



Security and data protection

What an IT team or an auditor needs to verify before connecting Aski to an ERP.

Version 1.3 · August 25, 2026 · Technical companion to the privacy policy published at aski.dev/en/privacy

What Aski does with the data

Aski is an assistant that answers business questions by querying the customer's ERP —Odoo, SAP S/4HANA or SAP Business One— in natural language. **It queries live, in read-only mode by default and with the permissions of the user who connects.** It does not replicate the customer's database and does not share it with other customers.

Data processing roles

CONTROLLER

The customer company

Owner of the ERP and the data it holds.
Decides what is processed and for what purpose.

PROCESSOR

The implementing partner

Manages the relationship with the customer company and contracts the service on its behalf.

SUB-PROCESSOR

Aski

Processes the data solely to answer the queries the user themselves submits.

We sign a data processing agreement and a confidentiality agreement on request, including international transfer clauses. If the organization has its own template, we review it and sign it.

Where it is hosted

Component	Provider	What it receives
Backend and database	Railway (United States)	Hosts the infrastructure. Operational access, without querying the data directly.
Language model	Anthropic — Claude (United States)	Question, ERP schema and a limited excerpt of rows. See below.
Website and web app	Vercel (United States)	Interface delivery only. It receives no ERP data.
Link to internal ERPs	Tailscale (United States)	Only on tunnel connections. Link data: organization name, machine name and internal network ranges. It does not receive the content of the queries.
Backups	Daily backup	Full copy of the database, retained for 30 days.
Email, logs and errors	Resend · Better Stack · Sentry (United States)	Platform emails and technical traces with no message content.

The full list of third parties, what each one receives and their country, is published at aski.dev/en/privacy, section 4. There is an international transfer of data to the United States and it is declared as such.

If the ERP is not reachable from the internet

Many on-premise installations are not published on the internet, and there is no reason they should be. For those cases a **private-network node** (Tailscale) is installed on a machine in the same network where the ERP lives, and the backend comes in through it.

What is NOT needed

- **No inbound port** open on the customer's firewall: the node establishes the connection outwards, just like a browser.
- No public IP, no port forwarding, no publishing the ERP.
- The ERP server is not touched: the node goes on any always-on machine of that network (Linux if the ERP uses HTTPS).

Isolation and control

- Each customer joins with **their own key**, tagged and revocable independently.
- The private-network rules only allow backend → customer node, and only towards the ERP ports. Two customers' nodes **cannot see each other**.
- The **ERP credentials are entered by the customer** in the application; they are not shared with us through any channel.

The link runs as a service separate from the main backend, and each connection is marked «through the tunnel» one by one: marked that way it always goes out through the tunnel and never over the internet; a normal connection never uses it.

Isolation between customers

1. **No copy of any customer's ERP is kept.** There is no shared repository where two customers' data could cross: every query runs live against that customer's instance and returns only the rows for that question. What is stored is the conversation history, tied to the account of whoever asked.
2. **Each connection belongs to a single user.** Credentials, conversations and messages are tied to their owner's identifier, and every query is filtered by the authenticated user. No API route returns a credential in the clear: it is not shown in the app, not exposed through the API and does not appear in the admin panel or in the logs.
3. **Aski sees no more than the connected user sees.** It queries the ERP with that user's credentials, with no privilege escalation. If that user cannot see costs, margins or another company's data, neither can Aski.

Technical precision: to speed up answers, a catalogue of names and labels of the ERP's *standard fields* is held in temporary memory, shared across instances of the same version and language. It contains nomenclature —field names and labels, and the values of low-cardinality classification fields: stages, categories, tags—, never custom models, never records and never figures. Before being used it is cross-checked against the instance's real schema, so it never shows an instance anything it does not have.

Encryption and access control

Encryption

- **In transit:** HTTPS with TLS 1.2 or higher on every leg (app ↔ backend, backend ↔ ERP). **Exception:** over the tunnel that leg is encrypted by WireGuard towards a pinned private address and the ERP's certificate is not validated — details at aski.dev/en/security, section 6.
- **At rest:** the ERP password or API Key is encrypted with AES-256-GCM before being stored.
- **Accounts:** passwords stored as bcrypt hashes; sessions with signed tokens.
- **Device:** encrypted storage with a key managed by the Android Keystore.

Access and detection

- Operational access to the database is restricted to a minimal number of administrators and is audited.
- SQL injection or model manipulation attempts are detected before reaching the AI and are logged.
- Requests for known sensitive fields and restricted models are rejected.
- Cutting off access does not depend on Aski: it is enough to disable the key or the service user in the ERP itself.

What this does not mean: the key that encrypts the credentials lives on the server, because the backend needs to decrypt them to open the connection to the ERP. As the platform operator, technical access exists. We would rather state it than let anything else be understood.

Read-only by default, and actions with confirmation

By default, the only operations the system issues against the ERP are queries, and on SAP S/4HANA that is always the case. The exception is **actions with confirmation**: they require explicit activation and exist on Enterprise Plus, on the SAP plans and on the Dedicated plans, over Odoo and SAP Business One. They are not free-form writing — the system only knows a closed catalogue of ten operations on a specific record (payment reminder, single or to the customers on a list; follow-up activity, mark it done or reschedule it; approve or reject a document; change the owner; mark an opportunity won or lost — on Business One only the first two), nothing runs without the user's explicit confirmation, and every execution is logged with who asked, what was done and with exactly what data. Anything outside that catalogue is cut off before touching the ERP. There is one more write, outside that catalogue: if the user chooses to receive a scheduled alert in the inbox of their own Odoo, each delivery creates a notification message there addressed to them, without touching any business record. The permissions and record rules configured in the ERP remain in charge; Aski opens no new door. Full detail at aski.dev/en/security.

What the artificial intelligence model receives

To write the answer in natural language, Anthropic receives the question, the ERP schema (model and field names) and a limited excerpt of the records that query returned: **up to 20 rows per answer in normal mode and up to 80 rows per query in Deep analysis**. That excerpt may contain business information, such as customer names or amounts. **The full database and the credentials are never sent**. Anthropic retains that content for up to 30 days solely for abuse detection, per its terms, and does not use it to train models. Aski does not use it to train anything either.

Retention and deletion

While the account is active, the profile, the encrypted credentials, the message history and the billing history are kept. Deletion from the app is immediate and permanent, requires confirmation and re-authentication, and erases chat history, credentials, learned vocabulary, sessions, tokens and the associated security log. Two caveats: billing history is kept for five years under Peruvian tax regulations, with the email anonymized; and a deleted account may remain in backups for up to 30 days, until those copies expire.

What we do not have

Stated by us, so it does not turn up as an audit finding

- **There is no SOC 2 or ISO 27001 certification.**
- **The published pentest is our own**, run and recorded by us; it is not an independent third party's audit.
- **Hosting in the European Union is not offered**, nor data residency by region: the whole infrastructure is in the United States.

Data controller contact: Jhon Jairo Rojas Ortiz · Peru · contacto@aski.dev

We answer security questions and agreement requests within a maximum of 7 business days. If the auditor has a questionnaire, it is answered in writing.

Reference documents: aski.dev/en/security · aski.dev/en/privacy · aski.dev/en/terms