CHATINFLOW SECURITY: HOW YOUR CONVERSATIONS ARE PROTECTED

Where your data lives, how secrets are sealed, sign-in and roles, approvals for big sends, the audit trail, backups and your data rights, with the gaps listed just as plainly.

Updated October 17, 2026 · chatinflow.com/security

A DM automation tool holds some of the most sensitive data a small business has: every conversation with every customer, the tokens that let software post as your brand, and the keys to your AI and payment accounts. Before you connect anything, you should know where that data lives, who can see it, how it is protected and what you can do when something goes wrong. This guide explains ChatinFlow's security in plain terms: the infrastructure, how secrets are sealed, sign-in and sessions, roles and approvals, the audit trail, backups, and your data rights. It also lists, just as plainly, what ChatinFlow does not have yet, so you can judge it against your own requirements.

Key points

- Data is stored on ChatinFlow's servers in a Hetzner data center in Finland, inside the European Economic Area, behind Cloudflare, with the database and cache closed to the internet.
- Channel tokens, integration secrets and AI keys are sealed with AES-256-GCM, with a separate data key for each workspace, and every connection uses TLS 1.2 or 1.3.
- Every account can use two-step sign-in with an authenticator app and sign out every other session; Business and up add single sign-on through OpenID Connect and an IP allowlist.
- Roles, custom roles and a second approval for flows and broadcasts that reach many people keep one click from reaching everyone by mistake.
- ChatinFlow does not hold a SOC 2 report or an ISO 27001 certificate; this guide describes the controls that are in place today.

WHERE YOUR DATA LIVES

ChatinFlow runs on its own servers in a Hetzner data center in Finland, inside the European Economic Area. The dashboard, the API and the automation workers run there, and contacts, conversations and uploaded files are stored on the same servers, closed to the internet: the database and cache accept no connections from outside.

Cloudflare sits in front of chatinflow.com. It filters traffic before it reaches the servers, absorbs attacks and serves the site's static files from a nearby location. Every connection between your browser, the platforms and ChatinFlow is encrypted with TLS 1.2 or 1.3, and HSTS tells browsers never to fall back to an unencrypted connection.

Layer	What protects it
Network edge	Cloudflare in front of chatinflow.com, filtering traffic and absorbing attacks
Connections	TLS 1.2 or 1.3 only, with HSTS
Database and cache	Closed to the internet, reachable only from the servers themselves
Secrets	AES-256-GCM, with a separate data key for each workspace
Backups	A nightly copy of the database and uploaded files
Monitoring	An automated health check every five minutes

