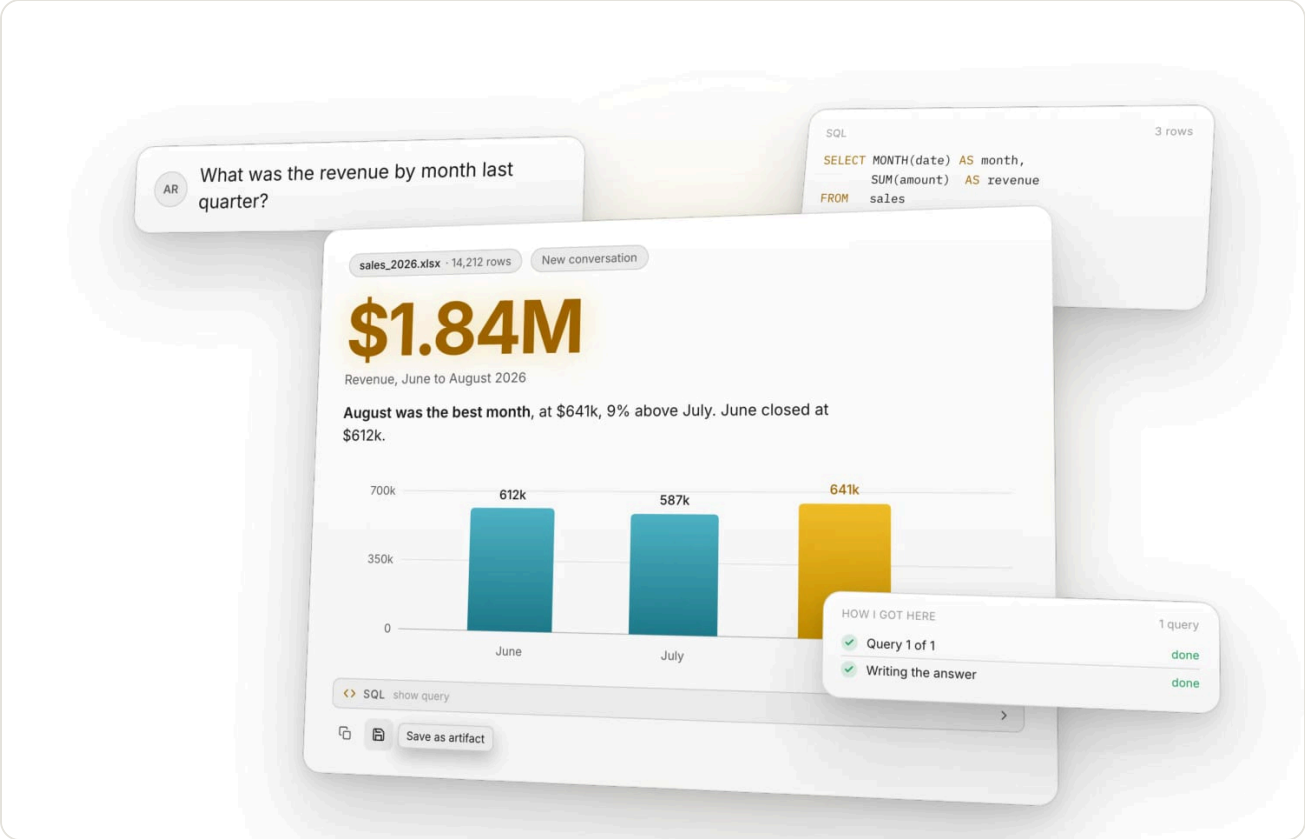


TRUST

Numbers you can trust

Every answer comes from a query that ran over your rows. Every number shows where it came from, and one that could not be checked carries a mark that says so.

- The source is read and described before the first question.
- The query only reads, and it sits one click under the answer.
- A query that fails is fixed and run again, and the steps show what was tried.
- Charts are drawn from the rows, never from a number the model wrote.
- A number taken from a document carries the document mark, so you know where it came from.

