

Data Processing Agreement.

Version 3.0 · Effective 5 October 2026 · Last updated 5 October 2026

This Agreement applies where a Business User (the "Controller") submits personal data about its own customers, staff, suppliers or contacts to SALOA, and the Operator (the "Processor") processes that data on the Controller's behalf. It is entered into by accepting the Terms & Conditions and forms part of them.

It does not apply where the Operator is itself controller, such as for account data, billing records, acceptance records and security logs. Those are covered by the Privacy Policy.

HOW TO READ THIS DOCUMENT — This text is written to satisfy Article 28(3) GDPR.

1. Subject matter and duration

The Processor processes Controller Personal Data only to provide SALOA under the Terms: running Interviews and Company Analyses, generating and storing Output, maintaining Projects, securing the service and providing support. Processing lasts for as long as the Controller's account or Projects exist, subject to clause 10.

2. Nature, purpose, categories

Nature of processing: collection, storage, structuring, transmission to the AI providers listed in clause 5, generation of derived text, retrieval of publicly available web pages for a requested analysis, and deletion.

Purpose: performance of the Engagement and provision of the Business OS to the Controller.

Categories of data subjects: the Controller's customers, prospects, staff, founders, suppliers and other contacts described in User Content; individuals named in public sources where the Controller requests an analysis.

Categories of personal data: names, contact details, professional role, commercial relationship information, and any other personal data the Controller chooses to submit.

Special categories: not requested and not required. The Controller should not submit special category or criminal offence data. If it does, it remains responsible for having a valid Article 9 or 10 basis.

3. Processor obligations

- Process only on documented instructions from the Controller, which include the Terms, this Agreement and the Controller's use of the product features.
- Inform the Controller if an instruction appears to infringe data protection law.
- Not process for its own purposes. The Processor does not train any model on Controller Personal Data. Whether an AI subprocessor retains prompts, and for how long, is governed by that provider's own terms; see clause 5.
- Ensure persons authorised to process are bound by confidentiality.
- Implement the technical and organisational measures in clause 6.
- Assist the Controller with data subject requests, security, impact assessments and prior consultation, taking into account the nature of the processing.
- Notify the Controller without undue delay after becoming aware of a personal data breach affecting Controller Personal Data, with the information available.
- Make available the information necessary to demonstrate compliance with this Agreement.

4. Controller obligations

- Ensure there is a valid legal basis for submitting the personal data to SALOA and for the analysis requested.

- Provide required information to its own data subjects.
- Not submit more personal data than necessary for the Engagement.
- Handle data subject requests as controller, using the export and deletion controls available in the account.

5. Subprocessors

The Controller gives general authorisation for the Processor to engage the subprocessors listed below, each under a contract imposing data protection obligations no less protective than this Agreement.

CATEGORY	PROVIDER	ROLE IN PROCESSING
Application hosting and delivery	Lovable (application platform) and its infrastructure providers	Serving the application and running server-side functions.
Database and authentication	Supabase	Accounts, authentication, sessions, projects, generated output, acceptance records, security events.
Authentication email delivery	Supabase (built-in authentication email service; no separate transactional email provider is configured)	Sign-in, sign-up and password-reset emails.
AI models	Lovable AI Gateway, routing to Google and OpenAI models	Interviews, analysis, adversarial review, generated assets, support answers. User Content is transmitted to these providers; this cannot be switched off while using SALOA.
Web research	Firecrawl	Retrieving publicly available web pages used as evidence for a requested analysis.

These are the providers actually used by the product. AI processing is essential: Controller Personal Data contained in User Content is transmitted to the AI providers listed above and this cannot be disabled while using SALOA. Retention and training settings applied by each AI provider are governed by that provider's terms.

New subprocessors are announced on this page before they start processing, wherever reasonably possible. The Controller may object to a new subprocessor on reasonable data protection grounds by writing to studio@getsaloe.com. No alternative provider is promised: where the objection concerns a provider the service depends on and no reasonable alternative exists, either party may terminate the affected part of the service, and an unperformed paid Engagement is refunded.

6. Security measures

Measures include authenticated access, tenant isolation enforced at database level, server-side authorisation for privileged operations, managed secret storage, encryption in transit, rate limiting, audit logging of security-relevant events, isolation of untrusted text before it reaches AI models, and restricted administrative access. Detailed configuration is not published for security reasons and can be described under NDA on request. Absolute security is not warranted.

7. International transfers

Where a subprocessor processes personal data outside the EEA, the transfer relies on an adequacy decision, on Standard Contractual Clauses (Module 3, processor to processor) with supplementary measures where required, or on another Chapter V mechanism. The primary database is hosted in the EU (Frankfurt). Details per provider are available on request.

8. Audits

On reasonable written request, and not more than once a year unless a supervisory authority or a breach requires otherwise, the Processor will provide information and available third-party certifications or reports of its subprocessors to demonstrate compliance. On-site audits are limited to what is proportionate for a sole-proprietor operation and are subject to confidentiality and reasonable cost recovery.

9. Data subject requests

The Controller remains responsible for responding to its own data subjects and for meeting the statutory response deadlines. The Processor's duty is to assist: it makes the export and deletion controls in the account available for that purpose and, on request, provides the information about the processing that the Controller needs in order to answer.

If the Processor receives a request directly from one of the Controller's data subjects, it will not respond substantively on the merits. It will confirm receipt, forward the request to the Controller without undue delay and, where it can identify the person, tell them that the Controller is responsible for answering.

10. Deletion and return

The Controller can delete Projects and account data at any time using the controls in the account. On termination, Controller Personal Data is deleted from the active production database, except where retention is required by law. Backup copies held by the database provider persist for up to 30 days and are then overwritten. Prompts and inputs already transmitted to an AI subprocessor are subject to that provider's own retention, which the Processor cannot shorten retrospectively; see clause 5. Immediate irreversible erasure across every system is therefore not claimed.

Records the Operator holds as controller rather than as processor, in particular invoicing, acceptance and security records, are retained under the Privacy Policy and applicable statutory retention rules and are not deleted by this clause: invoicing and accounting records for six years (article 30 of the Spanish Commercial Code) and tax records for at least four years (article 66 of the Spanish General Tax Law).

11. Liability and precedence

Between the parties, liability under this Agreement follows the liability provisions of the Terms & Conditions, including the Business User limits in clause 30 of those Terms. Those limits do not apply to, and cannot reduce, a data subject's claim under Article 82 GDPR or the allocation of responsibility that Article 82 imposes between controller and processor, and they do not limit liability that law prohibits from being limited.

For processing carried out on the Controller's behalf, this Agreement prevails over the Terms & Conditions in case of conflict. For everything else, including the commercial terms of the Engagement, the Terms prevail. Mandatory statutory rules prevail over both.

12. External agents connected by the Controller

Where the Controller connects an external AI assistant to its own account through the MCP endpoint, that assistant reads the Controller's own data at the Controller's instruction. The operator of that assistant is not a subprocessor of the Processor: the Controller chooses it, authorises the access and is responsible for that provider's terms and for any onward processing it performs. The connection can be removed by the Controller at any time.