

Data Processing Agreement

Template v1.0 · October 2026 · THE PROJECT MASTER S.A.S. (PMOvio)

Between **[CUSTOMER NAME]**, tax ID **[TAX ID]**, with address at **[ADDRESS]** (the "**Controller**"), and **THE PROJECT MASTER S.A.S.**, a Colombian company with tax ID (NIT) 902.080.975-1, with address at Carrera 3G # 55-49, Bogotá D.C., owner of the PMOvio platform (the "**Processor**"). This agreement forms part of the contract or terms of service under which the Controller uses PMOvio (the "**Contract**").

1. Subject matter

The Processor processes personal data on behalf of the Controller solely to provide the PMOvio service, a project and portfolio management platform, under the Contract and this agreement. The processing is described in Annex I.

2. Applicable law

This agreement is governed by Colombian Law 1581 of 2012 and its regulations. Where processing is subject to Regulation (EU) 2016/679 (GDPR) or another data protection law of the Controller's country, the Parties will also comply with it, and this agreement will be read so as to comply, including Article 28 GDPR.

3. Processor obligations

1. Process the data only on the Controller's documented instructions, which are the Contract, this agreement and the configuration the Controller sets in the platform. The Processor will inform the Controller if it believes an instruction infringes the law.
2. Not use the data for its own purposes, nor sell, assign or disclose it to third parties, except to the sub-processors in clause 5 or where required by law, in which case it will inform the Controller where legally allowed.
3. Ensure that persons authorised to process the data have committed to confidentiality.
4. Apply the technical and organisational measures in Annex II, which it may improve but not degrade.
5. Assist the Controller in responding to data subject requests (access, rectification, erasure, objection, portability) through the platform's features or, where these are not enough, on request. Requests received directly by the Processor will be forwarded to the Controller without answering them.
6. Assist the Controller, with the information available to it, with data protection impact assessments and consultations with the supervisory authority.

4. Security incidents

The Processor will notify the Controller of any personal data breach affecting its data without undue delay and in any case within **48 hours** of becoming aware of it. The notice will describe, as far as known, the nature of the breach, the categories and approximate number of data subjects and records concerned, its likely consequences and the measures taken or proposed. Information not yet available will be provided as soon as it is.

5. Sub-processors

1. The Controller authorises the Processor to engage the sub-processors listed in Annex III and at pmovio.com/seguridad.
2. The Processor will give at least **30 days'** notice before adding or replacing a sub-processor. The Controller may object on reasonable data protection grounds; if the Parties cannot find a solution, the Controller may terminate the affected service without penalty, with a refund of any prepaid amount for the period not provided.
3. The Processor will bind each sub-processor by contract to data protection obligations equivalent to this agreement and remains liable to the Controller for their performance.

6. Location and international transfers

PMOvio's database is hosted in the European Union (Ireland). Some sub-processors (Annex III) process data outside it, mainly in the United States. Those transfers rely on the safeguards required by applicable law: the European Commission's standard contractual clauses or the EU-U.S. Data Privacy Framework, depending on the provider. For Colombian law purposes, the Controller authorises the transmission to those countries under this agreement.

7. Audits

The Processor will make available the information needed to demonstrate compliance with this agreement and will answer the Controller's security questionnaires. Where that is not enough, the Controller, or an auditor bound by confidentiality who is not a competitor of the Processor, may carry out an audit at most once a year, with 30 days' notice, during business hours, at the Controller's expense and without access to other customers' data. Security certifications held by the infrastructure providers are accepted as evidence of the controls they cover.

8. End of processing

When the service ends, the Controller may export its data from the platform or ask the Processor to deliver it in a commonly used format. Within **30 days**, the Processor will delete the Controller's data unless the law requires it to keep some of it, and will confirm this in writing on request. Backups are deleted in their ordinary rotation cycle and remain covered by this agreement while they exist.

9. Liability, term and precedence

Each Party's liability is governed by the Contract. This agreement lasts as long as the service and thereafter for as long as the Processor holds the Controller's data. In case of conflict with the Contract on data protection matters, this agreement prevails. Disputes will be resolved as provided in the Contract.

Annex I • Description of the processing

Data subjects	The Controller's users (employees, contractors) and people listed in its projects as resources, owners or stakeholders.
Categories of data	Name, email, job title and platform role; resource assignments, hours and cost; project comments and activity; technical access data (date, time, IP address). No special categories of data are requested; the Controller must not upload them.
Purpose	Providing the PMOvio service: project, portfolio, resource, risk and change management, reports, AI assistant, notifications and support.
Operations	Collection, storage, retrieval, calculation, modification, disclosure to sub-processors and erasure.
Duration	For the term of the service, plus the period in clause 8.

Annex II • Technical and organisational measures

- **Encryption:** TLS in transit with HSTS; AES-256 at rest in the database.
- **Isolation:** each organisation sees only its own data, enforced by row-level security (RLS) policies in the database, not just in the application.
- **Access:** minimum password requirements, two-factor authentication (TOTP) that the organisation can require for all its users, and roles with different permissions.
- **Administrative access:** support operations go through a gateway that validates permissions; no master key ever reaches the browser. Partners manage accounts and users, not project content.

- **Traceability:** per-project change history with author, date and previous and new values.
- **AI:** by default the assistant receives metrics with pseudonymised projects (P1, P2...) and people only by role; AI providers do not train models on that data.
- **Continuity:** automatic database backups by the infrastructure provider.
- **Staff:** access to customer data limited to those who need it to provide the service, under a duty of confidentiality.

Annex III • Authorised sub-processors

Provider	Function	Location
Supabase	Database and authentication	European Union (Ireland)
Vercel	Application hosting	Global infrastructure
Groq	Primary AI engine	United States
Anthropic	Fallback AI engine	United States
Resend	Transactional email	United States
Paddle	Billing and payments, when the Controller pays that way	United Kingdom / EU

The current list is at pmovio.com/seguridad.

The Controller

[Name, title]

Date:

The Processor

Ronny Castro Fonseca, Legal Representative

THE PROJECT MASTER S.A.S.

Date: