MineInterop

GDPR ARTICLE 28

Data Processing Agreement

Pursuant to Article 28 of the General Data Protection Regulation (GDPR)

Version v1.0 — July 2026

Solarius DeepTech SAS — MineInterop API Platform

CONFIDENTIAL — SOLARIUS DEEPTECH

Data Processing Agreement

This Data Processing Agreement (the “DPA”) forms part of the Service Agreement (the “Agreement”) between the client entity subscribing to the MineInterop services (the “Controller”) and **Solarius DeepTech SAS**, a company incorporated under the laws of France, operating the MineInterop API platform (the “Processor”). This DPA reflects the parties’ agreement with respect to the Processing of Personal Data by the Processor on behalf of the Controller in accordance with the requirements of Regulation (EU) 2016/679 (the “GDPR”).

In the course of providing the Services, the Processor may Process Personal Data on behalf of the Controller. This DPA governs such Processing and sets out the respective obligations of the parties under Article 28 of the GDPR. Where the terms of this DPA conflict with any other agreement between the parties in respect of the Processing of Personal Data, this DPA shall prevail.

Article 1 Definitions

For the purposes of this DPA, the following definitions apply. Capitalised terms not defined herein have the meaning given to them in the GDPR.

“Controller” means the Client entity that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Processor” means Solarius DeepTech SAS, operating the MineInterop API platform, which Processes Personal Data on behalf of the Controller.

“Personal Data” means any information relating to an identified or identifiable natural person, as defined in Article 4(1) of the GDPR.

“Processing” means any operation or set of operations performed on Personal Data, whether or not by automated means, as defined in Article 4(2) of the GDPR.

“Sub-processor” means any third party engaged by the Processor to Process Personal Data on behalf of the Controller.

“Services” means the MineInterop API platform accessible at api.mineinterop.com and the associated services described in the Terms of Service.

Article 2 Subject Matter and Duration

Subject matter. The Processor provides API-based block model processing services to the Controller, as further described in the Agreement and the Terms of Service.

Nature of processing. Transmission and Processing of API usage metadata, including email addresses, usage counters and request logs, strictly for the operation of the Services.

Purpose. The provision of the MineInterop API services as described in the Terms of Service.

Categories of data subjects. The Controller's employees and contractors who use the API.

Categories of personal data. Email addresses, names, API usage counters and request timestamps.

Duration. This DPA applies for the entire term of the Service Agreement between the parties and for so long as the Processor Processes Personal Data on behalf of the Controller.

IMPORTANT: Block model files (geological data) are Processed entirely in-memory and are **never stored, logged, or retained** by the Processor. No Personal Data is contained in or derived from block model files.

Article 3 Obligations of the Processor

The Processor shall, in respect of Personal Data Processed on behalf of the Controller:

3.1 Process the Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country, unless required to do so by Union or Member State law.

3.2 ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.3 implement appropriate technical and organisational security measures as set out in Article 5 of this DPA.

3.4 respect the conditions for engaging Sub-processors set out in Article 4 of this DPA.

3.5 assist the Controller, by appropriate technical and organisational measures, in responding to requests from data subjects exercising their rights under Articles 15 to 22 of the GDPR.

3.6 assist the Controller in ensuring compliance with its obligations relating to security of Processing, notification of Personal Data Breaches, and data protection impact assessments (Articles 32 to 36 of the GDPR).

3.7 at the choice of the Controller, delete or return all Personal Data upon termination of the Services, as set out in Article 9 of this DPA.

3.8 make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR, and allow for and contribute to audits.

Article 4 Sub-processors

The Controller provides a general authorisation for the engagement of the Sub-processors listed below. Each Sub-processor is bound by data protection obligations no less protective than those set out in this DPA.

Sub-processor	Purpose	Location	Safeguard
Google Cloud Platform (GCP)	API hosting & infrastructure	EU (europe-west1, Belgium)	Standard Contractual Clauses
Stripe Inc.	Payment processing	USA	Standard Contractual Clauses + EU-US DPF
Abacus.AI Inc.	Portal hosting	USA	Standard Contractual Clauses

The Controller consents to the above Sub-processors. The Processor shall notify the Controller of any intended changes concerning the addition or replacement of Sub-processors with **30 days' prior notice**, thereby giving the Controller the opportunity to object to such changes. If the Controller objects on reasonable data protection grounds, the parties shall work together in good faith to find a mutually acceptable resolution.

