

Data Processing Agreement

Between Sovarium Limited and the Customer named in the Order Form

Version 1.0 – October 2026

This Data Processing Agreement (“**DPA**”) forms part of the Agreement between Sovarium Limited (company number 14710982), whose registered office is at 167-169 Great Portland Street, 5th Floor, London W1W 5PF (“**Sovarium**”), and the Customer named in the Order Form. It applies to Customer Personal Data that Sovarium processes in providing the Services.

The Customer accepts this DPA by signing an Order Form that incorporates it; it needs no separate signature. It takes effect on the Effective Date and continues for as long as Sovarium processes Customer Personal Data.

The short version

A plain-English guide to the terms that follow. In it, “you” means the Customer and “we” means Sovarium. It is not part of the Agreement and does not change it: if anything here differs from the clauses, the clauses apply.

Who does what Clauses 2 and 4	You are the controller of your data and we are your processor. We process it only on your instructions, to provide Sovarium.
What we process Clause 3, Annex 1	Your team’s account details, their questions and our answers, and whatever data your read-only warehouse user lets us query. You decide what we can reach through the permissions you give that user.
AI Clauses 4.4 and 4.5	To answer a question, the AI sees your schema, your Context Layer, the conversation and a limited sample of query results (up to 100 rows per query, or 500 for a dashboard card). AI providers retain nothing, and your data never trains models.
Our own use Clause 4.6	We use feature usage, query metrics and conversation analytics (such as topic and sentiment) to run and improve Sovarium. We use your data for nothing else, and never sell it.
Where it goes Clauses 7 and 13, Annex 3	Stored in London. Some sub-processors work outside the UK (AI and email in the EU; Cloudflare, Google and Slack globally or in the US), with recognised legal safeguards. We give 30 days’ notice of any new sub-processor, and you can object.
Security Clause 6, Annex 2	Encryption in transit and at rest, each organisation’s data kept separate, two-factor sign-in you can require for your team, and staff access limited to people bound by confidentiality and logged.
Breaches Clause 10	We tell you within 48 hours of becoming aware of a breach affecting your personal data, and help you respond and notify.
Your part Clause 3	Have a lawful basis and give any notices needed for the data you connect, use a read-only user limited to what we need, and keep special category data out unless agreed.
Help and audits Clauses 8, 9 and 12	We help with data subject requests and impact assessments, answer one security questionnaire a year, and allow audits where a regulator requires one or after a breach.
When you leave Clause 11	Ask for an export before the end. We delete your data within 30 days and confirm in writing; backup copies expire within 7 days.
Contacts Clause 16	Data protection: privacy@sovarium.com . Security incidents: security@sovarium.com .

1. Definitions and interpretation

- 1.1 Capitalised terms used but not defined in this DPA (including Customer Data, Customer Personal Data, Customer Warehouse, Context Layer, AI Features, Beta Features, Authorised Users, Business Day, Data Protection Laws, Sub-processor, Security Incident and Confidential Information) have the meaning given in the Master Subscription Agreement.
- 1.2 In this DPA:
- (a) **“UK GDPR”** means the UK General Data Protection Regulation as defined in section 3(10) of the Data Protection Act 2018, read with that Act.
 - (b) **“EU GDPR”** means Regulation (EU) 2016/679 (the General Data Protection Regulation).
 - (c) **“Controller”**, **“Processor”** and **“Data Subject”** have the meanings given in the UK GDPR or, where it applies, the EU GDPR.
 - (d) **“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise processed by Sovarium or a Sub-processor. It does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, such as blocked sign-in attempts, pings and port scans.
 - (e) **“Supervisory Authority”** means the UK Information Commissioner, or any other independent public authority responsible for monitoring the application of Data Protection Laws, including one established under Article 51 of the EU GDPR.
 - (f) **“EU SCCs”** means the standard contractual clauses for the transfer of personal data to third countries in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
 - (g) **“UK Addendum”** means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 (version B1.0, in force from 21 March 2022), as revised under its Section 18.
 - (h) **“Restricted Transfer”** means a transfer of Customer Personal Data that is restricted under Chapter V of the UK GDPR or Chapter V of the EU GDPR and is not covered by adequacy regulations (UK) or an adequacy decision (EU).
 - (i) **“Privacy Policy”** means Sovarium’s privacy policy at sovarium.com/privacy, as updated from time to time.
- 1.3 The terms personal data, processing and special categories of personal data have the meanings given in the Data Protection Laws. “Including” means including without limitation.
- 1.4 **Order of precedence.** If the documents of the Agreement conflict, the order of precedence is: the Order Form, then this DPA (as to the processing of personal data), then the SLA and Support Schedule (Schedule 2 of the Master Subscription Agreement), then the rest of the Master Subscription Agreement. Where the EU SCCs or the UK Addendum apply, they prevail over every document of the Agreement to the extent of any conflict.

