Kliv Data Processing Addendum

Version 1.0

1. Scope and how this addendum takes effect

1.1 This Data Processing Addendum ("DPA") is between Rational Ventures, Inc., 848 N Rainbow Blvd #3037, Las Vegas, NV 89107-1103, USA, which operates Kliv at kliv.dev ("Kliv"), and the person or entity that has accepted the Kliv Terms of Service ("Customer").

1.2 This DPA is part of the Kliv Terms of Service (the "Terms"). It takes effect when Customer accepts the Terms. For customers who accepted the Terms earlier, it takes effect when this version is published. No signature is needed.

1.3 Customer may request a countersigned copy by writing to feedback@kliv.dev.

1.4 This DPA applies where Data Protection Law applies to Kliv's processing of Customer Data that contains personal data.

2. Definitions

"Customer Data" means the personal data that Kliv processes on Customer's behalf in providing the Services. This includes data that Customer or the users of Customer's apps upload to or store in the apps Customer builds and hosts on Kliv, and personal data in Customer's builder inputs, app source, and the inputs to app functions and AI features. Annex I describes it.

"End Users" means the people who visit or use Customer's apps.

"Account Data" means personal data about Customer and its team members that Kliv processes for its own purposes, such as account registration, billing, security, support and service improvement, as described in the Kliv Privacy Policy. Account Data does not include Customer Data.

"Data Protection Law" means the EU General Data Protection Regulation 2016/679 ("GDPR"), the UK GDPR and UK Data Protection Act 2018, the Swiss Federal Act on Data Protection, and any other data protection law that applies to the processing of Customer Data under this DPA.

"Services" means the Kliv services provided under the Terms.

"Sub-processor" means a third party that Kliv engages to process Customer Data.

"SCCs" means the standard contractual clauses in the Annex to Commission Implementing Decision (EU) 2021/914.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, version B1.0 or its successor.

"Security Incident" means a personal data breach affecting Customer Data processed by Kliv or its Sub-processors, regardless of cause.

"controller", "processor", "data subject", "personal data", "processing" and "supervisory authority" have the meanings given in the GDPR.

3. Roles

3.1 Kliv provides hosting and app-building infrastructure. For Customer Data, Customer is the controller (or a processor acting for its own client) and Kliv is the processor (or sub-processor). Kliv processes Customer Data only on Customer's behalf.

3.2 For Account Data, Kliv is an independent controller. The Privacy Policy governs that processing and this DPA does not apply to it.

3.3 Connected services. Customer may connect third-party services to an app: the integrations under App Settings > Integrations, Customer's own Stripe account, its own SMTP server, its own domain registrar, and any API the app calls. Customer engages each of these services under its own agreement with that service. Kliv transmits data to and from them on Customer's instruction. They are not Kliv's Sub-processors, and any data processing agreement with them is for Customer to conclude.

4. Customer's instructions

4.1 Kliv processes Customer Data only on Customer's documented instructions. The Terms, this DPA, and Customer's use and configuration of the Services are Customer's complete instructions. Additional instructions need Kliv's written agreement.

4.2 Kliv will tell Customer if it believes an instruction breaks Data Protection Law. Kliv may pause that instruction until Customer confirms or changes it.

4.3 If a law that applies to Kliv requires other processing, Kliv will tell Customer before the processing, unless that law forbids it.

4.4 Kliv does not sell Customer Data, does not use it for advertising, and does not use it to train AI models. Kliv uses AI model providers with training on Customer Data turned off.

4.5 Enterprise customers may agree in an order form that AI processing for their account uses an AI model provider and credentials that Customer supplies. In that case the provider is engaged by Customer and is not Kliv's Sub-processor.

5. Customer's responsibilities

5.1 Customer is responsible for its apps: what they collect, their content, their End Users, and their compliance with the law. This includes having a legal basis for the processing, giving End Users the required notices, obtaining consents, and answering data subjects.

5.2 Customer controls its apps and their data through the Services. Customer is responsible for the access rules of its app databases and files, for what its apps send to connected services, and for the security of its own accounts and credentials.

5.3 Customer is responsible for deciding whether the Services and the measures in Annex II are appropriate for the Customer Data it chooses to process, including any special categories of personal data.

6. Confidentiality

Kliv limits access to Customer Data to people who need it to provide the Services and who are bound by a duty of confidentiality.

7. Security

7.1 Kliv applies the technical and organizational measures in Annex II. Kliv may change them, as long as the overall level of protection does not go down.

7.2 Kliv holds no security certification of its own. Certifications held by Sub-processors apply to their services only.

8. Sub-processors

8.1 Customer gives Kliv general written authorization to engage Sub-processors. The current list is in Annex III and at https://kliv.dev/subprocessors.