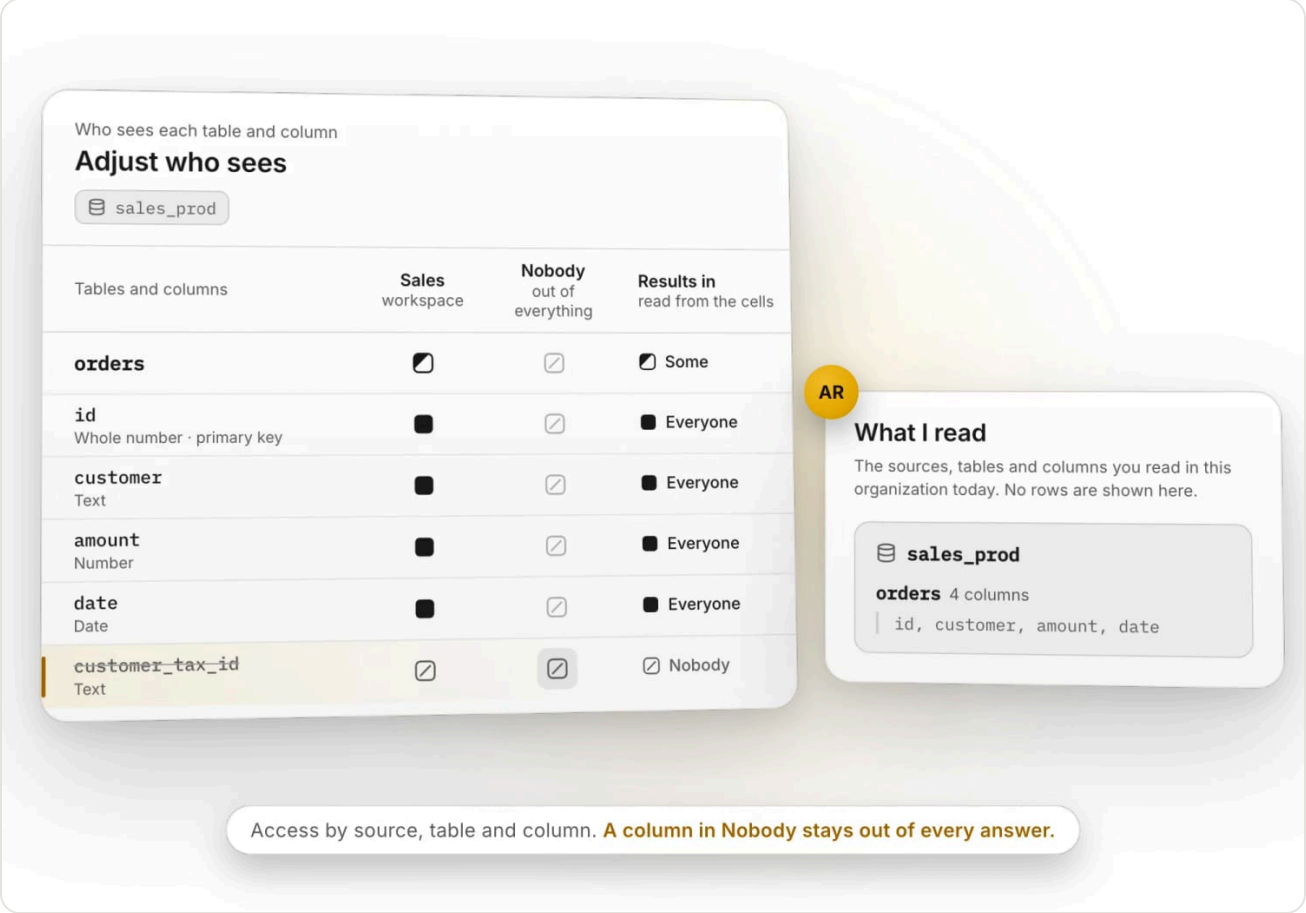


GOVERNED DATA

Your data, under your rules

Connect PostgreSQL, Redshift or MySQL, upload spreadsheets and folders, and link Google Drive. Then decide who reads each source, table and column, by workspace or by person.

- Google Drive, read-only, with Sheets, Docs and folders: TalkWithData reads only what each person picks and never writes to the Drive.
- Documents are context for the analysis, never a table.

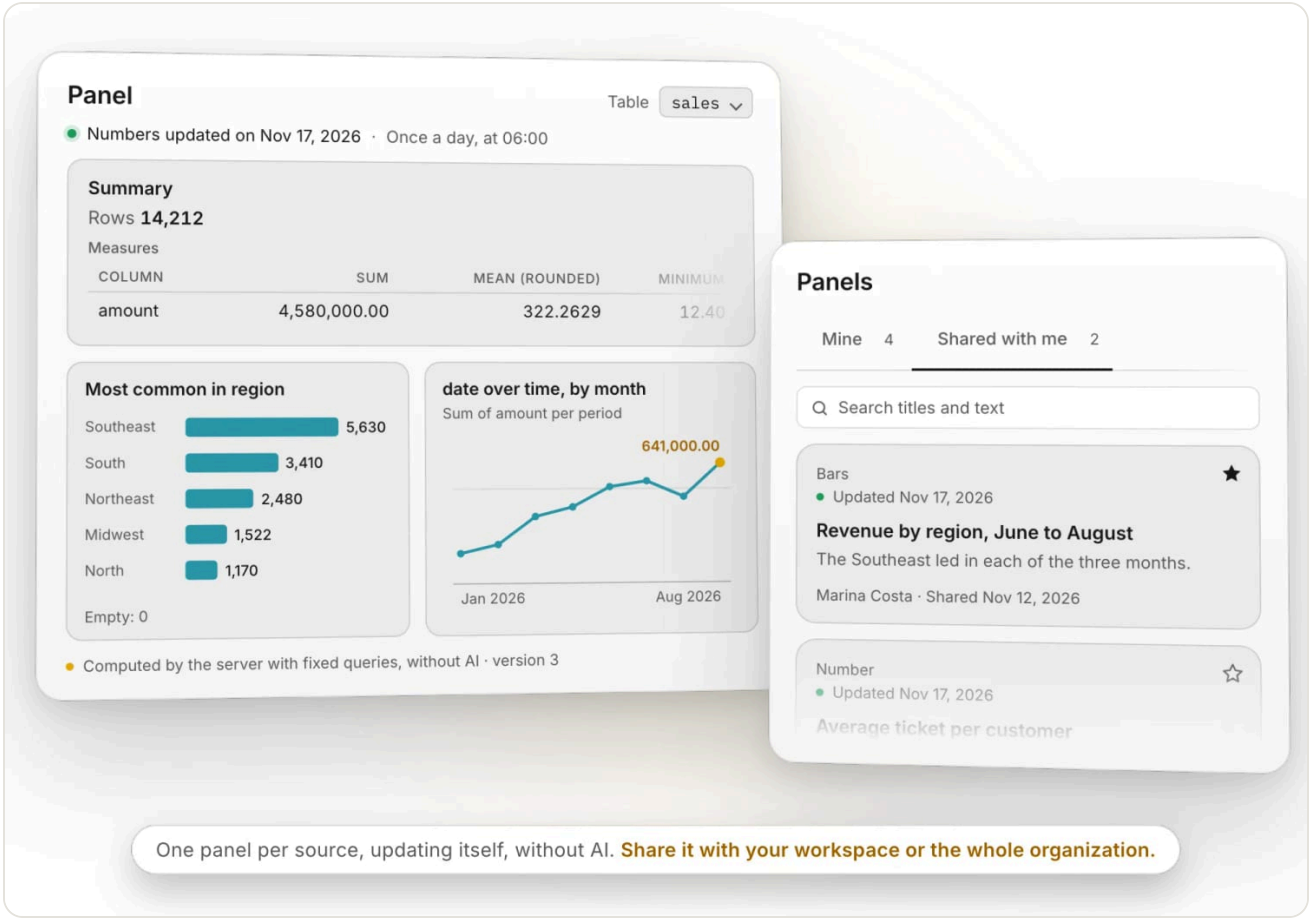


PANELS

Share the panel, not the spreadsheet

Each source gets a panel computed from the rows, with no AI in between. Save an answer and share it with your workspace or the whole organization.

- Panels that update themselves without AI, on open or once a day.
- A library with favorites and search.