2. Roles and scope

- 2.1 The Customer is the Controller of Customer Personal Data and Sovarium is its Processor. Where the Customer acts as a Processor on behalf of its own controllers, Sovarium is the Customer’s sub-processor: the Customer confirms that those controllers have authorised its

instructions, including the appointment of Sovarium and its Sub-processors, and the Customer remains Sovarium's only point of contact for them.

- 2.2 Sovarium is a Controller only of personal data it processes for its own business: business contact details, contract and billing information (including invoices), and account-security data, such as the logs of Sovarium staff access to the Customer's organisation and records used to detect and prevent abuse. Sovarium processes that data under its Privacy Policy; this DPA does not apply to it.
- 2.3 The subject matter, duration, nature and purpose of the processing, and the types of personal data and categories of Data Subjects, are set out in Annex 1.
- 2.4 Each party will comply with the Data Protection Laws that apply to it in connection with the Agreement.

3. The Customer's responsibilities

- 3.1 The Customer is responsible for having a lawful basis for the processing and for giving any notices it requires, including to the individuals whose personal data is held in the Customer Warehouse; for having the right to connect the Customer Warehouse and to have Sovarium process its data; and for ensuring its instructions comply with Data Protection Laws.
- 3.2 **Minimisation.** The Customer decides which data Sovarium can reach. It will connect the Platform with a read-only database user that it creates and controls, with only the access the Services need, and will not give that user access to data it does not want processed.
- 3.3 **Special categories.** No special categories of personal data, or personal data relating to criminal convictions and offences, are intended to be processed. The Customer will not connect such data, or include it in questions or Context Layer requests, unless the parties have agreed in writing (for example in the Order Form) the additional measures that will apply.
- 3.4 **Users and channels.** The Customer chooses its Authorised Users and their roles, whether two-factor authentication is required, the email recipients of alerts and digests, and any Slack workspace and channels it connects. Content that Sovarium delivers to a Slack workspace is then processed under the Customer's own agreement with Slack. The Customer will remove Authorised Users' access promptly when it is no longer needed.

4. Processing on the Customer's instructions

- 4.1 Sovarium will process Customer Personal Data only on the Customer's documented instructions, including with regard to international transfers, unless UK law (or, where the EU GDPR applies, EU or Member State law) requires otherwise. In that case Sovarium will inform the Customer of that legal requirement before processing, unless the law prohibits this on important grounds of public interest.
- 4.2 The Customer's documented instructions are:
 - (a) the Agreement;
 - (b) the Customer's use and configuration of the Platform, including the data sources it connects, the questions its Authorised Users ask, the dashboards, alerts and monitored tables it sets up, the delivery channels it connects and its retention settings;
 - (c) its requests to Sovarium for support and for changes to the Context Layer; and
 - (d) any other reasonable written instruction consistent with the Agreement. An instruction outside the scope of the Agreement needs the parties' written agreement and may be charged for.