8.2 Kliv will update that list at least 30 days before a new Sub-processor starts processing Customer Data.

8.3 Customer may object on reasonable data protection grounds within 14 days of the update, by writing to the contact in section 1.3. The parties will look for a solution in good faith. If none is found, Customer may stop using the affected Services and terminate them. This is Customer's only remedy for an objection.

8.4 Kliv binds each Sub-processor by a written agreement with data protection obligations that give in substance the same protection as this DPA, and remains responsible to Customer for the Sub-processor's performance of them.

9. International transfers

9.1 Data location. The Services run in the regions Kliv operates from time to time, currently the United States. Sub-processors process Customer Data in the locations in Annex III. Customer authorizes these transfers. Enterprise customers may arrange a dedicated region or a private deployment of the service, as agreed in an order form.

9.2 Where Customer transfers Customer Data that is subject to the GDPR to Kliv, and no adequacy decision covers the transfer, the SCCs apply and are incorporated by reference, as follows:

- (a) Module Two (controller to processor) applies where Customer is a controller. Module Three (processor to processor) applies where Customer is a processor.
- (b) Clause 7 (docking clause) does not apply.
- (c) Clause 9: Option 2 (general written authorization) applies, with the notice period in section 8.2.
- (d) Clause 11: the optional language does not apply.
- (e) Clause 17: Option 1 applies. The governing law is the law of Ireland.
- (f) Clause 18(b): the courts of Ireland.
- (g) Annex I, Annex II and Annex III of the SCCs are Annex I, Annex II and Annex III of this DPA. Customer is the data exporter and Kliv the data importer.

- (h) The competent supervisory authority is determined under Clause 13 of the SCCs.
- (i) Audits under Clause 8.9 of the SCCs are carried out as described in section 13. This does not limit the rights of data subjects under the SCCs.

9.3 United Kingdom. For transfers subject to the UK GDPR, the UK Addendum applies and is incorporated by reference. Tables 1 to 3 are completed with the information in this DPA and its Annexes. In Table 4, neither party may end the UK Addendum under its section 19.

9.4 Switzerland. For transfers subject to the Swiss Federal Act on Data Protection, the SCCs apply with these changes: references to the GDPR mean the Swiss Act, the competent authority is the Federal Data Protection and Information Commissioner, and "Member State" includes Switzerland.

9.5 Where Kliv transfers Customer Data onward to a Sub-processor outside the European Economic Area, the United Kingdom or Switzerland, Kliv uses a transfer mechanism that Data Protection Law permits.

9.6 If the SCCs or the UK Addendum conflict with the rest of this DPA or the Terms, the SCCs or the UK Addendum prevail.

10. Assistance

10.1 Data subject requests. The Services let Customer read, correct, export and delete the data in its apps, and Customer uses these functions to answer requests from data subjects. If a data subject sends a request about Customer Data to Kliv, Kliv will refer the person to Customer where Kliv can identify the Customer, and will not answer the request itself.

10.2 Taking into account the nature of the processing and the information available to Kliv, Kliv will give Customer reasonable help with data subject requests that Customer cannot handle through the Services, with data protection impact assessments, and with consultations with a supervisory authority.

10.3 Kliv may charge its reasonable costs for help that goes beyond the standard functions of the Services and Kliv's published information.

11. Security Incidents

11.1 Kliv will notify Customer without undue delay after it becomes aware of a Security Incident.

11.2 The notice goes to the email address of the account owner. It will describe what Kliv knows about the nature of the incident, the data concerned, the likely consequences and the measures taken or planned. Kliv may give this information in stages.

11.3 Kliv will take reasonable steps to contain and remedy the incident. Customer is responsible for its own notifications to supervisory authorities and data subjects, and Kliv will give reasonable help with them.

11.4 A notice under this section is not an admission of fault or liability.

12. Deletion and return

12.1 During the term, Customer can retrieve and delete Customer Data through the Services.

12.2 At the end of the Services, Customer chooses whether Kliv returns or deletes Customer Data. Kliv returns Customer Data through the export functions of the Services. Further help with return is available under section 10.3.

12.3 Kliv deletes Customer Data from its production systems within a reasonable period after the Services end and any return is complete, or after Customer deletes an app or its account.

12.4 Copies in backups are not deleted individually. They expire on the backup schedule and are used only for recovery until then.

12.5 Kliv may keep Customer Data where a law that applies to Kliv requires it, for as long as that law requires.

13. Information and audits

13.1 On written request, at most once in any 12 months, Kliv will give Customer the information reasonably needed to show that Kliv meets its obligations under this DPA. This includes written answers to reasonable questions about Kliv's security measures, and the audit reports and certifications that its Sub-processors make available.

