Personal Data Processing Agreement

Under Article 28 GDPR · Version 1.12 (setembro de 2026)

1. Parties

Controller: the customer identified on the account Recato (hereinafter the «Customer»).
Processor: Forsnaps AI - Soluções Tecnológicas, Unipessoal Lda, VAT no. 518932494, with registered office at Rua da Igreja Nº99, Varziela, 4650-722 Felgueiras (hereinafter the «Provider»).

This agreement forms an integral part of the Terms of Use and applies to all processing of personal data carried out by the Processor on behalf of the Customer in providing the service Recato, where the Customer is a company, an entity or a professional. It does not apply to an individual using the service for purely personal or household purposes: in that case the Provider is the controller of the account data, under the Privacy Policy, and maintains the same commitments on location, non-use for training, retention and security described here.

2. Subject matter, nature and purpose

Hosting, processing and provision of an artificial intelligence assistant for the Customer's users, including storage of conversations and submitted files, generation of answers by language models, management of accounts and usage, and, where the user connects one, access to their mailbox to read and send on their behalf.

3. Categories of data and data subjects

Data subjects: the Customer's users (staff and others they invite) and any individuals referred to in the content submitted (clients, suppliers, patients, parties to proceedings, among others), according to how the Customer uses the service; senders and recipients of emails in a connected mailbox.
Data: identification and contact details of users; the content of conversations and files, which may include any category of data, including special categories, under the Customer's responsibility; credentials for the connected mailbox and the content of the emails processed.

4. Obligations of the Processor

1. Process the data only on documented instructions from the Customer, being the account settings and the use of the service, save where legally required.
2. Ensure that persons authorised to process the data are bound by confidentiality.
3. Apply the technical and organisational measures set out in Annex II.
4. Not engage other sub-processors without informing the Customer 30 days in advance, giving them the opportunity to object; the current list is in Annex I.
5. Assist the Customer in complying with its obligations to respond to data subjects, on security, on breach notification and on impact assessments.
6. Notify the Customer of any personal data breach without undue delay and within 48 hours of becoming aware of it.
7. Delete or return all data at the end of the provision of the service, as the Customer chooses, and delete existing copies within a maximum of 90 days, save where retention is legally required.
8. Make available the information necessary to demonstrate compliance with these obligations and allow audits, on 30 days' notice and at most once a year, save in the event of an incident.

5. Location and transfers

All processing carried out by the Processor takes place within the European Union, and the Processor does not engage sub-processors outside the European Economic Area. Where a user connects their mailbox, the Processor communicates with the Customer's mail provider on the Customer's instruction; that provider is contracted by the Customer and is not a sub-processor of the Processor.

6. No use for training

The Processor and its sub-processors do not use the Customer's data to train, fine-tune or evaluate artificial intelligence models. Requests sent to the inference sub-processor are not retained by it once answered.

7. Usage measurement

The Processor measures use of the service, including within the Customer's space, in order to understand at which step users stop being able to use it and to fix what is blocking them. That measurement records only the step, the plan, the date and time, the country and the type of browser, and a technical identifier of the space; it does not record the content of conversations, the files, names, email addresses or any text written by the Customer's users. Measurement takes place on the Processor's own infrastructure, in the European Union, without third-party analytics services and without cookies. This processing is carried out by the Processor as controller, for the administration and improvement of the service, under Recital 49 and Article 6(1)(f) GDPR, and does not constitute use of the Customer's data for the Processor's own purposes within the meaning of Article 28(10).

8. Retention

The Customer controls the retention period for conversations, files and memories through the account settings. The Processor carries out the automatic deletion as configured and logs its execution. The Processor does not submit conversations to abuse classifiers, nor does it retain content, scores or flagging records on that basis beyond the retention period set by the Customer.

9. Term, return and deletion

It remains in force for as long as the service is provided. Confidentiality obligations survive termination.

Once the provision of the service ends, the Provider deletes or returns to the Customer all personal data processed on its behalf, at the Customer's choice, under Article 28(3)(g) of the GDPR. The return is made through the export available in the account itself, which the Customer performs alone, at any time and at no cost, including the export of the whole workspace with one folder per user; if access is no longer possible, the Provider delivers the same export on request. The data remains available for export for 30 days after termination and is then deleted, including from the backups within a maximum of 90 days, save where the law requires it to be kept.

Annex I: sub-processors

The Processor engages sub-processors in the following categories, all within the European Union and bound by contract to the same obligations. The named list, with each entity and its country, is made available to the Customer on request and notified 30 days in advance whenever it changes.

Category	Service	Location
Language model inference	Generating the answers, with no prompt retention and no training	European Union
Hosting	Application servers, database and files	European Union

Category	Service	Location
Backups	Encrypted storage of the daily backups	European Union
Transactional email	Sending account and notification emails	European Union
Payments	Processing card and local payment methods	European Union

Annex II: technical and organisational measures

- Encryption in transit (TLS 1.2 or above) and at rest (encrypted disk).
- Logical isolation per customer: one database and one file store per account.
- Strong password authentication, optional two-factor authentication, lockout after failed attempts.
- Role-based access control; administrative access by the Processor is limited, logged and for support only.
- Daily encrypted backups, held in the European Union, with periodic restore testing.
- Security event logs retained for 90 days; error monitoring without personal data.
- Server hardening: remote access by key only, firewall, automatic security updates.
- Incident management with a written procedure and notification within 48 hours.

Signed electronically by acceptance of the Terms of Use when the account is created. For a signed paper copy, write to info@recato.pt.