Article 5 Technical and Organisational Measures (TOMs)

The Processor implements and maintains the following technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR:

- **Encryption in transit** — TLS 1.3 for all API communications; HSTS enforced.
- **Encryption at rest** — AES-256 for stored data (usage records, account data).
- **Access control** — IAM least-privilege on GCP; API key authentication (X-API-Key header only).
- **Stateless processing** — block model files Processed in-memory only, never persisted.
- **Audit logging** — API request logs retained for 30 days, then automatically deleted.
- **Incident response** — security incidents notified to the Controller within 72 hours.
- **Personnel** — all Solarius DeepTech personnel with data access are bound by confidentiality agreements.
- **Enterprise on-premise** — clients may deploy entirely within their own infrastructure (zero data leaves the client environment).

Article 6 Data Subject Rights

The Processor shall assist the Controller, insofar as possible and by appropriate technical and organisational measures, in fulfilling the Controller's obligation to respond to requests from data subjects exercising their rights under Articles 15 to 22 of the GDPR (access, rectification, erasure, restriction of Processing, data portability, and objection).

Where the Processor receives a request directly from a data subject, it shall not respond to the request itself (except to confirm receipt where appropriate) but shall forward the request to the Controller **within 5 business days** of receipt.

Article 7 Personal Data Breaches

The Processor shall notify the Controller without undue delay and in any event **no later than 72 hours** after becoming aware of a Personal Data Breach affecting the Controller's Personal Data. Such notification shall, at a minimum, include:

- the nature of the Personal Data Breach;
- the categories and approximate number of data subjects concerned;
- the likely consequences of the Personal Data Breach;
- the measures taken or proposed to be taken to address the breach and mitigate its possible adverse effects.

Article 8 Data Transfers

Personal Data is primarily Processed within the European Economic Area (GCP europe-west1, Belgium). Transfers to Sub-processors located outside the EEA (Stripe, Abacus.AI) are governed by Standard Contractual Clauses as approved by the European Commission, supplemented where applicable by additional safeguards such as the EU-US Data Privacy Framework.

Article 9 Return and Deletion

Upon termination of the Service Agreement, the Processor shall, at the choice of the Controller: (i) return all Personal Data in a machine-readable format; or (ii) securely delete all Personal Data. The Processor shall certify such deletion in writing within **30 days** of termination. Backup copies shall be deleted within **90 days** of termination, save where storage is required by Union or Member State law.

Article 10 Governing Law and Jurisdiction

This DPA is governed by and construed in accordance with the laws of France. Any dispute arising out of or in connection with this DPA shall be submitted to the exclusive jurisdiction of the Tribunal de Commerce de Paris.

Article 11 Execution

To execute this DPA as part of your Enterprise agreement, please contact **enterprise@solariustechnology.com**. By signing below, each party agrees to be bound by the terms of this Data Processing Agreement.

For and on behalf of [CLIENT COMPANY]	**For and on behalf of Solarius DeepTech SAS**
_____ Name:	_____ Name:
_____ Title:	_____ Title:
_____ Date:	_____ Date:
_____ Signature	_____ Signature

Annex A List of Processing Activities

The following table sets out the specific Processing activities carried out by the Processor on behalf of the Controller, together with the legal basis and retention period for each.

Activity	Data Categories	Legal Basis	Retention
Account registration	Email, name, company	Contract (Art. 6(1)(b))	Duration of account
API authentication	API key prefix, last used timestamp	Contract	Duration of account
Usage metering	Endpoint, timestamp, bytes	Contract + Legitimate interest	30 days rolling
Billing	Email, Stripe customer ID	Contract	7 years (legal)
Support	Email, support ticket content	Contract	2 years

Annex B Technical and Organisational Measures (Detail)

This Annex details the technical and organisational measures referenced in Article 5, together with their implementation and the evidence available to demonstrate compliance.

Measure	Implementation	Evidence
Transport encryption	TLS 1.3 on all endpoints; HSTS; automatic HTTP→HTTPS redirect	SSL Labs A+ report; nginx config
Encryption at rest	AES-256 on GCP persistent disks and managed datastore	GCP encryption attestation
Access control	IAM least-privilege; MFA on admin accounts; API-key auth	IAM policy export; access review log
Stateless compute	Block model files held in-memory; no disk persistence or logging	Architecture review; source audit
Audit logging	Structured request logs retained 30 days then auto-purged	Log retention policy; purge job
Breach response	72-hour notification workflow; documented runbook	Incident response runbook
Personnel security	Confidentiality agreements; least-privilege onboarding	Signed NDAs; onboarding checklist
Business continuity	Automated daily backups; documented restore procedure	Backup logs; restore test records
On-premise option	Full self-hosted deployment; zero data egress from client estate	On-premise install guide; Docker image

---

MineInterop is developed by **Solarius DeepTech SAS**. This document and the software it describes are confidential and intended solely for licensed Enterprise customers. © 2026 Solarius DeepTech. All rights reserved.