HOW SECRETS ARE SEALED

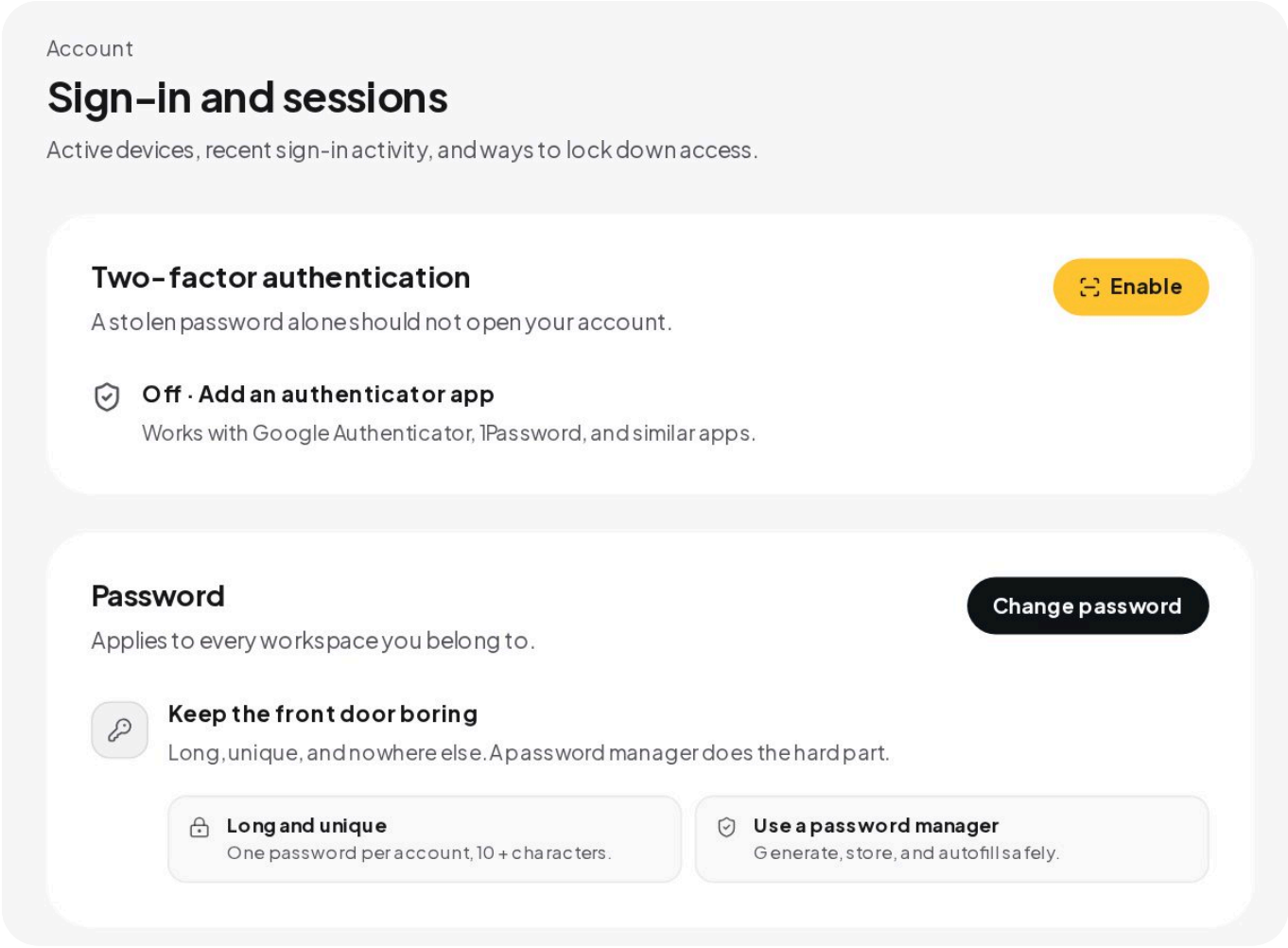
The most valuable things in a ChatinFlow workspace are not messages but keys: the token that lets ChatinFlow answer as your Instagram account, the secret of a webhook, your OpenAI or Stripe key. A leaked token is worse than a leaked conversation, because someone could send as you.

ChatinFlow seals them with envelope encryption before they reach the database. Each workspace has its own data key; each secret is encrypted with AES-256-GCM under that key. After you save a key, the dashboard only ever shows a masked preview. If you rotate a key at the provider, update it in ChatinFlow and the old one is replaced.

Payments work the same way from the other side: card details never reach ChatinFlow at all. Subscription payments are handled by Paddle and Stripe, and Buy button payments in your flows go through your own Stripe or PayPal account, straight to you.

STEP 1: LOCK DOWN SIGN-IN

Open **Settings, Security**. Three things live here.



