

DATA PROCESSING AGREEMENT

Last updated on October 1st, 2026

This Data Processing Agreement ("**DPA**") forms part of the agreement between:

Processor	Edgar SAS , a French société par actions simplifiée with share capital of €1,000, RCS Compiègne 920 349 073, registered office 20 rue des Maraîchers, 60700 Pontpoint, France, operating the Inrô platform (" Inrô " or the " Processor ").
Data-protection contact	Pierre de Milly, privacy@inroapp.com

and

Customer legal name	_____
Registered address	_____
Registration number	_____
Privacy contact email	_____
Role	(the " Customer " or the " Controller ")

This DPA applies to the Inrô Terms of Service (the "**Terms**"). If the DPA and the Terms conflict on the processing of Personal Data, the DPA prevails.

1. Definitions

"**Data Protection Laws**" means Regulation (EU) 2016/679 (GDPR), the French Data Protection Act, and, where applicable, the UK GDPR and the Swiss FADP. "Personal Data", "Processing", "Controller", "Processor", "Data Subject" and "Personal Data Breach" have the meanings given in the GDPR. "**Customer Personal Data**" means Personal Data that Inrô processes on behalf of the Customer through the Inrô service (the "**Service**").

2. Roles and scope

- 2.1** The Customer is the Controller and Inrô is the Processor of Customer Personal Data, as set out in section 5 of the Terms.
- 2.2** Inrô acts as an independent Controller for its own account, billing, analytics, marketing and trust-and-safety processing, which is governed by the Inrô Privacy Policy and is outside this DPA.
- 2.3** The subject matter, duration, nature, purpose, data types and Data Subjects are described in Annex I.

3. Customer instructions

- 3.1** Inrô processes Customer Personal Data only on the Customer's documented instructions: the Terms, this DPA, and the Customer's use and configuration of the Service (automations, campaigns, inbox, AI agent, integrations).
- 3.2** Inrô informs the Customer if it believes an instruction infringes Data Protection Laws.
- 3.3** The Customer is responsible for having a lawful basis, providing required notices and obtaining required consents for its Data Subjects, including Instagram contacts, and for using the Service in line with Meta's platform terms.

4. Confidentiality

Inrô ensures that personnel authorised to process Customer Personal Data are bound by confidentiality obligations. Only Inrô's internal team has access to Customer Personal Data; no external contractors or agencies do.

5. Security

Inrô implements the technical and organisational measures in Annex II and keeps them appropriate to the risk.

6. Sub-processors

- 6.1** The Customer gives general authorisation to the sub-processors in Annex III.
- 6.2** Inrō will notify the Customer at least 30 days before adding or replacing a sub-processor, by email or by notice on its sub-processors page.
- 6.3** The Customer may object on reasonable data-protection grounds within that period. If the parties cannot resolve the objection, the Customer may terminate the affected Service and receive a pro-rata refund of prepaid fees for the remaining term.
- 6.4** Inrō imposes on each sub-processor data-protection obligations no less protective than this DPA and remains liable for their performance.

7. Hosting, international transfers and AI processing

- 7.1** Customer Personal Data is stored in the EU: application, databases and cache on Heroku (EU region), and media and files on AWS S3 in France (eu-west-3).
- 7.2** When the Customer uses AI features, message content is sent to OpenAI (United States) for processing. Inrō relies on the EU Standard Contractual Clauses and the EU-US Data Privacy Framework for this transfer. Customer Personal Data is not used to train AI models.
- 7.3** Where Customer Personal Data is otherwise transferred to a country without an adequacy decision, Inrō relies on the same mechanisms.
- 7.4** Where the Customer is not established in the EEA, Module 2 (controller to processor) of the Standard Contractual Clauses is incorporated by reference, with the Customer as exporter and Edgar SAS as importer; Annexes I to III serve as the annexes to the Standard Contractual Clauses.

8. Data Subject rights

Inrō will, taking into account the nature of the processing, assist the Customer with requests to exercise Data Subject rights (access, rectification, deletion, restriction, portability, objection). Inrō forwards requests it receives directly from Data Subjects to the Customer without responding, unless legally required.

9. Personal Data Breach

- 9.1** Inrō notifies the Customer without undue delay, and within 48 hours of becoming aware of a Personal Data Breach affecting Customer Personal Data.
- 9.2** The notification includes, as far as known: the nature of the breach, categories and approximate number of Data Subjects and records, likely consequences, and the measures taken or proposed.

10. Assistance

Inrō provides reasonable assistance with the Customer's obligations on security, breach notification, data protection impact assessments and prior consultation with supervisory authorities, taking into account the information available to Inrō.

