

Data Processing Agreement (DPA)

Version 2.0 — July 10, 2026

WHAT CHANGED

Added the processor's intra-EU VAT number (FR05106974637). Agreement otherwise unchanged.



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") 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, 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.

A signable version of this agreement is made available to customers on trust.oto.ninja.



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, storage, secrets management, transactional email — European Union (France)

Stancer — Collecting subscription payments; payment institution supervised by the French ACPR — France

Logto — Authentication (self-hosted at Scaleway, EU)

PostHog — Audience measurement, only after consent — European Union

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

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

Optional connector services — some connectors (e.g. hosted browser, messaging) rely on third-party services, enabled only if you use them and possibly operating outside the EU (covered by standard contractual clauses); up-to-date list on trust.oto.ninja

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



Security measures

In short: Encryption at rest of secrets (AES-256-GCM), master key kept out of the database, per-user isolation, multi-level revocation. Details on trust.oto.ninja.

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.

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

Authentication via OAuth 2.0 / PKCE (self-hosted Logto), end-to-end encrypted transport (TLS).

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.ninja. 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.

Some sub-processors (notably Anthropic, for the Publisher's operations tooling, and certain optional connector services) may operate outside the EU. In that case, 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.

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.ninja.

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