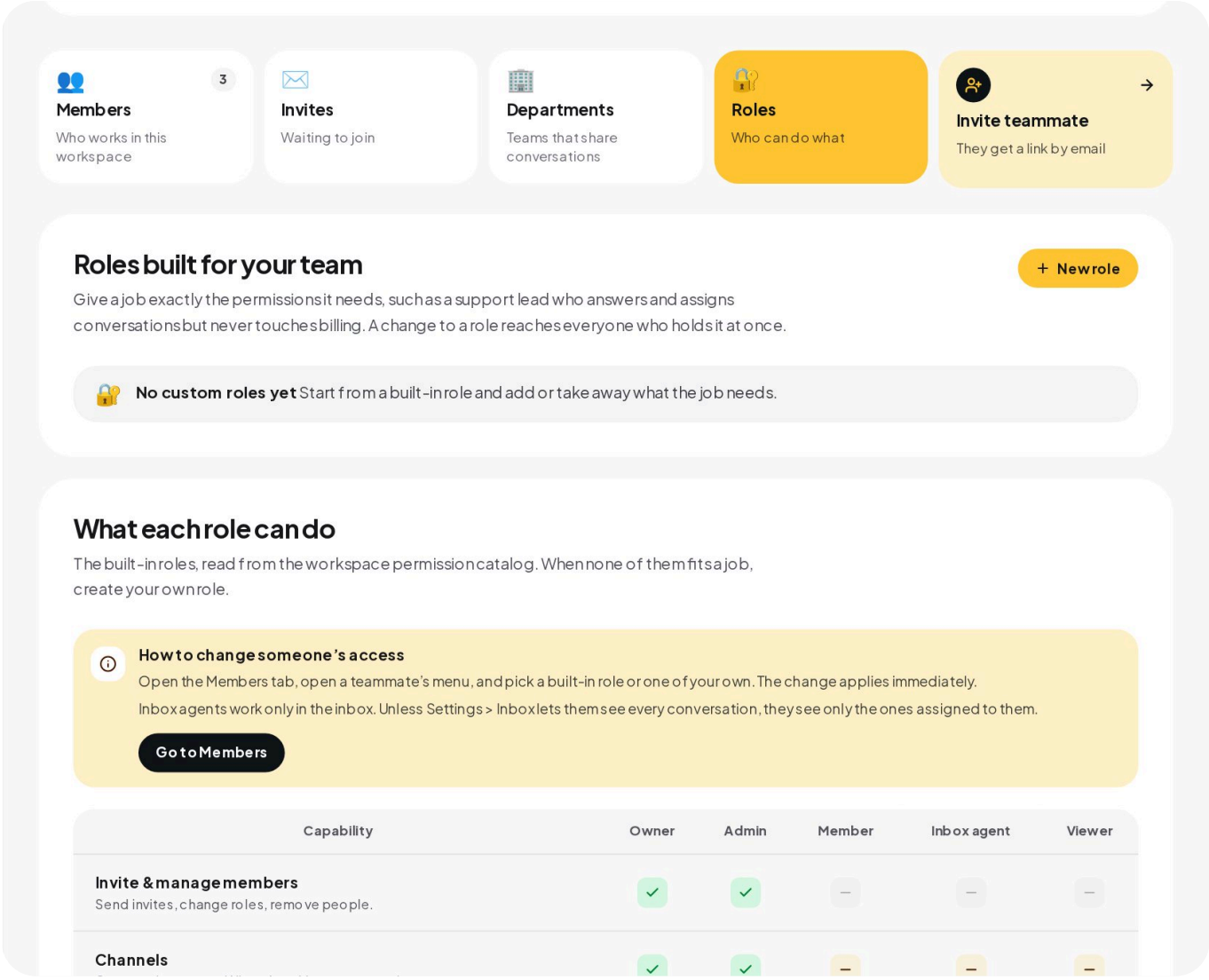
Turn on two-factor authentication and keep a long, unique password.

- **Two-factor authentication.** A stolen password alone should not open your account. Turn it on with Google Authenticator, 1Password or a similar app, on every plan. After that, each sign-in asks for the six-digit code.
- **Password.** It applies to every workspace you belong to. Long, unique and stored in a password manager is the whole recipe.
- **Active sessions and recent activity.** Every device signed in to your account is listed, with the browser, the system and the time. Revoke one, or revoke all other sessions in one click when a laptop goes missing.

Sign-in with an outside identity is guarded too. A social login or single sign-on is never attached to an existing account with the same email that has not been verified, which closes a common account takeover trick.

STEP 2: GIVE EACH PERSON THE RIGHT ROLE

Open **Team** to invite teammates and choose their roles. The **Roles** tab shows what each built-in role can do, capability by capability.



Built-in roles side by side, and room for your own.

- **Owner and Admin** can do everything in the table: invite and manage members, connect channels, build and publish automations, launch broadcasts, change the plan and read the audit log.
- **Member** works in the inbox and with contacts, with limited access to channels, automations, deals and broadcasts, and no access to members, billing or the audit log.
- **Inbox agent** works only in the inbox. Unless Settings, Inbox lets them see every conversation, they see only the ones assigned to them, and they cannot build automations or launch broadcasts.
- **Viewer** has limited access across the workspace and cannot manage members, billing or the audit log.

When none of them fits a job, create a **custom role**: start from a built-in role and add or take away what the job needs, such as a support lead who answers and assigns conversations but never touches billing. A change to a role reaches everyone who holds it at once.