- 4.3** Sovarium will inform the Customer promptly if, in its opinion, an instruction infringes Data Protection Laws, and may suspend the processing concerned until the Customer confirms or changes the instruction. Sovarium is not obliged to give the Customer legal advice.
- 4.4** **AI Features.** The Customer instructs Sovarium to process Customer Personal Data with the AI Features. To answer questions and diagnose findings, Sovarium's AI models receive:
- (a) database schema information (table and column names, data types) and the Context Layer;
 - (b) the question and the conversation so far;
 - (c) the results of the queries the AI runs: up to the first 100 rows of each result, plus summary statistics for each column;
 - (d) the data prepared for each chart and dashboard card it creates (up to 500 rows for a card); and
 - (e) for Anomalies (a Beta Feature), the column profiles, baselines (including sample values) and check results of a flagged table, and the rows it queries to investigate a finding.
- These can include individual records, and any personal data in the columns queried. Alert evaluations make no AI call.
- 4.5** Sovarium reaches AI models through OpenRouter, configured to route requests only to model providers with zero data retention, which do not store Customer Data or use it for training. Sovarium does not use Customer Data to train AI models, and tests its AI with synthetic data, not Customer Data.
- 4.6** **Service analytics.** The Customer authorises Sovarium to use feature usage, query metrics and analytics derived from conversations (such as topic and sentiment) to operate, secure, support and improve the Services, as described in the Privacy Policy. Sovarium will not otherwise process Customer Personal Data for its own purposes, and does not sell it.

5. Confidentiality of personnel

- 5.1** Sovarium will ensure that everyone it authorises to process Customer Personal Data is bound by an appropriate duty of confidentiality, contractual or statutory. Within Sovarium, access to Customer Personal Data is restricted to Sovarium employees and contractors who are bound by confidentiality obligations and need it to provide the Services.

6. Security

- 6.1** Sovarium will implement and maintain technical and organisational measures that ensure a level of security appropriate to the risk, as required by Article 32 of the UK GDPR (and, where it applies, the EU GDPR), including the measures in Annex 2.
- 6.2** Sovarium may update those measures from time to time, provided the overall level of protection of Customer Personal Data is not materially reduced.
- 6.3** The Customer is responsible for the security of the Customer Warehouse, of any Slack workspace it connects and of its Authorised Users' sign-in credentials, and for the security choices it makes in the Platform, such as requiring two-factor authentication.

7. Sub-processors

- 7.1** The Customer gives Sovarium general written authorisation to engage Sub-processors. The Sub-processors engaged at the date of this DPA are listed in Annex 3.

- 7.2** Sovarium will give the Customer at least 30 days' notice before engaging a new Sub-processor or replacing one, by email to the Customer's notice contact named in the Order Form. The notice will give the Sub-processor's name, the processing it will carry out and its location.
- 7.3** The Customer may object to the change on reasonable data-protection grounds by email to privacy@sovarium.com within that notice period. The parties will discuss the objection in good faith, and Sovarium may propose an alternative. If the objection is not resolved within 30 days of its receipt, the Customer may terminate the affected Services by written notice, and Sovarium will refund any prepaid fees for those Services covering the period after termination. This is the Customer's only remedy for an objection under this clause.
- 7.4** Sovarium will engage each Sub-processor under a written contract imposing data protection obligations that give at least the same level of protection for Customer Personal Data as this DPA, as appropriate to the Sub-processor's services. Sovarium remains liable to the Customer for each Sub-processor's performance of those obligations.

8. Data Subject requests

- 8.1** If Sovarium receives a request from a Data Subject to exercise their rights in relation to Customer Personal Data, it will pass the request to the Customer without undue delay and will not respond to it, except to direct the Data Subject to the Customer, unless the law requires otherwise.
- 8.2** Taking into account the nature of the processing, Sovarium will assist the Customer by appropriate technical and organisational measures, insofar as this is possible, to respond to such requests. Where the Customer cannot fulfil a request itself through the Platform, Sovarium will, on the Customer's written instruction to privacy@sovarium.com, help it locate, export, correct or delete the Customer Personal Data concerned.
- 8.3** Sovarium may charge its reasonable costs for assistance under this clause or clause 9 (DPIAs and prior consultation) that goes materially beyond what the Platform provides, unless the request arises from Sovarium's breach of this DPA.

