

Data Processing Agreement (DPA)

Version 2.1 — August 29, 2026

WHAT CHANGED

Sub-processor list updated and restructured into three families. Added Mistral AI (vectorization for semantic search), Unipile (hosted messaging) and Browserbase (hosted browser), previously covered only by the generic clause. Stancer replaced by Mollie, and Pennylane added (invoicing) — both now presented as the Publisher's own billing providers. Added two-factor authentication as an organization requirement and the cryptographic binding of secrets to their row in the security measures. Trust center moved to trust.oto.zone.



Purpose & roles

In short: This agreement governs, under Article 28 GDPR, the personal-data processing carried out by oto on behalf of its customers. The Customer is the controller; the Publisher is the processor.

This data processing agreement ("DPA", version 2.1) supplements the [subscription terms](#) and governs, in accordance with **Article 28 GDPR**, the processing of personal data carried out by the Publisher (Otomata, a SASU registered in Marseille, SIREN 106 974 637, intra-EU VAT FR05106974637 — the "processor") on behalf of the Customer (the "controller").

Subject and duration: provision of the oto automation platform, for the duration of the subscription. **Nature and purpose:** hosting, running the automations requested by the Customer and its agents, indexing the Customer's content so that it can be searched, encrypted storage of connection secrets. **Categories of data subjects and data:** determined by the Customer based on the tools it connects and the processing it triggers. The processor processes this data **on the controller's documented instructions** and uses it for no other purpose.

What this agreement does not cover. The Publisher acts as a **controller on its own account** for the processing that is its own: account and organization management, billing identity and billing contact, collection and invoicing of the subscription, and the timestamped record of acceptance of the contractual documents. That processing is described in the [privacy policy](#) and in the [terms of sale](#).

A signable version of this agreement is made available to customers on [trust.oto.zone](#).



Sub-processors

In short: The controller authorizes the sub-processors listed below and is informed of any change, with the ability to object.

The controller authorizes the Publisher to use the following sub-processors, each bound by an Article 28-compliant contract:

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

Logto — Authentication (self-hosted by the Publisher at Scaleway) — European Union (France)

Mistral AI — Vectorization of the text of the Customer's pages, documents and files, solely for semantic search within the platform (`mistral-embed` model, API mode, no training on submitted content) — European Union (France)

Sentry — Monitoring and logging of technical errors (may contain personal data) — European Union (Germany)

PostHog — Audience measurement on the website and dashboard, 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

The Publisher informs the controller of any addition or replacement of a sub-processor, allowing a reasonable period to object on legitimate grounds.



Connector services

In short: Some connectors rely on third-party services, engaged only if you enable and use them. The two main ones are named below; the up-to-date list lives on trust.oto.zone.

oto connects to third-party tools. Two cases must be distinguished, and they do not have the same regime:

Your own access. When you connect a tool with **your own key or your own account** (the most common case in the catalog), oto carries out your instruction by calling a service you **already have a contract with**. The Publisher adds no sub-processor: it carries your request and your credential, which it stores encrypted.

Services the Publisher makes available. Some connectors rely on a third-party service contracted by the Publisher, engaged **only if you enable and use that connector**:

Unipile — Hosted messaging: the session of your messaging or social account (LinkedIn, WhatsApp, Telegram, Instagram, Messenger, X) is operated at Unipile, which in that context processes your messages and your correspondents' data — European Union (France)

Browserbase — Hosted browser, to read a site behind authentication from a session you open yourself; it holds the corresponding session profile — United States; transfers covered by standard contractual clauses

Other connector services — other connectors (company data, enrichment, search) may rely on third-party services contracted by the Publisher and possibly operating outside the European Union, covered by standard contractual clauses

The **up-to-date list** of these services, with their role and location, is published on trust.oto.zone. The Publisher applies to them the same commitment to prior notice and right to object as to sub-processors.



The Publisher's billing providers

In short: Collection and invoicing of the subscription are the Publisher's own processing. They are listed here for information: Mollie collects, PennyLane issues the invoices.

The processing below is that of the **Publisher acting on its own account** — it does not concern the data the Customer entrusts to the platform. It is listed here for the controller's complete information:

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

PennyLane — Issuing subscription invoices and credit notes, on the Publisher's own accounts; processes the Customer's billing identity and billing contact — European Union (France)



Security measures

In short: Encryption at rest of secrets (AES-256-GCM), master key kept out of the database, per-user isolation, two-factor authentication available as an organization requirement, multi-level revocation. Details on trust.oto.zone.

The Publisher implements appropriate technical and organizational measures (Article 32 GDPR):

Encryption at rest of secrets and connection credentials (AES-256-GCM), with the **master key kept out of the database** and never written in clear on disk. Each encrypted secret is **cryptographically bound to its row**: a secret cannot be transplanted to another connector or another organization.

Per-user isolation of secrets and per-organization partitioning.

Authentication via OAuth 2.0 / PKCE (self-hosted Logto), end-to-end encrypted transport (TLS). An organization may **require two-factor authentication** from its members.

Revocation at several levels: removing a user's access, deleting an organization credential.

Restricted-privilege remote connectors ("bridges") for sensitive access (read-only depending on the deployment): the customer credential lives in an isolated service, never in the platform. *Option*: this service can be hosted within the customer's own infrastructure (the credential then never leaves their cloud) — offered case by case, not the default configuration.

The details of these measures, their deployment status, and the hardening in progress are published on trust.oto.zone. The Publisher notifies the controller of any breach affecting its data without undue delay after becoming aware of it.



Hosting & location

In short: Data hosted in the European Union (France, Scaleway). Any transfers outside the EU are covered by standard contractual clauses.

Customer data is hosted in the **European Union** (France, Scaleway fr-par region): managed database, object storage, secrets vault, transactional email.

Two sub-processors operate **outside the European Union: Anthropic** (the Publisher's operations tooling) and **Browserbase** (hosted browser, optional connector), both in the United States. Other optional connector services may also operate outside the Union. In all such cases, transfers are covered by the appropriate safeguards under the GDPR (European Commission **standard contractual clauses**, with supplementary measures where relevant).



Controller rights & obligations

In short: Assistance with data-subject requests, breach notification, audit, and deletion or return of data at the end of the contract.

As processor, the Publisher undertakes to:

Instructions — Process data only on the controller's documented instructions.

Confidentiality — Ensure the confidentiality of the data and of the persons authorized to process it.

Assistance — Help the controller respond to data-subject rights requests and meet its security and notification obligations.

Breaches — Notify the controller of any data breach without undue delay.

Audit — Make available the information needed to demonstrate compliance with Article 28 and allow reasonable audits.

End of contract — Delete or return the data at the controller's choice at the end of the service, unless a legal retention obligation applies. Cancelling a subscription, or its closure for non-payment, does not on its own cause **any deletion of data**: it closes access rights to paid features.

The controller, for its part, warrants that it has a legal basis for the processing it triggers via oto and for the data it connects.

This DPA forms an integral part of the [subscription terms](#) and is governed by French law. A signable version is available on trust.oto.zone.

[Privacy Policy](#) [Subscription Terms](#) [Terms of Sale](#) [Legal Notice](#)