

Privacy Policy

Version 2.2 — September 13, 2026

WHAT CHANGED

Added Logo.dev among the providers (display of company logos on oto.cx and in Scout).



Our Commitment

In short: oto is built with privacy as a principle. Your secrets are encrypted (AES-256-GCM), bound to their location, isolated per user and partitioned per organization. This policy describes what the Publisher processes on its own behalf; what you entrust to the platform is covered by the DPA.

We believe your data belongs to you. oto minimizes data collection and encrypts sensitive items: your secrets and credentials for third-party tools are encrypted at rest (AES-256-GCM), with the master key kept out of the database. Each encrypted secret is **bound to its row**: it cannot be transplanted to another connector or another organization. Secrets are **isolated per user** and **partitioned per organization**. An organization can **require two-factor authentication** from its members.

The data controller is **Otomata**, a SASU registered in Marseille (SIREN 106 974 637, EU VAT FR05106974637) — see the [legal notice](#).

Two roles, two documents. This policy covers the processing for which the Publisher is the **controller on its own behalf**: your account and organization, billing, the proof of acceptance of the contractual documents, the technical call log, platform monitoring and security. The data you **entrust to the platform** — content, contacts, messages and documents handled by your connectors and agents — is processed on your behalf, as a processor: it is governed by the [data processing agreement \(DPA\)](#). Details of our security measures are published on [trust.oto.zone](#).



What We Don't Collect

In short: No ad cookies, no ad networks, no data selling, no card data on our servers.
No analytics or session replay before your explicit consent.

Ad cookies — No advertising cookies, no ad networks, no retargeting pixel.

Fingerprinting — We don't use any browser fingerprinting techniques.

Data selling — Your data is never sold, traded, or shared for commercial purposes.

No tracker without consent — No analytics and no session replay is active before your explicit agreement. The oto.cx website has none at all.

Card data — Card number and security code are entered on a page hosted by our payment provider and never pass through our servers.

Internal variables in error tracking — An error report contains neither the arguments of your calls nor the program's internal variables.



What We Collect

In short: What is needed to run your account and organization, bill a subscription and prove acceptance of the contractual documents.

Account and organization

Data	Purpose	Legal basis
Sign-in identity (Logto), email address, name, avatar, preferred language	Authentication, account identification, notifications	Contract
Two-factor authentication factors, when your organization requires them (held by the authentication service)	Account security	Contract
Usage profile (job, goals, desired connectors), filled in by you or by your agents	Tailoring the session to your context	Contract
Organizations, members, roles, invitations	Access management	Contract
Secrets and credentials for connected tools (encrypted AES-256-GCM)	Running automations	Contract
Content (pages, documents, files, tables) and its search index	Search and running your automations	Contract — processed on your behalf, see DPA

Billing (subscribed organizations)

Data	Purpose	Legal basis
Billing identity: legal name, country, EU VAT number, address, postal code, city, billing email address	Determining the applicable VAT, issuing the invoice	Contract, legal obligation
Subscription: tier, status, billing dates, customer and mandate identifiers at Mollie	Subscription and charge management	Contract
Payment log: amounts excluding VAT, VAT and including VAT, VAT scheme, country retained, Mollie payment identifiers, status, attempt number	Collection, reconciliation, handling of failed payments	Contract, legal obligation

Data	Purpose	Legal basis
Invoices and credit notes: number, amounts, period covered, PDF document, recipient address and sending date	Accounting and tax obligations	Legal obligation
The amount charged, its breakdown and the VAT scheme are frozen at each payment and shown on the corresponding invoice (see the terms of sale). Proof of acceptance of the contractual documents Each acceptance of the terms, the terms of sale and the DPA is logged, never overwritten: account, organization on whose behalf it is given, document and version accepted, context (access to the service or purchase), IP address, browser (user-agent string, truncated to 512 characters) and date. Purpose: proof of contractual consent. Legal basis: legitimate interest (establishing evidence).		



Call Log & Retention Periods

In short: Every tool call is logged, with truncated arguments and masked secrets. The log stays available for 90 days, then goes to an offline archive. Billing data is kept for ten years.

Call log. Every tool call (by an agent via MCP, or by the dashboard via the API) is logged: date, account (identifier and email), tool called, **truncated arguments** — tokens and secrets are **masked at write time** —, success or error, duration, session, run, organization, client application (for example claude.ai or Claude Code) and, for a code error, the identifier of the error report. Purposes: platform monitoring, **your organization's audit log** (available to its administrators), reconstruction of your runs, incident investigation. Legal basis: contract and legitimate interest.

Data	Retention period
Call log	90 days online; beyond that, each closed month is exported to an offline archive (private object, storage hosted in the European Union) and then deleted from the database. The opening and closing facts of a run are kept with it.
Execution thread of hosted agents (intermediate messages)	30 days
Usage counters per tool and per day; usage signals (feedback on a tool, unmet need)	Lifetime of the account
Account, organization, content and secrets	Lifetime of the account; deletion on request (see "Your rights")
Billing identity, payment log, invoices and credit notes	Ten years from the close of the financial year (accounting records, Article L.123-22 of the French Commercial Code)
Proof of acceptance of the contractual documents	For the applicable limitation period
Error reports (Sentry)	Kept by the provider, in the European Union, for diagnosis



Cookies, Local Storage & Analytics

In short: The `oto.cx` website sets no cookie and no tracker. The `manage.oto.cx` dashboard uses the browser's local storage for the session and preferences, and analytics with session replay (PostHog, EU) **only after your consent**.