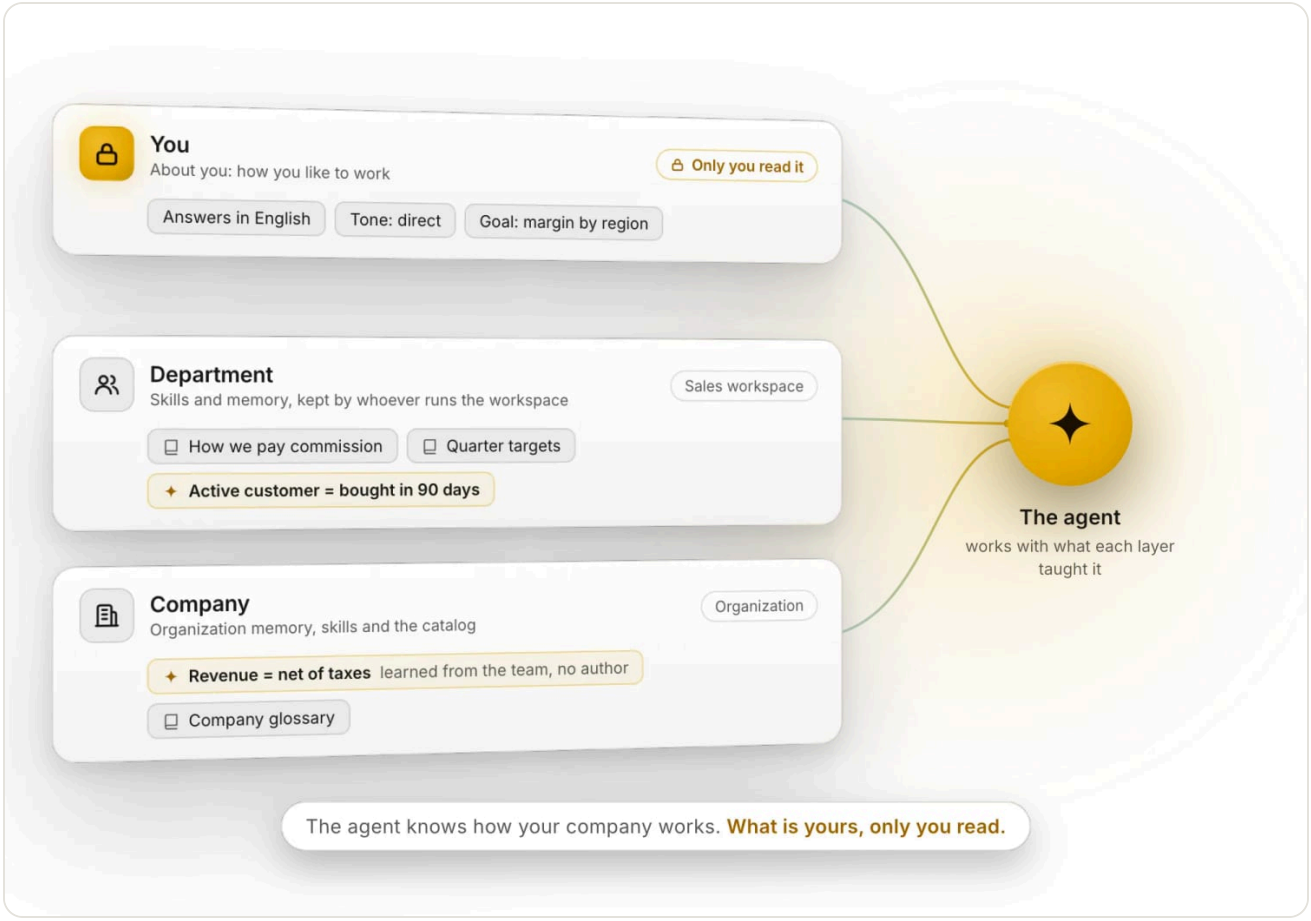


MEMORY

What your company taught the agent

It starts with you: "About you" keeps how you like to work, and only you read it. The organization keeps what holds for everyone, without identifying who asked.

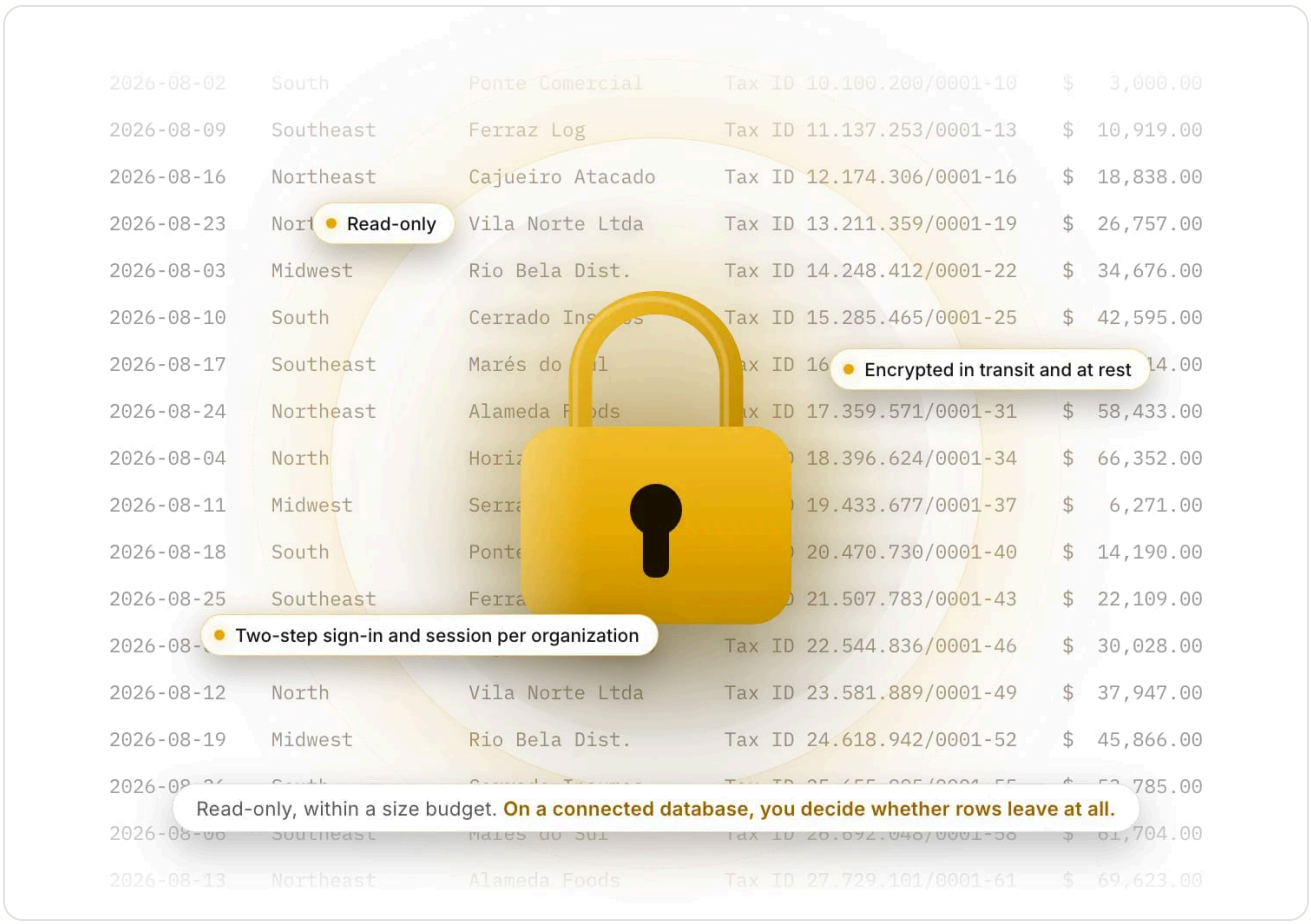
- About you: your preferences and the agent's notes, shown only to you.
- Skills and memory for each workspace and for the company.



