Data Processing Addendum

HSLA0001 Inc. · rams.ai · security@rams.ai

This DPA applies to every customer who uses Rams under the Rams Terms of Service, from the moment Rams processes Customer Personal Data. No signature is needed for it to apply. For a countersigned copy, email security@rams.ai.

This Data Processing Addendum ("DPA") forms part of the agreement under which HSLA0001 Inc., a New York corporation ("Rams", "Rams.ai" or "Processor"), provides its Rams product and service to the customer that uses it ("Customer", "Controller") (the "Agreement", meaning the Rams Terms of Service at rams.ai/terms together with any order form the parties sign). It applies wherever Rams processes Personal Data on Customer's behalf in providing the service.

1. Definitions

- Data Protection Laws: the EU General Data Protection Regulation 2016/679 ("EU GDPR"), the EU GDPR as retained in UK law with the UK Data Protection Act 2018 ("UK GDPR"), and any other data protection law that applies to the processing under the Agreement.
- Personal Data, Processing, Controller, Processor, Data Subject and Supervisory Authority have the meanings given in the Data Protection Laws.
- Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.
- Customer Personal Data: Personal Data processed by Rams on Customer's behalf under the Agreement, described in Annex 1.
- Subprocessor: a third party engaged by Rams that processes Customer Personal Data.
- EU SCCs: the standard contractual clauses approved by European Commission Implementing Decision (EU) 2021/914, Module Two (controller to processor).
- UK Addendum: the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018 (version B1.0, in force 21 March 2022).

2. Roles and instructions

2.1 Customer is the Controller and Rams is the Processor of Customer Personal Data.

2.2 Rams processes Customer Personal Data only on Customer's documented instructions, which are the Agreement, this DPA and Customer's use and configuration of the service, unless the law requires otherwise; in that case Rams informs Customer before processing unless the law prohibits it.

2.3 Rams tells Customer promptly if it believes an instruction breaks the Data Protection Laws.

2.4 Rams does not sell Customer Personal Data and does not use Customer content, including source code, to train machine learning models.

3. Confidentiality

Rams ensures that everyone it authorises to process Customer Personal Data is bound by confidentiality and has access only as needed to provide the service.

4. Security

Rams implements and maintains the technical and organisational measures in Annex 2, appropriate to the risk. Rams may update them over time provided the overall level of protection is not reduced.

5. Subprocessors

5.1 Customer gives general authorisation for Rams to engage the Subprocessors listed in Annex 3.

5.2 Rams gives Customer at least 30 days' notice by email before adding or replacing a Subprocessor. Customer may object on reasonable data protection grounds within that period; the parties will then discuss in good faith, and if they cannot resolve it, Customer may terminate the affected service and receive a pro-rata refund of prepaid fees for it.

5.3 Rams imposes data protection obligations on each Subprocessor that are no less protective than this DPA, and remains responsible to Customer for its Subprocessors' performance.

6. Data Subject requests

Taking into account the nature of the processing, Rams assists Customer by appropriate measures in responding to Data Subject requests. If Rams receives a request directly, it forwards it to Customer without undue delay and does not respond except on Customer's instruction.

7. Personal Data Breach

7.1 Rams notifies Customer without undue delay, and in any event within 72 hours of becoming aware of a Personal Data Breach.

7.2 The notice describes, as far as then known: the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed. Rams provides further information as it becomes available.

7.3 Rams takes reasonable steps to contain and remediate the breach and cooperates with Customer's own notifications. Notice goes to the email address of Customer's account owner, or to the address Customer designates in a countersigned copy of this DPA.

8. Assistance

Rams provides reasonable assistance with data protection impact assessments and prior consultations with Supervisory Authorities, to the extent required by the Data Protection Laws and taking into account the nature of the processing and the information available to Rams.