STEP 3: REQUIRE A SECOND PAIR OF EYES FOR BIG SENDS

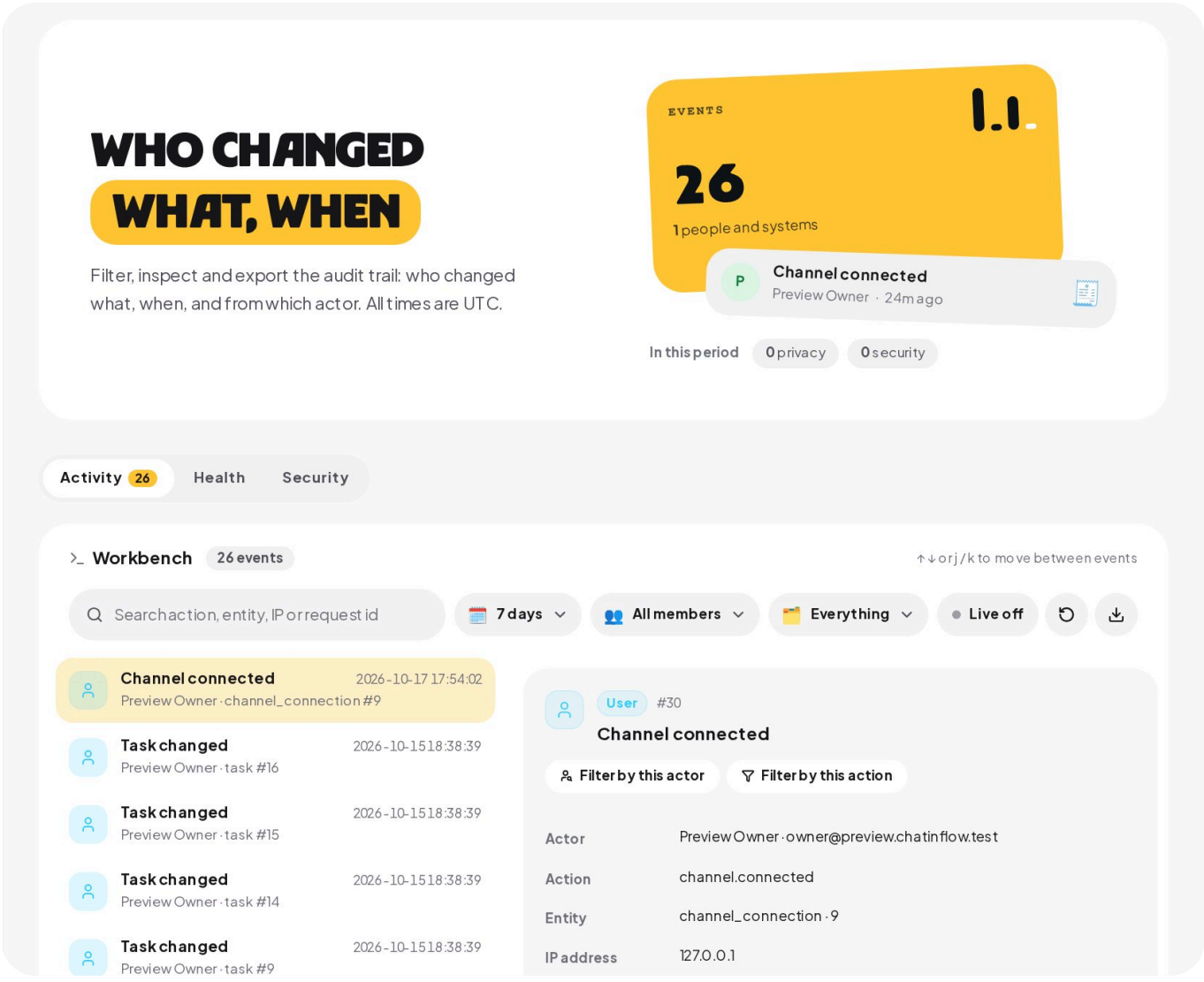
A flow or a broadcast that can message a large share of your contacts does not go live on one person's click. When a flow with a sending step is published in a workspace with 1,000 contacts or more, or a broadcast's audience reaches 1,000, another teammate who can publish approves it first. If you are the only one who can

publish, you approve your own request with a fresh two-factor code. The approval covers what was reviewed, so changing the content asks again.