Full adherence to GDPR, LGPD and the European AI Act

Every control is published, and most are held by a test that fails if the product drifts from the promise.

- **You can freeze processing.** A restriction you can ask for at any time: the product's AI features refuse to run over your data, while reading, export, deletion and sign-in stay open. Most products only offer you the door.
- **Erasure is exercised, not asserted.** A test seeds a full account against a real database, exports it, deletes it, then sweeps the schema for anything left behind. It runs on every change.
- **Retention runs, it is not just promised.** Usage records are deleted after 12 months by a job this very sentence shares its constant with. Off-box backups expire after 30 days — there the deletion is our cloud provider’s lifecycle rule, and this number is a mirror of it, cross-checked by a test against our published retention matrix.
- **Backups are encrypted before they leave.** The daily dump is encrypted on our machine, with our own key, before it is copied anywhere. No key, no upload — it fails closed rather than quietly.
- **In the cloud, encrypted, under US and EU frameworks.** Hosted in Nuremberg, Germany (European Union) and reached only over TLS, with your database credentials sealed by AES-256-GCM. Transfers abroad rely on Standard Contractual Clauses, and on the EU-US Data Privacy Framework where the provider is certified. Every subprocessor is named in the published notice.
- **The SQL can only read.** The generated query passes a guard that admits reads and nothing else. A database you connect is checked against loopback, link-local and private ranges before we accept it, and checked again after its name is resolved.


Read-only
Encrypted in transit and at rest
Two-step sign-in and session per organization
Read-only, within a size budget. On a connected database, you decide whether rows leave at all.

Privacy and Data Protection Policy

November 18, 2026 · v42

This Policy tells you which personal data we process, for what, with whom and for how long, and what your rights are.

1. Who we are and roles

1.1 TalkWithData (the "Service") is operated by KGPX Serviços Administrativos LTDA, trade name TalkWithData, CNPJ 23.543.381/0001-50, Rua Gustavo Ambrust, 464, Campinas/SP, postal code 13092-106, Brazil. Data Protection Officer (DPO): Guilherme Favaron, contact@talkwithdata.ai.

1.2 The Service is used within organizations. Every account belongs to at least one organization: its own, created with the account, or another to which it was invited. An organization has an owner, may have people who help run it (AI Champions) and is divided into workspaces arranged in a tree. The owner represents the organization and accepts these documents on its behalf.

1.3 For an organization's content, the organization is the controller and we are the processor. The organization's content is:

- the data sources and files;
- the conversations, artifacts and panels;
- the skills, memory and About you profile;
- the people, roles and invitations;
- the governance records.

We process this content on the organization's behalf, only to provide the Service, under Annex C of the Terms of Use.

1.4 For account data, we are the controller. Account data is:

- your identity and sign-in;
- acceptances and preferences;
- usage and billing records;
- usage analytics;
- the feedback reports you choose to send us.

1.5 This Policy describes what we process by category of data and by purpose, not feature by feature. A new feature that processes a category already described, for a purpose already described and with recipients already described, follows this Policy as it stands. Where it says the Service "may offer" something, the feature is not yet available in every account. Until it is, nothing that passage describes happens; when it is, it works as the passage says.

1.6 The Service is not directed to children under 16, and we do not knowingly collect data from children. If you believe a child has registered, write to contact@talkwithdata.ai.

2. Data we process

2.1 **Account and access.** We process:

- name and email address;
- the password, stored only in irreversible form;
- the Google account identifier, when you sign in with it;
- the link to the company sign-in identity (Google Workspace or Microsoft Entra), never the company's password or a token of it;
- the two-step verification settings;
- the records of your sessions.

Of sessions we keep when they began and when they were used, never the IP address or the device. We also keep the record of each acceptance of these documents.

2.2 **Organization and governance.** We process:

- the organizations and workspaces to which you belong and your role in each;
- invitations and requests to join, and who decided them;
- who governs each source and to whom it was opened, in whole or in part;
- access requests and the decisions on them;
- the plan and seats contracted by the organization.

2.3 **Governance log.** We keep a record of the organization's management acts: who acted, on whom, which act and when. We also keep people's sign-ins and sign-outs and refused attempts to sign in to the account. The record identifies people by an internal identifier, never keeps the content of the data and never says who read which data. Refused attempts do not say who tried, nor the IP address or the device.

A log entry is not changed afterwards, except to remove the identifier of someone who deletes their account. The organization's management sees its log. Whoever runs a workspace sees the entries about it and about the workspaces below it.

2.4 **Content you bring.** We process:

- the files you upload, including those that come from Google Drive;
- the earlier versions of each file;
- the structure and catalog of connected databases;
- connection credentials, always encrypted;
- uploads waiting to be applied.

2.5 **Content you create.** We process:

- the questions, answers and results they keep;
- the record of each step of the agent, without the rows read;
- saved artifacts and panels and with whom they were shared;
- favorites and recent items.

When the Service offers them, also panel templates, which keep the design of a panel and never rows.

2.6 **Organization context.** We process skills: instructions the organization writes for the agent, such as business rules, definitions and tone of voice. For each skill we keep the versions, who uploaded them and to whom they were granted. A skill may contain personal data, such as names and roles. We also process the organization's visual identity.

2.7 **Memory and profile.** We process:

- your About you profile, with how you prefer to be called, language, tone and goals;
- notes about how you prefer to work, written by you or by the agent;
- when the Service offers it, the memory of a workspace or of the organization, without an author.

Memory and the profile never keep rows, values from the data, numbers from an answer, another person's personal data or sensitive data.

2.8 **Connected systems.** If you connect Google Drive, we process:

- the authorization you gave, stored encrypted;
- the email address of the connected Google account, which only you see;
- the metadata of the items you chose.

When the Service offers other inputs and outputs, we process their credentials and accesses, always encrypted or kept only as a cryptographic digest.

2.9 **Access trail.** When the Service offers it, we keep of each read of data:

- who read, when and where;
- which tables and columns were read;
- how many rows came back;
- whether the rows went to the AI provider.

The trail never keeps the values read.

2.10 **Usage and technical data.** We process:

- usage records of AI calls and consumption;
- one receipt per question, without its content, which counts toward the organization's allowance;
- error logs;
- IP address, browser and access times, for security.

When we validate a change to the engine that executes queries, we keep technical comparison records. Those records have no account identifier, data values or question text.

