Data Processing Agreement

TerraLab SAS, processor. Version 2026-09, effective on the date of the last signature.

This Data Processing Agreement (the "DPA") is entered into under Article 28(3) of Regulation (EU) 2016/679 (the "GDPR") between:

The Controller

- Organisation: [CONTROLLER NAME]
- Legal form and registration number: [LEGAL FORM, SIREN OR EQUIVALENT]
- Address: [ADDRESS]
- Represented by: [NAME, TITLE]
- Contact for data protection matters: [EMAIL]

and

The Processor

- TerraLab SAS, a société par actions simplifiée under French law
- SIREN: 104 501 861 (RCS Paris)
- Registered office: 173 rue de Courcelles, 75017 Paris, France
- Represented by: Yvann Barbot, President
- Contact for data protection matters: yvann.barbot@terra-lab.ai

Each a "Party", together the "Parties".

This DPA forms part of the Terms of Sale and the Terms of Use published at https://terra-lab.ai (the "Agreement"). Where this DPA and the Agreement conflict on the processing of personal data, this DPA prevails.

1. Subject matter

The Processor provides the TerraLab plugins for QGIS (AI Edit, AI Segmentation, AI Agent), the account dashboard at https://terra-lab.ai and the hosted services behind them (the "Services"). In providing the Services, the Processor processes personal data on behalf of the Controller. This DPA sets the terms of that processing.

2. Duration

This DPA applies for as long as the Processor processes personal data on behalf of the Controller under the Agreement, and until the deletion or return described in clause 11 is complete.

3. Nature and purpose of the processing

The Processor processes personal data for the sole purpose of providing the Services to the Controller: creating and securing user accounts, receiving the imagery, prompts and project descriptions that a user sends from QGIS, running the requested detection, generation or planning, returning the result to QGIS, metering usage against the Controller's plan, invoicing, sending account and service emails, and keeping the Services reliable and secure.

The processing is carried out by hosted software. The Processor never trains a model on the Controller's imagery and never sells or otherwise discloses the Controller's data to any third party other than the sub-processors listed under clause 7.

4. Types of personal data

- Account data: email address, name if given, organisation, country, language, plan and billing status.
- Authentication data: sign-in links, session tokens, activation keys stored as hashes.
- Usage data: date, plugin, mode, quota consumed, run duration, error diagnostics tied to the account.
- Content data: the imagery tiles or squares, the area extent and coordinate reference system, the text prompts, the reference images and the project or layer descriptions that a user chooses to send from QGIS, and the results returned. Such content may incidentally contain personal data (for instance an address in a layer name or a person visible in aerial imagery).
- Billing data: invoices, VAT number, payment status. Card numbers are entered on Stripe's own page and never reach the Processor.
- Support data: the content of emails sent to the Processor.

5. Categories of data subjects

- Employees, agents and contractors of the Controller who hold a user account.
- Persons whose data appears in the content the Controller's users send from QGIS.
- Contacts of the Controller involved in ordering, billing or support.

6. Obligations of the Parties

6.1 The Processor shall

- process personal data only on the Controller's documented instructions, including with regard to transfers to a third country, unless required to do so by Union or Member State law, in which case the Processor informs the Controller of that requirement before processing, unless that law prohibits it on important grounds of public interest. The Agreement, this DPA and the use of the Services by the Controller's users constitute the documented instructions;
- inform the Controller without delay if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions;

- ensure that the persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- implement the technical and organisational measures set out in clause 8;
- respect the conditions of clause 7 for engaging another processor;
- assist the Controller as set out in clause 9;
- delete or return the personal data as set out in clause 11;
- make available the information necessary to demonstrate compliance and allow for audits as set out in clause 12;
- maintain a record of the categories of processing carried out on behalf of the Controller, as required by Article 30(2) GDPR.

6.2 The Controller shall

- ensure that it has a lawful basis for the processing and that the data subjects have received the information required by Articles 13 and 14 GDPR;
- give only lawful instructions and be responsible for the content that its users send through the Services;
- not send through the Services special categories of data within the meaning of Article 9 GDPR, or data relating to criminal convictions, unless agreed in writing with the Processor beforehand;
- keep its users' credentials confidential and notify the Processor of any account that must be closed.

7. Sub-processors

7.1 The Controller gives general written authorisation to the Processor to engage the sub-processors listed on the page https://terra-lab.ai/legal/subprocessors (the "Sub-processor Page"). At the date of this version the list is: Supabase, Google Cloud Storage, Google Cloud Run, Microsoft Azure OpenAI, fal.ai, Vercel, PostHog, Loops, Upstash, Google Translate API and Stripe. The Sub-processor Page states, for each of them, the purpose, the country, the hosting region, the transfer mechanism and the retention period.

7.2 The Processor announces any intended addition or replacement of a sub-processor on the Sub-processor Page at least 30 days before it takes effect. The Controller may object in writing, on reasonable data protection grounds, within that period. If the Parties cannot resolve the objection in good faith, the Controller may terminate the affected Services with no penalty, and the Processor refunds any prepaid fees for the period after termination.

7.3 The Processor imposes on each sub-processor, by written contract, data protection obligations that are no less protective than those in this DPA, in particular sufficient guarantees to implement appropriate technical and organisational measures. Where a sub-processor fails to fulfil its data protection obligations, the Processor remains fully liable to the Controller for the performance of that sub-processor's obligations.