9. DPIAs and prior consultation

- 9.1** Taking into account the nature of the processing and the information available to it, Sovarium will give the Customer reasonable assistance with any data protection impact assessment, and any prior consultation with a Supervisory Authority, that the Customer is required to carry out in relation to the Services. Sovarium will do so mainly by providing documentation, such as this DPA, the Privacy Policy and the security information described in clause 12 (Audits and information).

10. Personal Data Breaches

- 10.1** Sovarium will notify the Customer of a Personal Data Breach without undue delay, and in any event within 48 hours after becoming aware of it, by email to the Customer's notice contact named in the Order Form and to any security contact the Customer has given Sovarium.
- 10.2** The notice will, as far as the information is then available, describe:
- (a) the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects and of personal data records concerned;
 - (b) the name and contact details of the contact point where more information can be obtained (security@sovarium.com);
 - (c) the likely consequences of the Personal Data Breach; and

- (d) the measures taken or proposed to address it, including measures to mitigate its possible adverse effects.

Where the information is not all available at once, Sovarium will provide it in phases as it becomes available, without undue further delay.

- 10.3** Sovarium will promptly take reasonable steps to contain, investigate and mitigate the Personal Data Breach, keep the Customer informed, and give the Customer reasonable cooperation with any notification it must make to a Supervisory Authority or to Data Subjects.
- 10.4** The Customer decides whether to notify Supervisory Authorities and Data Subjects. Sovarium will not notify third parties of a Personal Data Breach in a way that identifies the Customer without the Customer's consent, unless the law requires it.
- 10.5** Notifying or responding to a Personal Data Breach is not an acknowledgement by Sovarium of any fault or liability.
- 10.6** The Customer should report any suspected security issue affecting the Services to security@sovarium.com.

11. Return and deletion

- 11.1** Before the end of the Subscription Term, the Customer may ask Sovarium, by email to privacy@sovarium.com, for an export of the Customer Personal Data held in the Platform (such as stored answers, dashboards and conversations). Sovarium will provide it within a reasonable time in a commonly used electronic format. The Customer's source data remains in the Customer Warehouse.
- 11.2** When the Agreement ends, Sovarium will:
 - (a) end access to the Platform for the Customer's Authorised Users;
 - (b) at the same time, delete the Customer Warehouse credentials it holds, and revoke and delete any Slack token for the Customer's workspace; and
 - (c) within 30 days, delete all remaining Customer Personal Data in the Platform, including Authorised User accounts and stored files, and confirm the deletion to the Customer in writing.
- 11.3** The Customer should also delete the database user it created for Sovarium and remove the Sovarium app from its Slack workspace: Sovarium's copies of those credentials are deleted, but the Customer's action is what revokes them.
- 11.4** Copies of Customer Personal Data in database backups expire on their normal cycle, within 7 days. Copies in Sub-processors' operational logs and in short-lived job queues expire on their own schedules. Until then, those copies remain protected by this DPA and are not otherwise processed.
- 11.5** Sovarium may keep Customer Personal Data where UK law (or, where the EU GDPR applies, EU or Member State law) requires it to, for as long as required. That data remains protected by this DPA and is processed only for that purpose. This clause does not affect the data described in clause 2.2, which Sovarium keeps under its Privacy Policy.

12. Audits and information

- 12.1** Sovarium will make available to the Customer the information necessary to demonstrate its compliance with Article 28 of the UK GDPR (and, where it applies, the EU GDPR). On request, Sovarium will provide documentation of its security measures and will answer one reasonable written security questionnaire in any 12-month period, and a further one after a Personal Data Breach.

12.2 An on-site audit, or an audit by a third party, may take place only:

- (a) where a Supervisory Authority requires it; or
- (b) after a Personal Data Breach, where the information provided under clause 12.1 does not reasonably answer the Customer's concerns.