9. Deletion and return

9.1 Customer may delete its account at any time from Settings. Deletion is immediate and removes Customer's workspace, its stored reviews and the associated account records (it requires any active subscription to be cancelled and any other workspace members to be removed first). Database backups roll off after 7 days, so deleted data leaves backups within 7 days.

9.2 On termination of the Agreement, on Customer's written request, Rams deletes any remaining Customer Personal Data within 30 days, unless the law requires Rams to keep it. Before deletion, on request, Rams prepares an export of Customer's stored reviews in a machine-readable format.

9.3 Visual screenshots and applied patches are deleted automatically after 30 days, except those shown in a pull-request comment or an agent result, which are kept while that comment or result shows them and are deleted with the account.

10. Audits and information

10.1 Rams makes available all information reasonably needed to demonstrate compliance with this DPA, including written answers to Customer's security questionnaires and the current security reports its Subprocessors publish.

10.2 Where that information is not enough to meet an audit obligation under the Data Protection Laws, Customer may audit Rams' compliance once in any 12 months, on at least 30 days' written notice, during business hours, at Customer's cost, under confidentiality, and without access to other customers' data.

10.3 Rams has no independent security certification today. It will tell Customer if it obtains one.

11. International transfers

11.1 Rams and its Subprocessors process Customer Personal Data primarily in the United States (Annex 3).

11.2 EU transfers. To the extent Customer Personal Data subject to the EU GDPR is transferred to Rams outside the EEA in a country without an adequacy decision, the EU SCCs (Module Two) are incorporated into this DPA by reference, with: Clause 7 (docking) applying; Clause 9 option 2 (general authorisation, with the notice period in section 5.2); the optional language in Clause 11 not applying; Clause 17 option 1, governed by the law of Ireland; Clause 18, the courts of Ireland. Annexes I to III of the EU SCCs are completed by Annexes 1 to 3 of this DPA.

11.3 UK transfers. To the extent Customer Personal Data subject to the UK GDPR is transferred to Rams outside the UK, the UK Addendum is incorporated into this DPA by reference and applies to the EU SCCs as set out in section 11.2. For the UK Addendum: Table 1 is completed by the parties' details in this DPA (or in a

countersigned copy) and Annex 1; Table 2 selects the Approved EU SCCs, Module Two, as set out in section 11.2; Table 3 is completed by Annexes 1 to 3; and in Table 4, either party may end the UK Addendum as permitted by its Section 19.

11.4 Where a transfer can rely on an adequacy regulation or decision (including the UK-US data bridge for a certified recipient), the parties may rely on it instead.

12. Liability and precedence

12.1 Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement. Under the Rams Terms of Service (rams.ai/terms), neither party is liable for indirect, incidental, special, consequential or punitive damages, or for lost profits, revenue or data, and Rams' total liability arising out of or relating to the service, the Agreement and this DPA together is limited to the greater of the fees Customer paid in the 12 months before the event giving rise to the claim, or US$100. These limits do not apply to Customer's payment obligations, to liability that the law does not allow to be limited (such as for fraud or gross negligence), or where the Data Protection Laws do not permit them.

12.2 If this DPA conflicts with the Agreement, this DPA prevails as to the processing of Customer Personal Data. If the EU SCCs or the UK Addendum conflict with this DPA, the EU SCCs or the UK Addendum prevail.

13. Term

This DPA lasts as long as Rams processes Customer Personal Data under the Agreement.