Item	Where	Purpose	Type
<code>Lang</code> (local storage)	<code>oto.cx</code>	Remember your language	Essential
Authentication session (local storage; session cookies on <code>auth.oto.zone</code>)	<code>manage.oto.cx</code> , <code>auth.oto.zone</code>	Stay signed in	Essential
<code>oto-analytics-consent</code> (local storage)	<code>manage.oto.cx</code>	Remember your consent choice	Essential
Display preferences (local storage)	<code>manage.oto.cx</code>	Chosen view and layout	Essential

oto.cx website. No cookie, no analytics: only your language preference is remembered in your browser's local storage.

manage.oto.cx dashboard. We measure dashboard usage with **PostHog** (hosted in the European Union), which starts **disabled** and is enabled **only after your explicit agreement** via the dedicated banner. After consent, PostHog collects page views and actions, performs **session replay** (input fields are **masked**), and links the session to your account (identifier, email, role, active organization). Data passes through a relay on our own domain before reaching PostHog. Without consent, nothing is collected. You can withdraw your consent at any time by writing to us, or by clearing your browser's site data so that the banner is shown to you again.



Error Tracking

In short: Code errors are sent to Sentry (EU) with the tool name and your account identifier — never with the arguments of your calls, internal variables, your IP address or your cookies.

To detect and fix platform defects, **code errors** are sent to **Sentry** (hosted in the European Union, Germany):

Server side — error type, message, stack trace, tool name and account identifier. The report **contains no internal variables, no call arguments, no IP address, no cookies and no headers**. Refusals from third-party services and input errors are not sent: they are not platform defects.

Dashboard side — JavaScript errors and account identifier, with no IP address, no session replay and no performance tracing.

Legal basis: legitimate interest (reliability and security of the service). This processing is not subject to the analytics consent.



Processors & Providers

In short: The processors are those of DPA 2.1, in three families: sub-processors, connector services (used only if you enable them) and the Publisher's billing providers. They are joined by one of the Publisher's technical providers, for displaying company logos.

Sub-processors (process on behalf of your organizations, bound by an Article 28 GDPR contract):

Scaleway — Hosting, database, object storage, secrets management, transactional email — European Union (France)

Logto — OAuth 2.0 / PKCE authentication and two-factor authentication (self-hosted by the Publisher at Scaleway) — European Union (France)

Mistral AI — Vectorization of the text of your pages, documents and files, solely for search within the platform (API mode, no training on submitted content) — European Union (France)

Sentry — Technical error tracking — European Union (Germany)

PostHog — Dashboard analytics and session replay, *only after consent* — European Union

Anthropic (Claude) — AI assistant used by the Publisher's team for operations, support and hands-on services (may occasionally process customer data in that context) — API mode with no training on submitted content; transfers outside the EU covered by standard contractual clauses — United States

Connector services (used only if you enable and use the connector):

Unipile — Hosted messaging: the session of your messaging or social network account is operated at Unipile, which processes your messages and your correspondents' data in the process — European Union (France)

Browserbase — Hosted browser, which holds the session profile you open — United States; transfers covered by standard contractual clauses

Other connector services — up-to-date list, with role and location, on trust.oto.zone

When you connect a tool with **your own key or your own account**, oto carries out your instruction with a service you already have a relationship with: the Publisher adds no processor.

The Publisher's billing providers (the Publisher's own processing):

Mollie B.V. — Collection of subscription payments; electronic money institution licensed and supervised by the Dutch central bank — Netherlands (European Union)

Pennylane — Issuance of invoices and credit notes on the Publisher's books; receives your organization's legal name, address, VAT number and billing email address —

European Union (France)

In accordance with Article 28 GDPR, the [data processing agreement \(DPA\)](#) governs this processing; it is also available on [trust.oto.zone](#). Transfers outside the European Union (Anthropic, Browserbase) are covered by the European Commission's standard contractual clauses.

The Publisher's technical providers (the Publisher's own processing, contacted directly by your browser):

Logo.dev — Display of company logos on oto.cx and in Scout (receives the domain of the company displayed, the visitor's IP address and referring page) — United States



Your Rights (GDPR)

In short: You have control over your data. Access, rectification, deletion, portability, objection, withdrawal of consent — on request.

Access — Get a copy of your data

Rectification — Correct inaccurate data (your profile and your organization's billing identity can be edited from [manage.oto.cx](#))

Deletion — Have your data erased, on request. Invoices, the payment log and the proof of acceptance are kept for the legal periods stated above.

Portability — Get your data in a standard format

Objection — Object to processing based on legitimate interest

Withdrawal of consent — Withdraw your agreement to analytics at any time

Complaint — To the [CNIL](#) (French data authority)

To exercise your rights: email alexis@otomata.tech. We respond within 30 days.

This policy supplements the [legal notice](#), the [subscription terms](#), the [terms of sale](#) and the [data processing agreement \(DPA\)](#). Previous versions remain available.