Such an audit will be carried out on at least 30 days' written notice (or any shorter period a Supervisory Authority requires), on Business Days, to a scope and timing agreed in advance, in a way that minimises disruption to the Services, and at the Customer's cost. It may be carried out by the Customer or by an independent auditor that is not a competitor of Sovarium, in each case bound by confidentiality obligations. It does not extend to other customers' data, or to Sub-processors' facilities, for which Sovarium will provide the Sub-processors' own security documentation where available. Audit information and reports are Sovarium's Confidential Information.

12.3 Sovarium will keep a record of its processing activities as a Processor, and will cooperate with Supervisory Authorities in the performance of their tasks.

12.4 Where the EU SCCs apply, the Customer's audit rights under them will be exercised as this clause describes, to the extent this is consistent with the EU SCCs.

13. International transfers

13.1 Sovarium stores Customer Personal Data in London, United Kingdom. Some Sub-processors process it outside the UK, as shown in Annex 3: notably OpenRouter, the AI model providers and Resend (email delivery), in the European Union; Cloudflare and Google, on their global infrastructure; and Slack, in the United States. The Customer authorises those transfers.

13.2 Sovarium will ensure that each transfer of Customer Personal Data to a Sub-processor outside the UK (and, where the EU GDPR applies, outside the European Economic Area) relies on adequacy regulations (UK) or an adequacy decision (EU) where one is available, and otherwise on appropriate safeguards under the Data Protection Laws, such as the UK Addendum and the EU SCCs (Module 3, processor to processor).

13.3 A transfer from a Customer in the UK to Sovarium is not a Restricted Transfer, and a transfer from a Customer in the European Economic Area to Sovarium relies on the European Commission's adequacy decision for the UK. To the extent a transfer between the Customer and Sovarium is nevertheless a Restricted Transfer:

- (a) the EU SCCs are incorporated into this DPA by reference: Module 2 (controller to processor) where the Customer is a Controller, and Module 3 (processor to processor) where it is a Processor, with the elections in the first table below;
- (b) for a transfer under the UK GDPR, the UK Addendum is incorporated into this DPA by reference, with the information in the second table below; and
- (c) the Customer is the data exporter and Sovarium the data importer, and signing an Order Form that incorporates this DPA counts as signing the EU SCCs and the UK Addendum.

13.4 EU SCCs elections

Clause	Election
Modules	Module 2 where the Customer is a Controller; Module 3 where the Customer is a Processor.
Clause 7 (Docking clause)	Not included.

Clause	Election
Clause 9(a) (Use of sub-processors)	Option 2: general written authorisation. Sovarium will inform the Customer of intended changes at least 30 days in advance, as clause 7 (Sub-processors) of this DPA describes.
Clause 11(a) (Redress)	The optional language does not apply.
Clause 13(a) (Supervision)	The supervisory authority determined under Clause 13(a); where none can be determined that way, the Data Protection Commission (Ireland).
Clause 17 (Governing law)	Option 1: the law of Ireland.
Clause 18(b) (Choice of forum and jurisdiction)	The courts of Ireland.
Annex I.A (List of parties)	Data exporter: the Customer named in the Order Form (Controller under Module 2, Processor under Module 3). Data importer: Sovarium Limited, 167-169 Great Portland Street, 5th Floor, London W1W 5PF, Processor, contact privacy@sovarium.com . Activities: the Services. Signature and date: the Order Form.
Annex I.B (Description of transfer)	Annex 1 of this DPA.
Annex I.C (Competent supervisory authority)	As in Clause 13(a) above.
Annex II (Technical and organisational measures)	Annex 2 of this DPA.
Annex III (List of sub-processors)	Annex 3 of this DPA.