2.11 **Feedback reports.** If you choose to send us a report, it carries:

- the type, title and text;
- the page type, screen size, language and time zone;
- your name and email address;
- the screenshots you attach.

A screenshot shows what was on your screen and may contain data from your sources. You see each screenshot before sending and may remove it.

3. Purposes and legal bases

3.1 We process account data under these legal bases:

Purpose	Legal basis
Create the account, authenticate and provide the Service, including the AI processing necessary to answer	Performance of a contract (GDPR art. 6(1)(b); LGPD art. 7, V)
Security, abuse prevention and usage limits	Legitimate interests or legal obligation, as applicable (GDPR art. 6(1)(f)/(c); LGPD art. 7, IX/II)
Validate the accuracy of the numbers of a new query engine	Legitimate interest: the accuracy of what the Service answers (GDPR art. 6(1)(f); LGPD art. 7, IX)
Show whoever runs a workspace how many questions each member asked in the month and when the last one was, never the text	Legitimate interest: the organization's control over the allowance it contracts (GDPR art. 6(1)(f); LGPD art. 7, IX)
Read and process the feedback reports you send	Legitimate interest: fixing and improving the Service (GDPR art. 6(1)(f); LGPD art. 7, IX)
Getting-started messages: one welcome message and at most one reminder	Legitimate interests, with a right to object at any time (GDPR art. 6(1)(f); LGPD art. 7, IX and art. 10)
Aggregate usage analytics	Consent, refusable and revocable at any time (GDPR art. 6(1)(a); LGPD art. 7, I)
Billing, invoicing and usage metering	Performance of a contract and legal obligation
Respond to support and data subject requests	Legal obligation and contract

3.2 An organization's content is processed on its instructions, under its contract with us (GDPR art. 28; LGPD art. 39). The legal basis for that content is the organization's to establish, as controller.

3.3 We do not build marketing profiles about you or about the content of your data. A feedback report is never used for marketing.

4. Artificial intelligence

4.1 The Service uses artificial intelligence to write queries, read the results and answer in natural language. You interact with an AI agent, and what it writes is generated by AI. This includes:

- the answers;
- the reading of artifacts and panels;
- skills written in an interview;
- memory and the profile.

4.2 To answer, we send to a frontier AI model, from the provider listed in Annex B:

- your question and the Service's instructions;
- the description of the sources you may read, with a sample of values, from which columns that look like personal identifiers are excluded;
- the summary of earlier conversations, written by the server and without rows;
- the text of the skills that serve the question;
- the results of the queries necessary for the answer, within technical limits.

Query results and error messages may contain values from your data. We never send passwords, credentials or data from sources, tables or columns that you may not read.

4.3 When you upload a spreadsheet, before the first question, we may send the AI provider the structure, rows and file name, to generate the description and suggested questions. Where the organization does not use folders, the same applies to the text of a document uploaded on its own, once, on upload.

4.4 In a connected database, rows go to the AI provider only while two switches are on: the source's, controlled by whoever runs it, and your account's, in Settings. With either one off, the answer has no AI reading of the rows.

4.5 A document, such as PDF, DOCX, MD, TXT or Google Docs, never becomes a table: it is context for the analysis. With the question, its text goes to the AI provider only where the organization has turned on document context, and only from documents you may read. The only other transmission is the one in item 4.3. Every number taken from a document is marked with that origin.

4.6 The AI provider may not train models on the content we send and keeps inputs and outputs for up to 30 days, longer only when the law or its usage policy requires. Nothing that comes from Google Drive is used to train models.

4.7 After a turn, the agent may update your About you and the notes about you, and a second AI check reviews each change before it takes effect. The profile and notes are shown only to you: no owner, AI Champion or person at TalkWithData reads them. You see, correct and delete each change, and may turn off the automatic update.

The agent infers only working preferences, never sensitive data. The profile is never used to decide anything about you, evaluate your work or limit your access. A note you deleted is not recreated from earlier conversations.

4.8 When the Service offers the memory of a workspace or of the organization, an agent reads the conversations of the members of that scope and records what holds for everyone, without identifying who asked and without reproducing the question. No person reads those conversations because of this. You see in the chat, before the first question, that memory is on. If you do not want your conversations to feed it, the organization decides, and a request from you reaches it as item 9.4 says. In a small group, a preference may point to someone. Deleting a conversation does not delete a memory entry that came from it.

4.9 Saving or manually editing an artifact sends nothing to the AI provider. Refining an artifact with an instruction sends the instruction and the text the AI may rewrite, never table values.

4.10 The feedback reports you send are read by our team and by internal AI agents, which run on the provider listed in Annex B for that purpose, to become engineering tasks. The task is written without your name, email address or screenshots. No part of a report goes to the AI provider of the product's answers.

4.11 The Service does not make automated decisions with legal effect about people. The Terms of Use prohibit using it for high-risk decisions about people without the human oversight the law requires.

5. Access and sharing

5.1 Who reads what within an organization is decided by the organization:

- every source has an owner and only the owner opens it to others, in whole or in part;
- no one reads a source because of their role;
- whoever governs a source sees its structure, never its rows;
- what is opened to a workspace does not go down to the workspaces below it;
- a table or column marked as read by no one stays out of every answer, for everyone, including the person who connected the source and the organization's owner;
- a new table or column that a file brings starts closed to everyone until whoever curates the source releases it.

Who reads a file that comes from Google Drive is decided in the Service, never by the access in Drive.

5.2 Your conversations, subjects and artifacts are shown only to you, except an artifact you choose to share. No owner or AI Champion sees the text of a question of yours.

5.3 An artifact you share with your workspace or with the organization opens to all those people, with the text, tables and charts, even to someone who has no access to the sources it read. This includes whoever joins later. Sharing is giving access to what the artifact shows. Whoever receives it sees who

shared it and when, and cannot change, copy or download it. The organization's management sees that the share exists, never the title or content. It may cut it: it closes at once, and you cannot share it again until management undoes the cut, which does not reopen it.

5.4 When an access of yours closes, what an answer already read stays in it, marked as read before the cut, and the next question no longer reads it. The cut is never retroactive.

5.5 The members of a workspace see each other's names and roles, and whoever runs it also sees the email address. The organization's management sees all its people, with name, email address and role. Whoever runs a workspace sees, in it and in the workspaces below, the people, how many questions each one asked in the month and which sources exist, never the data or conversations.

5.6 We share personal data with:

- the subprocessors listed in Annex B, to operate the Service;
- the sign-in providers you choose to use (Google and Microsoft), which act as independent controllers of that sign-in;
- authorities, when the law requires.

We do not sell personal data.