11. Return and deletion

- 11.1** On termination of the Service, the Customer may export its data through the Service. Inrō deletes Customer Personal Data within 90 days of account closure. Backups are overwritten within their retention cycle (up to 4 days).
- 11.2** Inrō may keep data that it is required to keep by law (for example invoices, 10 years under French law), which remains subject to the confidentiality and security obligations of this DPA.
- 11.3** While the account is active, messages and interactions are kept up to 24 months and contacts are deleted after 24 months of inactivity, unless the Customer deletes data sooner.

12. Audits

- 12.1** Inrō makes available the information necessary to demonstrate compliance with this DPA, including its record of processing activities summary and security documentation on request.
- 12.2** If that is not sufficient, the Customer may audit Inrō once a year, with 30 days' written notice, during business hours, subject to confidentiality, at the Customer's cost, and without disrupting Inrō's operations or

exposing other customers' data.

13. Liability

The liability of each party under this DPA is subject to the limitations in section 11 of the Terms (amounts paid by the Customer in the 12 months preceding the claim), to the extent Data Protection Laws allow.

14. Term, law and jurisdiction

14.1 This DPA takes effect on the date of signature (or acceptance of the Terms) and lasts as long as Inrō processes Customer Personal Data.

14.2 This DPA is governed by French law. The competent courts have jurisdiction, subject to any mandatory rule to the contrary and to the Standard Contractual Clauses where they apply.

Signatures

	Edgar SAS (Inrō)	Customer
Name		
Title		
Signature		
Date		

Annex I - Description of the processing

Subject matter	Providing the Inrō Service to the Customer
Duration	Term of the Terms, plus the deletion period in section 11
Nature	Storage, retrieval, organisation, transmission, analysis and deletion of Instagram conversations and contact data; automated replies and campaigns; AI-generated replies
Purposes	Operating the inbox, automations, campaigns, CRM and AI agent for the Customer
Data Subjects	The Customer's Instagram contacts, followers and leads
Personal Data	Messages, comments, media, Instagram profile and interaction data, contact details and custom contact properties, and data from integrations enabled by the Customer. Source is the official Instagram API; there is no contact import
Special categories	None intended. The service is for business use, 18+. The Customer must not use the Service to collect special-category data without a valid basis; messages may incidentally contain such data
Retention	Messages and interactions up to 24 months; contacts deleted after 24 months of inactivity; account data deleted within 90 days of closure; backups 4 days
Frequency	Continuous

Annex II - Technical and organisational measures

Encryption in transit: HTTPS enforced everywhere with HSTS; TLS on all connections to third-party services.

Encryption at rest: AES-256 for third-party access tokens and account secrets; platform-level encryption at rest for the database and file storage; passwords stored with strong one-way hashing; encrypted session cookies.

Tenant isolation: every record is keyed to its owning account and all access is automatically scoped to the current account.

Access control: role-based access within each account; internal-only back-office access; API access requires a per-account secret token or OAuth2 with PKCE.

Application security: per-account rate limiting, parameterised queries, automatic output escaping, verified webhooks, secrets stored encrypted, sensitive fields scrubbed from logs.

Security testing: automated test suite on every change before merge; automated dependency scanning; internal security assessment in November 2025 with no critical or high findings.

Monitoring: error and performance monitoring, slow-request and reply-time alerts, uptime monitoring.

Availability and recovery: stateless, horizontally scalable application and workers; continuous database backups retained 4 days with point-in-time rollback.

Deletion: erasure-based model; data is deleted rather than kept in anonymised form.

Platform integration: Instagram access through the official API as a Meta Tech Provider; Instagram passwords are never stored.

Personnel: access to Customer Personal Data is limited to the internal team, under confidentiality obligations.

Annex III - Authorised sub-processors

Sub-processors that handle Customer Personal Data (Instagram contact data):

Sub-processor	Purpose	Location / transfer basis
Heroku (Salesforce, Inc.)	Application hosting and background processing	EU region
Heroku Postgres	Primary and AI (vector) databases	EU region
Heroku Redis	Cache and job queue	EU region
Amazon Web Services (AWS)	Media and file storage (S3)	France (eu-west-3)
OpenAI	AI features: language model and embeddings	United States; Standard Contractual Clauses and EU-US Data Privacy Framework

Integrations that the Customer chooses to connect (for example Shopify, Calendly, Google Calendar, Airtable, Notion, Make, Zapier) process data under the Customer's own agreement with each provider.

© 2026 Edgar SAS. All rights reserved.