13.5 UK Addendum information

UK Addendum	Information
Table 1 (Parties)	As in Annex I.A above. Start date: the Effective Date.
Table 2 (Selected SCCs, Modules and Clauses)	The EU SCCs incorporated by this DPA, with the Modules and elections in the table above.
Table 3 (Appendix Information)	Annexes 1, 2 and 3 of this DPA.
Table 4 (Ending this Addendum when the Approved Addendum changes)	Neither party.
Governing law and courts	England and Wales, as the UK Addendum provides.

14. US state privacy laws

- 14.1** Where the California Consumer Privacy Act (as amended) or a similar US state privacy law applies to Customer Personal Data, Sovarium acts as the Customer's "service provider" (or "processor") and will not: sell or share Customer Personal Data (as those terms are defined in that law); retain, use or disclose it for any purpose other than providing the Services, or outside the direct business relationship with the Customer; or combine it with personal information from other sources, except as that law permits. Sovarium will comply with the obligations that law places on it, provide the same level of privacy protection the law requires, and tell the Customer if it can no longer meet them.

15. Liability

- 15.1** Each party's liability arising out of or in connection with this DPA (including, to the extent the law permits, the EU SCCs and the UK Addendum) is subject to the "Limitation of liability" clause of the Master Subscription Agreement, including the separate cap for data protection that it sets.
- 15.2** Nothing in this DPA limits either party's liability to Data Subjects under the third-party beneficiary rights of the EU SCCs or the UK Addendum, or any liability that cannot be limited by law.

16. Term, changes and contacts

- 16.1** This DPA continues for as long as Sovarium processes Customer Personal Data, even after the Agreement ends.
- 16.2** Sovarium may update this DPA to reflect changes in Data Protection Laws or a Supervisory Authority's guidance, or to adopt a replacement transfer mechanism, by giving the Customer at least 30 days' written notice, provided the update does not materially reduce the protection of Customer Personal Data. Any other change needs the parties' written agreement.
- 16.3** Data protection questions and objections go to privacy@sovarium.com, and security incidents to security@sovarium.com. Legal notices are given to moid@sovarium.com under the "Notices" clause of the Master Subscription Agreement.
- 16.4** This DPA is governed by the law, and subject to the jurisdiction of the courts, set out in the "Governing law and jurisdiction" clause of the Master Subscription Agreement (England and Wales), except that the EU SCCs and the UK Addendum are governed as elected in clause 13.

Annex 1 – Details of processing

This Annex describes the processing for the purposes of Article 28(3) of the UK GDPR and the EU GDPR, and is Annex I.B of the EU SCCs where they apply.

Subject matter	Sovarium's provision of the Services to the Customer under the Agreement.
Duration	The Subscription Term, plus up to 30 days after the Agreement ends for deletion under clause 11 (Return and deletion), and until backup copies expire.
Nature and purpose	Processing needed to provide the Services, namely: • hosting and storing Customer Personal Data on Sovarium's Platform; • generating SQL from questions, validating it, and running it against the Customer Warehouse; • analysing data with the AI Features, as described in clause 4.4 (AI Features); • producing answers, charts, Command View dashboards and insights, alerts and opportunities, and, if enabled, Anomalies scans, findings and digests (a Beta Feature); • building and maintaining the Context Layer; • providing support, which may involve Sovarium personnel viewing Customer Data to resolve a request; • delivering the emails and Slack messages the Customer configures, and answering questions asked in a connected Slack workspace; • securing the Platform, including session security and security logging; and • usage metrics and conversation analytics, as described in clause 4.6 (Service analytics).
Categories of Data Subjects	• Authorised Users, and people invited to become Authorised Users. • People who ask questions through a Slack workspace the Customer connects. • Individuals whose personal data is held in the Customer Warehouse, such as the Customer's customers, prospects, employees, contractors and suppliers, and their contacts. Which individuals are affected depends on the Customer's data and the questions asked.

Categories of personal data	Authorised User account data: name, email address, role, job role and interests, timezone, sign-in times, two-factor authentication (TOTP) factors, and IP address and browser user agent, used to secure the session. Usage data: questions, conversations and the SQL generated to answer them; the answers, charts, dashboard cards, alerts and opportunities produced; feedback and triage decisions; feature usage and query metrics; analytics derived from conversations (such as topic and sentiment); Slack workspace, channel and thread identifiers. Data from the Customer Warehouse: any personal data in the columns queried, as it appears in query results, chart data, dashboard card snapshots (up to 500 rows), opportunity evidence (up to 100 rows) and alerts; schema metadata and the Context Layer, to the extent they contain personal data. Anomalies (Beta Feature), if enabled: column profiles, including up to 10 sample values per text column (each cut to 100 characters), the baselines learned from them, and findings with their evidence, including up to 20 example rows.
Special categories	None intended. The Customer must not connect special categories of personal data or criminal offence data unless agreed in writing (clause 3.3).
Frequency	Continuous for the Subscription Term.
Retention during the Subscription Term	Chat answers and charts: until deleted, unless a retention period (1 to 365 days) is set for the Customer's organisation. Admins can delete all stored answers at any time. Questions, generated SQL and conversations: for the life of the Customer's account. Deleting a conversation removes it from view; the records are retained. Command View insights: 30 days. Dashboard cards and their snapshots: while on the dashboard, and deleted within two days of removal. Opportunities: for the life of the account, with their evidence. Feedback on them expires after 6 months, or 30 days after it is removed. Alert history: 90 days. Anomalies findings: the organisation's history period (30 days by default, configurable from 1 to 365 days). Column profiles: 180 days. Sessions: expire after 7 days of inactivity, and after 30 days at most. Account data: while the Customer's account exists. At the end of the Agreement, all of the above is deleted under clause 11 (Return and deletion).
Sub-processors	As listed in Annex 3, for the processing and duration described there and in this Annex.
Contacts	Customer: the notice contact named in the Order Form. Sovarium: privacy@sovarium.com (security incidents: security@sovarium.com).

Annex 2 – Technical and organisational security measures

Sovarium maintains the following measures, which may be updated under clause 6.2. This Annex is Annex II of the EU SCCs where they apply.

Encryption

- All traffic between users' browsers and Sovarium is encrypted in transit with TLS (HTTPS).
- Connections from Sovarium's application servers to its database and to its session and queue store use TLS. Connections to a Customer Warehouse at a public address use TLS.
- All Customer Data stored on the Platform is encrypted at rest with AES-256, including the database, file storage and backups held by Supabase.
- In addition, Sovarium encrypts Customer Warehouse credentials, Slack tokens and session tokens with AES-256-GCM before storage, with keys held as production secrets, separately from the encrypted data.

Separation of customers

- Each organisation's data is isolated at the database level: requests made by users run under row-level security policies bound to their organisation, and background processing filters explicitly by organisation.

Access control for Authorised Users

- Invite only: there is no public sign-up, and every account belongs to an organisation Sovarium sets up.
- Role-based access (owner, admin, standard user) decides what each Authorised User can do.
- Sign-in by password or Sign in with Google, with two-factor authentication (TOTP) that any user can add and the Customer can require for every member.
- Sessions are bound to the browser and IP address they started on, and expire after 7 days of inactivity and after 30 days at most. Removing a member signs them out.
- Rate limits on sign-in and two-factor verification attempts.

Sovarium staff access

- Only Sovarium employees and contractors bound by confidentiality obligations can reach customer data, through a separate administration application behind an identity-aware access proxy, with its own sign-in and role-based permissions.
- Every access to customer data through that application is logged: who, what, when, and from which IP address and browser.

Customer Warehouse access

- Every query is checked by Sovarium's SQL validator before it runs, and only a single read query passes. The saved queries behind alerts and dashboard cards are checked again before every run.
- For PostgreSQL, MySQL and ClickHouse the session is also opened in read-only mode. For other warehouses, read-only access depends on the credentials the Customer provides, which is why the Customer must connect with a read-only, least-privilege user that it creates and can revoke at any time.
- Sovarium connects from fixed, published IP addresses, so the Customer Warehouse can refuse connections from anywhere else. These addresses are shared by all Sovarium customers, so the Customer's credentials, not the allowlist, limit access.
- Query results are received and processed on Sovarium's servers in London.

Network and application security

- Cloudflare web application firewall and rate limiting in front of the Platform. Sovarium's application servers refuse requests that do not come through Cloudflare.
- Strict Content Security Policy on the web and administration applications.
- Application servers, database, and session and queue store hosted in London, United Kingdom. The API runs on more than one server; the session and queue store is persistent and replicated.

AI processing

- AI models are reached through OpenRouter, configured to route requests only to model providers with zero data retention, which do not store Customer Data or use it for training.
- Customer Data is not used to train AI models. Sovarium tests its AI with synthetic data, not Customer Data.

Operations

- Infrastructure (network edge, access proxy and the session and queue store) is defined as code.
- Production is separate from development. Real Customer Warehouse credentials exist only in production; development, testing and AI evaluation use synthetic data only.
- Production secrets are held in the hosting providers' secret stores, not in source code.
- Automated type checks, tests and dependency vulnerability checks run in continuous integration before changes are deployed.
- Operational logs record request metadata such as identifiers, timings and errors. They do not record questions or query results, though part of a blocked or failing SQL query may be logged.
- Documented procedures for incident response and for offboarding and deleting an organisation, and Personal Data Breach notification as set out in clause 10.
- Database backups are kept by Supabase for 7 days.

Personnel

- Personnel with access to Customer Personal Data are bound by confidentiality obligations.
- Access is granted on a least-privilege basis, limited to what each person's role needs.

Annex 3 – Sub-processors

Sovarium uses the following Sub-processors, under clause 7 (Sub-processors). This Annex is Annex III of the EU SCCs where they apply.

Sub-processor	Purpose	Customer Personal Data	Location
Cloudflare	DNS, network security (firewall, rate limiting), hosting of Sovarium's websites and web applications	All traffic between users and Sovarium, in transit	Global edge network
Fly.io	Application servers (API and background workers)	All Customer Personal Data the Services process	London, United Kingdom
Supabase	Database, authentication and file storage	All stored Customer Personal Data, including Authorised User accounts	London, United Kingdom
Redis Cloud	Sessions, job queues and caches	Session data; job data, including questions and results, held briefly	AWS London, United Kingdom
OpenRouter	Routing of AI requests, with zero data retention	The AI inputs described in clause 4.4 (AI Features)	European Union
AI model providers reached through OpenRouter: Baseten, Anthropic and Together AI	AI processing, only with zero data retention	The AI inputs described in clause 4.4 (AI Features)	European Union
Resend	Transactional email delivery	Recipients' names and email addresses; email content, including invitations, account and security emails, alerts and digests	European Union
Google	Business email (Google Workspace), including the support@sovarium.com inbox; Sign in with Google, if the Customer's users use it	Any Customer Personal Data in emails the Customer or its Authorised Users send to Sovarium, such as support requests and screenshots; for Sign in with Google, name, email address and Google account identifier	Google's global infrastructure

Sub-processor	Purpose	Customer Personal Data	Location
Slack	Sovarium's internal team communication	Details of support requests and incidents that Sovarium's team discusses internally, which may include Customer Personal Data	United States

Services the Customer connects. The Customer's own Slack workspace and the Customer Warehouse are services the Customer chooses and connects; they are not Sovarium's Sub-processors, and their processing is governed by the Customer's own agreements with their providers. This is separate from Sovarium's internal use of Slack, listed above.

Sovarium's business tools. Sovarium also uses Attio (CRM), FreeAgent (accounting and invoicing), GoCardless (payments), and BoldSign and PandaDoc (contract signing). These hold only business contact, contract, billing and payment information, which Sovarium processes as a Controller under clause 2.2, not Customer Personal Data, so they are not Sub-processors.