5.7 Before a new subprocessor receives any data, it enters Annex B, and we notify organizations through the Service or by email at least 30 days in advance. Within that period, the organization may object. If the objection is not resolved, it may end the contract without penalty.

5.8 The systems the organization chooses to connect as a source and those it chooses to receive data are not our subprocessors: they are its choices, under its contracts. The same applies to its account with an AI provider, when the Service offers that use.

5.9 A data input only reads: the Service never writes to the source system. An output, when offered, delivers only what whoever uses it may read in the Service.

5.10 The Service may offer the organization additional controls, turned on by it, that change processing only in the direction their name says:

- a sensitive mode for a source, in which nothing from it goes to the AI provider;
- shorter retention periods and the option not to keep the rows of answers;
- pseudonymization of columns, which reduces risk but does not make the data anonymous;
- an encryption key of its own;
- the choice of the AI model's provider and region;
- isolated hosting, in a region this Policy names first.

6. International transfers

6.1 The primary store is in the European Union, and the Service is operated from Brazil. Some subprocessors process data in other countries, including the United States, as Annex B indicates for

each one.

6.2 Those transfers rely on appropriate safeguards, such as Standard Contractual Clauses and the subprocessors' Data Processing Agreements, never on generic consent to transfer.

6.3 The data the organization brings from other systems, or delivers to them, comes from and goes to wherever those systems are, by its choice and under its contracts.

7. Security

7.1 We adopt technical and organizational measures proportionate to the risk:

- encryption in transit and at rest;
- connection credentials encrypted with a dedicated key;
- least-privilege access;
- queries against your data limited to reading;
- protection of connections against internal networks;
- two-step verification;
- backups outside the primary server.

7.2 The technical detail of the measures is in a security and data processing document, delivered to customer organizations under a confidentiality agreement. It describes what this Policy promises and neither widens nor reduces it; if there is a difference, this Policy prevails.

7.3 A security incident that affects personal data is communicated to the affected organization, the authority and the data subjects, when the law requires, under Annex C of the Terms of Use.

8. Retention and deletion

8.1 We keep each category of data for the period or criterion in Annex A, and only for the time necessary for the purpose.

8.2 Leaving a workspace or the organization, being removed or a workspace moving to another organization does not delete your conversations, subjects and artifacts. They stay stored in the workspace and no one opens them, not even you, while you are out. If you return, they will be there. An artifact you shared stays open to whoever received it, as it was, and no one changes it.

> When you leave or are removed from an organization, the files you uploaded and did not share are deleted, and answers about them lose the rows. Those you shared pass to the organization, with the shares they have. To avoid this, delete them or stop sharing them before leaving. The sources you connected stay with their owner.

8.3 When a workspace moves to another organization, the destination organization becomes the controller of its content, and we send an email notice to the members; if a notice cannot be sent, the

page tells whoever made the move. An artifact shared with the organization then opens to the people of the destination organization.

8.4 Archiving a workspace does not delete anything or shorten any retention. While it is archived, its sources are closed and no one opens the conversations and artifacts left in it. Once restored, everything returns as it was, except invitations and requests to join, which archiving cancels.

8.5 When you delete your account, your account data leaves the live database, except the records Annex A requires to be kept for their own period. In each organization that remains, item 8.2's rule for leaving applies, and your conversations and artifacts lose your account identifier. Your own organization, when no one else uses it, is deleted with everything in it. The owner of an organization that other people use transfers ownership to an AI Champion, or removes the other people, before deleting the account.

8.6 Whoever curates a source may delete it. Deleting a source deletes the questions and answers asked about it. An answer that read that and other sources keeps the text and loses the rows from the deleted source. A saved artifact keeps the rows it copied, until whoever created it deletes it.

8.7 A deletion removes the data from the live database at once. Backups are not edited: the deleted data expires from them within the period in Annex A.

> If a restore brings back deleted data, we reapply the deletions we can identify. After a total loss of the live database, a deletion made after the last backup may not be identifiable.

9. Your rights

9.1 Under the LGPD and, when applicable, the GDPR, you may request:

- confirmation and access;
- correction;
- anonymization, blocking or deletion;
- portability;
- information about with whom we share;
- restriction of processing;
- review of an automated decision.

You may also object to processing based on legitimate interests and revoke consents.

9.2 In the product itself, you see, export and delete your sources, conversations and artifacts, your account and your About you profile.

9.3 Restriction of processing is an account state. While it is in force, the product's AI features do not run for you and adding a new source is refused; signing in, reading, exporting, deleting and billing continue to work. The console we use to diagnose the Service runs under an administrator's session and is not blocked by the restriction. We impose and lift the restriction at your request, and both acts are recorded.

9.4 For an organization's content, the organization is the controller. A request about it, such as data about you in a source someone else added, is forwarded to it, and we tell you about the forwarding. Your About you profile is never handed to the organization's management to answer a request. Correction and deletion reach what the Service keeps; copies someone downloaded, or that an output delivered to another system, stay with whoever received them.

9.5 Privacy requests: contact@talkwithdata.ai. We aim to respond within 15 days under the LGPD and within 30 days under the GDPR, extendable as the law permits.

> You may complain to the Brazilian Data Protection Authority (ANPD), in Brazil, and, when applicable, to the data protection authority of the EU or EEA.

10. Cookies and local storage

10.1 We use essential authentication and session cookies. A session lasts up to 7 days after its last use, and an organization may set shorter limits.

10.2 Usage analytics uses cookies from an analytics provider, which persist for up to two years. It loads only after your acceptance, and a refusal ends collection.

10.3 We do not use advertising cookies or cross-site tracking.

10.4 Google scripts, for sign-in, Google Drive and the file picker, load only when you request the corresponding action. Google's terms and cookies apply within them.

10.5 The theme preference is kept in your browser's local storage.

11. Google User Data

11.1 The use of information received from Google Workspace scopes will adhere to the Google User Data Policy (https://developers.google.com/workspace/workspace-api-user-data-developer-policy), including the Limited Use requirements. TalkWithData's use and transfer to any other app of information received from Google APIs will adhere to the Google API Services User Data Policy (https://developers.google.com/terms/api-services-user-data-policy), including the Limited Use requirements.

11.2 We read only what you choose: the files you pick and, when you choose a folder, the list of what it and its subfolders hold, and the files on that list you did not leave out, including those added later. We never write to your Drive, use what we read only to provide the Service as this Policy describes, and no person at TalkWithData, and no AI agent that operates the Service, reads it except for security, to comply with the law, or at your request. We do not use or retain Google user data, raw or derived, to develop, improve or train generalized AI or machine-learning models.

11.3 Drive synchronization stops when you disconnect, revoke access at Google, leave the organization or the workspace that owns the folder, or stop curating it. When you disconnect, we delete

the stored authorization and, when no other connection of yours depends on it, revoke it at Google. You may choose to delete also what the connection brought: where you curate the folder, it is deleted for good; where you do not, it becomes a request to whoever curates it, who decides.

11.4 How to manage and delete Google Drive data: talkwithdata.ai/help/google-drive.

12. Changes and contact

12.1 We may update this Policy. Material changes are communicated through the Service or by email.

12.2 We ask for a new affirmative acceptance when a change:

- processes a category of personal data this Policy does not describe;
- uses data for a purpose it does not describe;
- sends data to a recipient that is neither a subprocessor announced as item 5.7 says nor a system the organization chooses;
- changes the country of the primary store;
- changes who is the controller or processor of some data;
- reduces one of your rights;
- otherwise widens who receives some data, how long it is kept or what the Service infers about a person;
- makes less true what you read here.

We also ask when the law requires it. A new feature within what this Policy already describes follows the text in force.

12.3 Contact for privacy and data requests: contact@talkwithdata.ai (Data Protection Officer: Guilherme Favaron).

Annex A. Retention periods

A.1 Each period applies to the category indicated; what has no period stays until the deletion described in section 8.

Category	Period
Account data	Until account deletion
Company sign-in link	Until deletion of the account or of the organization of that sign-in
Sources, files and conversations	Until deleted by whoever may delete them, or with the organization
Skills	Until whoever governs them deletes them, or with the workspace or organization
About you and agent notes	Until you delete them or delete the account, or with the organization

Category	Period
Memory of a workspace or of the organization	Until whoever runs the scope deletes it, or with the scope
Input credentials and output accesses	Until the connection is undone, whoever gave it can no longer use it, or the access is revoked or expires
Earlier versions of a file	The 3 most recent; whoever curates the source may delete earlier
Upload waiting to be applied	24 hours
Invitation link	Valid for 7 days
Session records	7 days after last use
Governance log	While the organization exists; sign-in and sign-out entries, 12 months
Usage and consumption records	12 months
Engine validation technical records	90 days; they have no account identifier and do not leave with it
Feedback reports	Rule of 12 months after receipt; deletion is still done by us, not automatically, and may occur later; or earlier, at your request. They are outside the product database and do not leave with the account.
Google Drive authorization	Until you disconnect, leave the organization or delete the account. If revocation at Google is not confirmed, up to 6 months.
Inputs and outputs of the answers' AI provider	Up to 30 days at the provider, longer only when the law or its usage policy requires
Reading of reports by the internal agents' provider	Under that provider's terms (Annex B)
Daily server image	7 days
Database backups	Expire 30 days after each copy; the provider deletes them afterwards, with no exact deadline
Access trail	For the period published here before it is turned on; survives deletion of the conversation and account, as the organization's proof of access

Terms of Use

November 18, 2026 · v42

These Terms govern the use of TalkWithData. The numbered paragraphs and the annexes are part of them.

1. Parties and acceptance

1.1 These Terms govern the use of TalkWithData (the "Service"), operated by KGPX Serviços Administrativos LTDA, trade name TalkWithData, CNPJ 23.543.381/0001-50, Rua Gustavo Ambrust, 464, Campinas/SP, postal code 13092-106, Brazil ("we").

1.2 By creating an account or using the Service, you agree to these Terms and to the Privacy and Data Protection Policy.

1.3 Whoever accepts on behalf of an organization represents that they have authority to bind that organization to these Terms.

2. Accounts and eligibility

2.1 You must be at least 16 years old and have the legal capacity to accept these Terms.

2.2 You keep your credentials secure, do not share your password and keep your registration data accurate.

2.3 You may turn on two-step verification, and an organization may require it of its people.

2.4 We may suspend or terminate accounts that violate these Terms or engage in fraudulent, abusive or illegal activity.

3. Organizations and roles

3.1 The Service is used within organizations, divided into workspaces. The owner represents the organization. AI Champions help run it, and whoever runs a workspace administers it.

3.2 The organization is responsible for:

- the legal basis of the personal data in its content;
- who joins it and with which role;
- what each person may read;
- the acts of its management in the Service;
- data subject requests about its content, which we forward to it.

3.3 The organization may set access and session rules for its people, including requiring two-step verification or the company sign-in. When it requires the company sign-in, it is responsible for whom its provider lets in, and the owner remains outside the requirement so that the organization is not locked out if the company sign-in stops working.

3.4 The owner may transfer ownership of the organization to an AI Champion, who then represents it.

4. Acceptable use

4.1 You agree not to:

- (a) upload or connect data you have no right to process;
- (b) attempt to access, probe or disrupt the Service's infrastructure;
- (c) process illegal, harmful or unauthorized data;
- (d) reverse engineer the Service or extract its code;
- (e) use the Service to build a competing product;
- (f) abuse the AI system with excessive or malicious requests;
- (g) upload malicious code;
- (h) use an output of the Service to deliver data to someone who may not read it in the Service, or to get around the access the organization set.

4.2 Do not connect or upload sensitive personal data, data on criminal convictions or data of children and adolescents without a legal basis of your own. When the Service offers a dedicated mode for such data, use it. Until that mode exists, do not connect such data. If you find that you connected it, disconnect the source and tell us.

4.3 The Service is made for the analysis of business data. Do not use it to decide about people in high-risk uses without the human oversight and the obligations that such use requires. Examples include hiring, performance evaluation, credit and access to essential services, as in Annex III of the EU AI Act. Whoever adapts the Service to such a use is responsible for it.

5. Data and artificial intelligence

5.1 We do not claim ownership of the data you upload or connect. What you add to an organization is its content. When you leave or delete your account, the sources you connected stay with their owner.

5.2 You and the organization are responsible for the data you bring, including having the rights, consents and legal basis to process it through the Service. The organization is responsible for the systems it connects and for the recipients to which it delivers data.

5.3 We process an organization's content as its processor, on its behalf, under Annex C, which is part of these Terms.

5.4 The Service uses a third-party AI provider under the conditions of the Privacy Policy (section 4). The organization and each person may prevent the rows of a connected database from being read by AI.

5.5 AI-generated content may contain errors. Check critical results before making decisions based on them. We do not guarantee the accuracy, completeness or reliability of AI-generated answers. Whoever publishes content written by the agent outside the Service is responsible for disclosing that it was written by AI.

5.6 We adopt reasonable security measures, but no system is perfectly secure. We are not liable for improper access caused by the compromise of your credentials or by your configuration.

6. Plans

6.1 The Service may offer a free plan and paid plans. Features and limits are described on the pricing page and may change.