8. Security measures

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, the Processor implements the following measures under Article 32 GDPR.

- Data location. Account data, imagery and inference run in the European Union: Paris (AWS eu-west-3 and Google Cloud europe-west9) for the database and files, Belgium (europe-west1) for AI Segmentation, the EU data zone in West Europe for the AI Agent model. AI Edit image generation runs at fal.ai in the United States under Standard Contractual Clauses.
- Encryption in transit. TLS 1.2 or higher on every connection between the plugin, the website and each provider.
- Encryption at rest. Provider-managed encryption (AES-256) on the database, the file storage and the model endpoints. Encrypted database backups expire within 12 months.
- Access control. Production access is held by the two founders of the Processor only, with two-factor authentication on every provider console. No contractor, no offshore support, no shared account. Activation keys are stored as truncated hashes.
- Segregation. Each account's data is keyed to that account and enforced at the database level (row-level security).
- Minimisation. The plugin sends only what the user chooses to send and strips file paths, layer names and imagery source URLs before sending. Nothing is sent in the background.
- Deletion. Self-service account deletion from the dashboard, with a 15-day grace period, after which every row, file and email contact is erased and the erasure is verified.
- Pro private tier. On the Pro private tier, no technical copy of imagery or results is kept after the request, and nothing sent is used to improve any model.
- Logging and monitoring. Error tracking and request counters in the EU, with no imagery in either.
- Resilience. Managed, redundant infrastructure at each provider; daily backups of the database.

The Processor may update these measures provided the level of protection does not decrease. The current description is kept on the Sub-processor Page.

9. Assistance to the Controller

9.1 Data subject rights. Taking into account the nature of the processing, the Processor assists the Controller by appropriate technical and organisational measures in responding to requests to exercise data subject rights under Chapter III GDPR. The Processor forwards to the Controller, without undue delay, any request it receives directly from a data subject of the Controller and does not answer it itself unless instructed.

9.2 Security, breach notification and impact assessments. The Processor assists the Controller in ensuring compliance with Articles 32 to 36 GDPR, taking into account the nature of the processing and the information available to the Processor.

9.3 Personal data breach. The Processor notifies the Controller without undue delay, and in any event within 48 hours, after becoming aware of a personal data breach affecting the Controller's personal data. The notification describes the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. Where the Processor is itself a controller for the data concerned, it also notifies the CNIL within 72 hours as required by Article 33 GDPR.

10. International transfers

10.1 The Processor processes personal data in the European Union, except as stated on the Sub-processor Page.

10.2 Where a sub-processor processes personal data outside the European Economic Area, the transfer is covered by an adequacy decision of the European Commission (including the EU-US Data Privacy Framework for certified companies) or by the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with the supplementary measures described in clause 8. The mechanism in force for each sub-processor is stated on the Sub-processor Page.

10.3 The Processor does not transfer personal data to a third country on its own initiative and informs the Controller before doing so at the Controller's request.

11. Deletion or return at the end of the Services

11.1 On termination of the Agreement, or at the Controller's earlier written request, the Processor deletes all personal data processed on the Controller's behalf, or returns it to the Controller, at the Controller's choice, and deletes existing copies, unless Union or Member State law requires storage of the personal data.

11.2 Deletion is available to the Controller's users at any time from the dashboard. It takes effect after a 15-day grace period during which the account can be restored; the Processor then erases every row, file and email contact tied to the account and verifies the erasure. Encrypted backups still holding erased rows expire on their own within 12 months.

11.3 Return takes the form of an export of account and usage data in JSON, provided within 30 days of the request. Results kept by the user already reside in QGIS on the Controller's own computers.

11.4 Invoices and billing records are retained for 10 years as required by article L123-22 of the French Code de commerce, with personal data limited to what that obligation requires.

12. Audit

12.1 The Processor makes available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR and with this DPA. In the first instance this takes the form of the Sub-processor Page, this DPA, the sub-processors' own certifications and reports, and written answers to the Controller's security questionnaire within 15 working days.

12.2 Where that information is not sufficient, the Controller, or an auditor mandated by the Controller and bound by confidentiality, may audit the Processor's compliance once per 12-month period, on 30 days' written notice, during business hours, in a manner that does not unreasonably disrupt the Processor's operations. The Controller bears its own costs. An audit following a personal data breach affecting the Controller's data may be requested without waiting for the annual window.

12.3 The Processor declares that it holds no SOC 2 report and no ISO 27001 certificate at the date of this version, and offers neither an on-premise nor a private-cloud deployment.

13. Liability

The liability of each Party under this DPA is subject to the limitations and exclusions of liability set out in the Terms of Sale and the Terms of Use, except where such limitation is prohibited by the GDPR, in particular Article 82. Nothing in this DPA limits a Party's liability towards data subjects.

14. Miscellaneous

14.1 This DPA is governed by French law. The courts of Paris have jurisdiction, without prejudice to the powers of the supervisory authorities.

14.2 If a provision of this DPA is held invalid, the remainder stays in force and the Parties replace the provision by one that achieves the same purpose.

14.3 This DPA may be signed electronically. Each Party keeps a signed copy.

Signatures

	The Controller	**The Processor**
Name	[NAME]	Yvann Barbot
Title	[TITLE]	President, TerraLab SAS
Date	[DATE]	[DATE]
Signature		