This is the control that prevents the worst automation accident: a test message sent to everyone.

STEP 4: KEEP AN AUDIT TRAIL

Every change in the workspace is written down. Open the **Workbench** to see who changed what, when and from which actor.



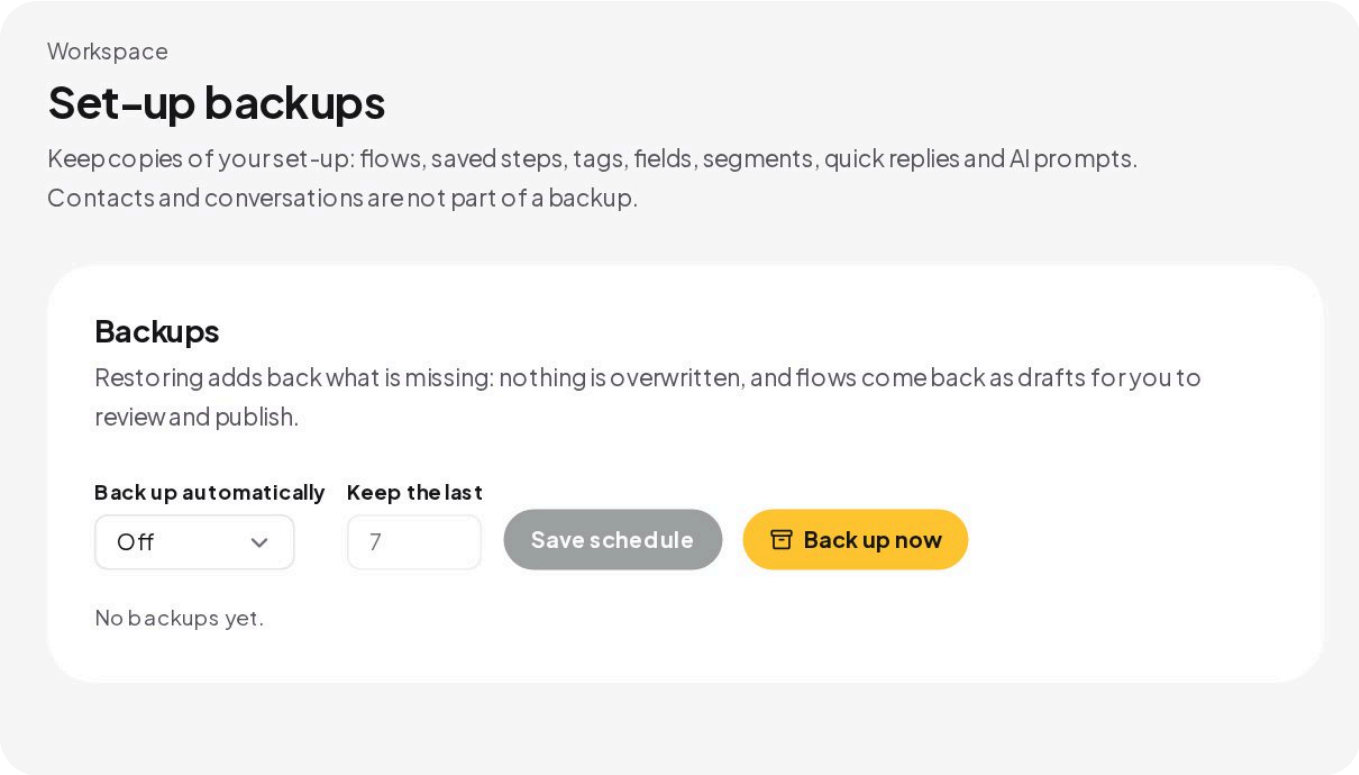
Filter, inspect and export the audit trail. Demo workspace.

- **Activity** lists workspace changes, such as a channel connected, a flow published or a member's role changed, with the actor, the time and the details.
- **Security** lists security events in their own view, apart from everyday changes.
- **Filters** narrow the list by time range, by member and by kind of event, and every event shows its details and IP address.
- **Export** downloads every event that matches the current filters as CSV, on eligible plans, for your own reviews.

All times are in UTC, so events from different time zones line up.

STEP 5: BACK UP YOUR SET-UP

The database and uploaded files are backed up every night. On top of that, workspaces on eligible plans can keep their own copies of their set-up under **Settings, Backups**.