Annex 1: Details of processing

- Subject matter and purpose: providing the Rams service: automated design and accessibility review of user-interface code in pull requests (GitHub App), through coding agents (MCP), and of public web pages Customer submits.
- Duration: the term of the Agreement and the deletion period in section 9.
- Nature of processing: receiving source files over TLS (the changed files of a pull request; and up to 50 existing UI files from the default branch for the first review on installation, an audit Customer requests, and a monthly drift check of one repository on paid plans), analysing them in memory with a third-party AI model, storing the resulting review (score, findings, short flagged excerpts and suggested fixes), posting reviews and check runs to Customer's pull requests, rendering components for visual before/after screenshots, account administration, billing and support.
- Data Subjects: Customer's users of the service (employees and contractors), and individuals whose names or identifiers may appear incidentally in reviewed source code or pull requests (for example authors in comments or commit metadata).
- Categories of Personal Data: account data (name, email address, GitHub or Google account identifiers and username); usage data (workspace activity, review metadata, IP address for rate limiting and security); pull-request metadata (repository, branch and pull-request identifiers, author usernames); any Personal Data contained incidentally in the source code excerpts Customer submits. Billing data is collected directly by Stripe.
- Special categories: none intended. Customer should not submit special category data in code.
- Frequency: continuous, for each review triggered.
- Retention: source files are discarded when a review returns; stored reviews persist for the life of the account; visual screenshots and patches are deleted after 30 days, except those shown in a pull-request comment or agent result, which are kept while shown and deleted with the account; pull-request outcome records hold no code and are deleted after 13 months; server logs, which can contain an email address or IP address but never source code, are kept up to 30 days; error reports are sent to Sentry without cookies, IP addresses or user identifiers and kept up to 90 days; database backups roll off after 7 days; deletion on request at any time, or within 30 days of a written request after termination (section 9).

Annex 2: Technical and organisational measures

- Encryption: all traffic over TLS; database encrypted at rest by the hosting provider.
- Data minimisation: for a pull request, only its changed files are fetched (plus up to six directly imported files for visual renders); outside pull requests, only UI files, at most 50 per review, from repositories Customer enables; source analysed in memory and discarded; only reviews and short excerpts stored.
- Access control: Row Level Security on every database table, scoped to the workspace; writes only from Rams servers; API keys stored as hashes, workspace-scoped and revocable; GitHub App tokens short-lived and scoped to one installation with minimal repository permissions; customer sign-in via GitHub or Google OAuth.
- Isolation: visual renders in a sandboxed headless browser that exists only for the render; artifacts in a private bucket scoped to the workspace and served through short-lived signed URLs; public page reviews in a fresh browser profile with private and internal addresses refused.

- Availability and resilience: managed hosting on providers that hold SOC 2 Type II reports; rate limiting on public API endpoints; error monitoring.
- Personnel: access to production limited to the founder and named staff bound by confidentiality. Two-factor authentication is required on every source-code, hosting, database, payments and email admin account (GitHub, Vercel, Google Cloud, Supabase, Stripe, Google Workspace).
- Operational alerts: internal alerts carry no names or email addresses (at most an email domain and a workspace identifier) and no source code.
- Vulnerability handling: security@rams.ai, with a response within 24 hours.
- AI provider terms: analysis under Anthropic's commercial API terms, under which customer content is not used to train models and inputs and outputs are deleted within 30 days, except requests its safety systems flag as usage-policy violations, which may be kept for up to 2 years. Rams has no zero-retention agreement with Anthropic.

Annex 3: Subprocessors

Subprocessor	Purpose	Location
Anthropic, PBC	AI analysis of submitted code	United States (Anthropic is a US company; it does not commit to US-only processing on its standard API)
Supabase, Inc.	Database and file storage	United States (AWS us-east-1, Virginia)
Google LLC (Google Cloud)	Review worker hosting	United States (us-east1, South Carolina)
Vercel Inc.	Web app hosting	United States (global edge network)
GitHub, Inc.	GitHub App integration	United States
Stripe, Inc.	Payments and billing	United States
Resend, Inc.	Transactional email	United States
Google LLC	Sign-in, site analytics and email (Google Workspace)	United States
Functional Software, Inc. (Sentry)	Error tracking	United States
Slack Technologies, LLC	Internal alerts to a private channel: Rams' operational alerts (at most an email domain and a workspace identifier, never a name or source code) and Sentry's error notifications	United States
Figma, Inc.	Only when Customer imports a Gate brand kit from Figma, with a token Customer provides for that request	United States