6.2 An organization's plan and seats are set under its contract. The monthly question allowance belongs to the organization. Once it is reached, new questions are refused until the next cycle, and members are notified in advance.

6.3 Anti-abuse limits apply to every account.

7. Availability

7.1 We strive for high availability but do not guarantee uninterrupted service. Maintenance and updates may affect availability.

7.2 We are not liable for interruptions or losses caused by factors beyond our control.

8. Liability

8.1 To the maximum extent permitted by law, we are not liable for indirect, incidental, special, consequential or punitive damages, or for loss of profits, data or opportunities.

8.2 Our total liability for any claim relating to the Service is limited to the greater of (a) the amount paid to us in the 12 months before the claim and (b) USD 100.

8.3 Nothing in these Terms limits rights that cannot be waived under consumer protection law.

9. Termination

9.1 You may delete your account in Settings. The owner of an organization that other people use transfers ownership or removes the other people first. After deletion, we process the data under the

Privacy Policy (section 8).

9.2 We may suspend or terminate access for violation of these Terms or for risk to the Service or to other people.

10. Changes

10.1 We may update these Terms. Material changes are communicated through the Service or by email.

10.2 We ask for a new affirmative acceptance in the cases of item 12.2 of the Privacy Policy and when the law requires it. In all other cases, continued use after the effective date constitutes acceptance.

11. Governing law, venue and language

11.1 These Terms are governed by the laws of the Federative Republic of Brazil, without regard to conflict-of-law rules.

11.2 The exclusive venue is the courts of Campinas, State of São Paulo, Brazil, unless consumer protection law provides otherwise.

11.3 These Terms exist in Portuguese and English. The accepted version is the one in the language in which you were using the Service when you accepted. If the versions differ, the Portuguese version prevails.

12. Contact

12.1 contact@talkwithdata.ai.

Annex C. Data processing agreement

C.1 **Subject matter.** This annex governs the processing of personal data that we carry out as processor, on behalf of the organization as controller, to provide the Service (GDPR art. 28; LGPD arts. 37 to 40).

C.2 **Nature and purpose.** The processing covers storing, organizing, querying and presenting the organization's content, and sending it to the AI provider under the conditions of the Privacy Policy, only to provide the Service.

C.3 **Duration.** The processing lasts while the organization uses the Service and, afterwards, for the periods in Annex A of the Privacy Policy.

C.4 **Categories.** The data subjects are the people of the organization and the people whose data the organization brings to the Service. The data are those of the organization's content, as item 1.3 of the

Privacy Policy defines it. Account data, under item 1.4, are outside this annex: we are the controller of those data.

C.5 **Instructions.** We process the content only under the organization's documented instructions, including as to international transfers, which follow section 6 of the Privacy Policy. Use of the Service and the settings the organization chooses in it are those instructions. If the law requires us to carry out other processing, we notify the organization in advance, except when the law prohibits notice. If an instruction appears to us to be contrary to the law, we notify the organization.

C.6 **Confidentiality.** Everyone who processes the content on our behalf is bound by confidentiality.

C.7 **Security.** We maintain the measures of section 7 of the Privacy Policy, appropriate to the risk.

C.8 **Subprocessors.** The organization authorizes the subprocessors in Annex B and new ones announced as item 5.7 of the Privacy Policy describes, with the right to object provided there. We impose on them data protection obligations equivalent to those of this annex and are responsible to the organization for their performance.

C.9 **Data subjects' rights.** We help the organization respond to data subject requests, with the Service's tools and with support on request. We forward to it the requests we receive about its content.

C.10 **Incidents.** We notify the organization, without undue delay, of a security incident that affects its content, with the information it needs to fulfil its own obligations.

C.11 **Assistance.** We assist the organization with impact assessments and consultations with the authority, to the extent the processing requires.

C.12 **End of the contract.** At the end of the contract, the organization chooses between the return and the deletion of its content. The return respects what the Privacy Policy keeps private to each person, such as conversations and the About you profile. Afterwards, we delete the content under the periods of Annex A, except what the law requires us to keep.

C.13 **Audit.** We make available to the organization the information necessary to demonstrate compliance with this annex, including the security document under confidentiality. We also accept reasonable audits, arranged in advance.

Fingerprint (SHA-256) of the text accepted in this version: 6c7f96cb884e0871641f146780bf987a12e147c9084c8fb20122ec5eaa58c7cc

PART IV. SUBPROCESSORS ON THE DATE OF THIS EDITION

Subprocessors

November 18, 2026

Before a new subprocessor receives any data, it enters this list, and we notify organizations through the Service or by email at least 30 days in advance, with a right to object (Policy, item 5.7).

The sign-in providers (Google and Microsoft) act as independent controllers of the sign-in you choose to make through them, and are not subprocessors. Google Drive is a system from which you choose to bring files, and Google is not a subprocessor because of that.

Subprocessor	Purpose	Where it processes	Safeguard
Hetzner Online GmbH	Application and database hosting, with a daily server image	Nuremberg, Germany (EU)	Data Processing Agreement (GDPR art. 28); processing in the EU
Hostinger	Operation of the Service and receipt of feedback reports; keeps no copy of the Service's database	São Paulo, Brazil	Processing in Brazil, the controller's country
Cloudflare	DNS, connection encryption, proxy and edge protection	Global network	Data Processing Agreement and Standard Contractual Clauses
Resend	Transactional email and receipt of email sent to the privacy contact	United States	Data Processing Agreement and Standard Contractual Clauses
Anthropic PBC	Frontier AI model that answers the product's AI calls; does not train models on the content sent	United States	Anthropic Data Processing Agreement with Standard Contractual Clauses
OpenAI	Models of the internal agents that read the feedback reports you send; no other product call	United States	Training disabled on the account used (confirmed by the controller, 2026-10-26); that account's Data Processing Agreement with Standard Contractual Clauses and the EU-US Data Privacy Framework certification are pending verification
Google (Analytics)	Aggregate usage analytics, only after your acceptance	United States	Data Processing Agreement and Standard Contractual Clauses

Subprocessor	Purpose	Where it processes	Safeguard
Google Cloud (Storage)	Daily database backups, outside the primary server	Frankfurt, Germany (EU); copies made before the move to Hetzner remain in the United States (multi-regional) until they expire	Google Cloud Data Processing Agreement; EU-US Data Privacy Framework
Google Cloud (Secret Manager)	Escrow of the encryption key, to restore backups	Multiple regions, selected by Google	Google Cloud Data Processing Agreement; EU-US Data Privacy Framework
Stripe	Payment processing for paid plans	United States and EU	Data Processing Agreement and Standard Contractual Clauses



TalkWithData
Contact: contact@talkwithdata.ai
talkwithdata.ai