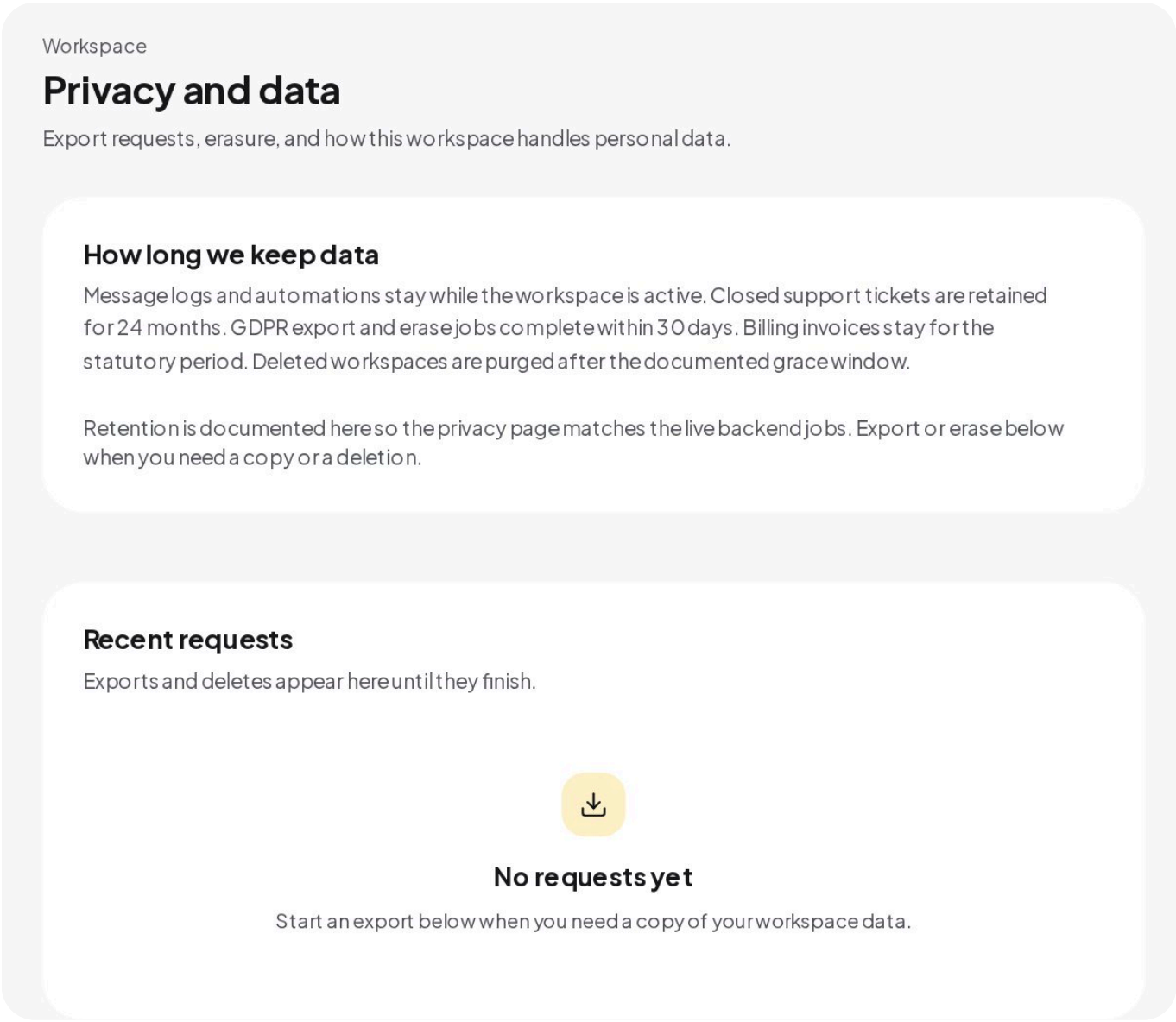


Back up flows, saved steps, tags, fields, segments, quick replies and AI prompts.

A set-up backup holds your flows, saved steps, tags, custom fields, segments, quick replies and AI prompts. Contacts and conversations are not part of it. Restoring adds back what is missing without overwriting anything, and flows come back as drafts for you to review and publish. Keep the last several backups on a schedule, or press Back up now before a big change.