13.2 Customer agrees that the information in section 13.1 satisfies its audit rights under Data Protection Law and the SCCs. An on-site audit takes place only where Data Protection Law or a supervisory authority requires one. It needs reasonable written notice, is carried out in business hours by Customer or an independent auditor bound by confidentiality, must not disrupt the Services or give access to other customers' data, and is at Customer's cost, including Kliv's reasonable costs.

13.3 Information given under this section is Kliv's confidential information.

14. Liability

14.1 Each party's liability arising out of or in connection with this DPA is subject to the exclusions and limits of liability in the Terms, to the extent permitted by applicable law and the SCCs.

14.2 Nothing in this DPA limits the rights of data subjects under the SCCs or Data Protection Law, or any liability that cannot be limited by law.

15. General

15.1 Order of precedence. If documents conflict, this order applies: (1) the SCCs and the UK Addendum, where they apply; (2) this DPA; (3) the Terms.

15.2 Changes. Kliv may update this DPA where a law, a supervisory authority or a change in the Services requires it, or where the update does not materially reduce the protection of Customer Data. Kliv will post the updated version with a new version number and the date it takes effect.

15.3 Except where the SCCs or the UK Addendum say otherwise, the governing law and courts are those of the Terms.

15.4 This DPA ends when Kliv no longer processes Customer Data. If part of it is invalid, the rest stays in force.

Annex I: Details of the processing

A. Parties

Data exporter: Customer, with the name, address and contact details in its Kliv account. Role: controller, or processor for its own clients.

Data importer: Rational Ventures, Inc., 848 N Rainbow Blvd #3037, Las Vegas, NV 89107-1103, USA. Contact: feedback@kliv.dev. Role: processor.

B. Description of the processing

Subject matter. Hosting and operating the apps Customer builds on Kliv, and building and changing them on Customer's instruction.

Duration. The term of the Terms, plus the period until deletion under section 12.

Nature and purpose. Storage, retrieval, transmission, display, backup and deletion of Customer Data in order to provide the Services: app database, End User sign-in, file storage, email sending, payments integration, custom domains, server-side functions and AI features.

Data subjects. End Users of Customer's apps, such as visitors, registered users, buyers, subscribers and recipients of email the apps send, and other people whose data Customer or its End Users put into an app or into the builder.

Categories of personal data. Decided by Customer. Typically:

- sign-in data of End Users: email address, name, hashed password, sign-in provider identifiers, session data;
- whatever Customer's app stores in its database and file storage;
- recipient addresses and contents of email the app sends, with delivery, bounce and complaint status;
- customer and order records exchanged with Customer's Stripe account, such as name, email address, addresses and purchase history. Payment card numbers are captured and held by Stripe and do not reach Kliv;
- technical data of End Users: IP address, browser and device information;
- content that End Users enter into AI features Customer has built into an app;
- personal data in Customer's builder conversations, app source, and the inputs to app functions and AI features.

Special categories of data. Decided by Customer. See section 5.3.

Frequency. Continuous, for as long as Customer uses the Services.

Retention. As in section 12.

Sub-processors. As in Annex III, for the same subject matter and duration.

C. Competent supervisory authority

As in section 9.2(h).

Annex II: Technical and organizational measures

Encryption. Data is encrypted in transit over public networks. Stored data is encrypted at rest.

Access. Access to production systems and Customer Data is limited to authorized staff who need it to provide the Services.

Separation of customers. The Services keep each customer's data separate from other customers' data.

Backups. Data is backed up regularly. Backups are kept for up to 365 days.

Logging and monitoring. Kliv logs application errors and alerts operations staff to service problems.

Annex III: Sub-processors

Sub-processor	Purpose	Customer Data	Location
Amazon Web Services, Inc.	Cloud infrastructure and hosting	Customer Data processed in providing the Services	United States
Cloudflare, Inc.	Content delivery and network security	Data in transit to and from hosted apps	Global
Turso (ChiselStrike Inc.)	Database hosting	Data stored in app databases	United States
Fly.io, Inc.	Cloud infrastructure	Customer Data processed in providing the Services	United States
Mailgun Technologies, Inc.	Email delivery	Email recipients and content	United States
AI model providers	AI features of the Services. Kliv selects these providers from time to time and uses them with training on Customer Data turned off	Content provided to the AI	United States and China

Where an Enterprise customer has agreed in an order form to use its own AI model provider and credentials, that provider is engaged by Customer and is not a Sub-processor (section 4.5).

Services that Customer connects to an app are not Sub-processors. This covers the integrations under App Settings > Integrations, Customer's own Stripe account, SMTP server and domain registrar, and any API the app calls. Customer engages them under its own agreement with each service (section 3.3).