STEP 6: HANDLE DATA REQUESTS FROM THE DASHBOARD

Customers have rights over their data, and so do you. **Settings, Privacy** handles the requests without a support ticket.



Export the workspace, erase a contact or delete your account, from the dashboard.

- **Export workspace data.** Messages, contacts and metadata as a downloadable archive.
- **Erase a contact.** Delete them in Audience when a customer asks to be forgotten.
- **Delete your account.** From your profile; your personal data is erased after a grace period you can cancel.
- **Retention.** Message logs and automations stay while the workspace is active, closed support tickets are kept for 24 months, and export and erase jobs complete within 30 days.

STEP 7: SINGLE SIGN-ON AND IP ALLOWLISTS FOR LARGER TEAMS

Business and up add two controls for teams with an IT department.

Single sign-on through OpenID Connect. Connect your identity provider, such as Okta, Microsoft Entra ID or Google Workspace, and verify your email domain with a DNS TXT record. With single sign-on required, members can no longer sign in with a password or a social login; the owner keeps a way in.

An IP allowlist. The owner can limit where members reach the workspace from: the dashboard, API keys, the realtime connection and notifications. Paths your customers use, such as the website chat and booking pages, are not affected.

AI AND OUTSIDE PROVIDERS

AI replies and the inbox helpers run on keys you connect, from OpenAI, Anthropic, Google Gemini or Azure OpenAI. Without a key, no conversation text is sent to an AI provider, and ChatinFlow does not train any model on your workspace. When those features run, the text goes to the provider you picked, under your account and that provider's terms. Incoming voice messages are transcribed automatically on ChatinFlow's own servers in Finland, in a process with no network access, so that audio never leaves them. Only when a teammate presses Transcribe on one message while that service is unavailable is the message sent to OpenAI, on the workspace's own key and only if one is connected.

The companies that process data for ChatinFlow itself are Hetzner, for hosting, Cloudflare, for the network edge, and Paddle and Stripe, for payments. Channels and tools you connect, such as Meta's apps, Telegram or your CRM, receive data because you connected them.

WHAT CHATINFLOW DOES NOT HAVE YET

Honest gaps help you decide.

- **No SOC 2 report or ISO 27001 certificate.**
- **No SAML and no SCIM.** Single sign-on works through OpenID Connect.
- **No end-to-end encryption.** Messages are encrypted in transit and stored on servers closed to the internet, but ChatinFlow can read them to run your automations.
- **No region choice.** Workspaces are hosted in Finland.
- **No paid bug bounty.** Security reports are welcome at security@chatinflow.com.

REPORTING A SECURITY ISSUE

Found a problem? Email security@chatinflow.com with the steps to reproduce it and its impact, and give ChatinFlow the chance to fix it before you share it publicly. The scope is chatinflow.com and its API.

TERMS IN THIS GUIDE

- **Envelope encryption.** Each workspace has its own data key, and each secret is encrypted with AES-256-GCM under that key.
- **Two-step sign-in.** A six-digit code from an authenticator app at each sign-in, available on every plan.
- **Second approval.** A check before a flow or broadcast that can reach 1,000 or more contacts goes live: another teammate who can publish confirms it.

- **Set-up backup.** A planned copy of flows, saved steps, tags, fields, segments, quick replies and AI prompts, restored without overwriting anything.

QUICK ANSWERS

Is two-factor authentication available on the free plan?

Yes. Two-step sign-in with an authenticator app works on every plan, as does signing out every other session.

Can an inbox agent see every conversation?

Only if you allow it. By default an inbox agent sees the conversations assigned to them; Settings, Inbox can let them see every one.

Are contacts part of a set-up backup?

No. A set-up backup holds flows, saved steps, tags, fields, segments, quick replies and AI prompts. The database itself, contacts and conversations included, is backed up every night.

Where do I see who changed a flow?

In the Workbench audit trail. Filter by the member or by the kind of event, and open the event for its details.

SOURCES

- **General Data Protection Regulation**, the full text, on data subject rights.
- **How OpenID Connect works**, OpenID Foundation, on single sign-on with OpenID Connect.
- **RFC 6797 : HTTP Strict Transport Security**, IETF.

DO IT IN SECONDS, FREE

chatinflow.com/security