RAILS CLOUD

Data Processing Agreement

Governing the processing of personal data by Rails Cloud on behalf of Customers

Version	Effective Date	Classification	Jurisdiction
1.0	**1 March 2026**	**CONFIDENTIAL**	**Republic of Zimbabwe**

Parties to This Agreement

This Data Processing Agreement ("DPA" or "Agreement") is entered into between:

DATA PROCESSOR

Rails Net (Private) Limited
Trading as: Rails Zimbabwe / Rails Cloud
Registration: 84172A0722026
TIN: 2002425765
Incorporated: 19 February 2026, Zimbabwe
Contact: dpa@railscloud.co

DATA CONTROLLER

The Customer as identified in the applicable Rails Cloud Order Form or Subscription Agreement

Company name, registration, and contact details as set out in Schedule 1 of this Agreement.

The parties agree that this DPA supplements and forms part of the Rails Cloud Terms of Service and Master Subscription Agreement. In the event of conflict between this DPA and those agreements on data protection matters, this DPA shall prevail.

1. Definitions

In this Agreement, the following terms have the meanings set out below. Terms not defined here have the meanings given in the Rails Cloud Terms of Service or applicable data protection law.

Term	Definition
Applicable Data Protection Law	The Zimbabwe Cyber and Data Protection Act (Chapter 11:23), and any other applicable national, regional, or international data protection legislation that applies to the processing of Personal Data under this Agreement, including GDPR, POPIA, and NDPR where relevant to the Controller's operations.
Controller	The Customer, who determines the purposes and means of processing Personal Data using the Rails Cloud platform.
Processor	Rails Cloud, acting on behalf of the Controller when processing Personal Data through the provision of Rails Cloud services.

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person processed by the Processor on behalf of the Controller in connection with the provision of Rails Cloud services.
Processing	Any operation or set of operations performed on Personal Data, including collection, recording, organisation, storage, adaptation, retrieval, use, disclosure, erasure, or destruction.
Data Subject	The identified or identifiable natural person to whom Personal Data relates.
Sub-processor	Any third party engaged by the Processor to carry out specific processing activities on Personal Data on behalf of the Controller.
Security Incident	A confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.
Standard Contractual Clauses (SCCs)	The standard contractual clauses for the transfer of Personal Data to third countries as approved by applicable supervisory authorities.
Services	The Rails Cloud infrastructure services provided to the Customer as described in the applicable Order Form or Subscription Agreement.

2. Scope and Duration

2.1 Scope of Processing

This DPA applies to all Personal Data that the Controller submits to, stores on, or processes through the Rails Cloud platform in connection with the Services. The nature, purpose, categories of data, and categories of Data Subjects are set out in Schedule 2 (Processing Details) to this Agreement.

2.2 Duration

This DPA commences on the date the Customer first uses the Rails Cloud Services and remains in force for the duration of the Services subscription. Upon termination or expiry of the Services, the provisions of this DPA relating to post-termination data handling (Section 11) continue to apply for the period specified therein.

2.3 Relationship

The parties acknowledge that:

- The Controller is the data controller and determines the purposes and means of processing Personal Data
- The Processor processes Personal Data only on behalf of and under the documented instructions of the Controller
- Each party shall comply with Applicable Data Protection Law in respect of their respective roles

3. Processor Obligations

3.1 Processing on Instructions Only

The Processor shall process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or international organisation, unless required to do so by applicable law. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless prohibited by law on grounds of public interest.

CORE COMMITMENT	Rails Cloud will never process your customers' personal data for its own purposes. We act solely as your infrastructure — we process what you instruct us to process, nothing more.

3.2 Confidentiality

The Processor shall ensure that persons authorised to process Personal Data have committed to confidentiality or are under an appropriate statutory obligation of confidentiality. Access to Personal Data shall be limited to personnel who require such access to perform their duties in connection with the Services.

3.3 Security Measures

The Processor shall implement and maintain the technical and organisational security measures set out in Schedule 3 (Security Measures) to protect Personal Data against:

- Accidental or unlawful destruction or accidental loss
- Alteration, unauthorised disclosure, or access
- All other unlawful forms of processing

The Processor shall regularly review and, where appropriate, update these measures to account for changes in technology, the scope of processing, and emerging threats.

3.4 Assistance to Controller

Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligations to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Law, including:

- Rights of access, rectification, erasure, restriction, and portability
- Rights to object to processing
- Rights related to automated decision-making

The Processor shall notify the Controller within five (5) business days of receiving a Data Subject request and shall not respond to such requests directly unless authorised to do so by the Controller.

3.5 Data Protection Impact Assessments

The Processor shall provide reasonable assistance to the Controller in conducting Data Protection Impact Assessments (DPIAs) and prior consultations with supervisory authorities where required by Applicable Data Protection Law, to the extent such assistance relates to the processing activities performed by the Processor.

4. Controller Obligations

The Controller warrants and represents that:

1. It has a valid legal basis for the processing of Personal Data that it submits to or instructs the Processor to process
2. All Personal Data provided to the Processor has been collected and is being processed in compliance with Applicable Data Protection Law
3. It will provide Data Subjects with all required notices and information about the processing of their Personal Data, including disclosure that the Processor is processing data on the Controller's behalf
4. It will obtain all necessary consents where consent is required as the legal basis for processing
5. It will promptly update the Processor of any changes to its processing instructions that materially affect the Processor's obligations under this DPA
6. Its instructions to the Processor comply with Applicable Data Protection Law and do not place the Processor in breach of any applicable regulation

5. Sub-Processors

5.1 Authorisation

The Controller provides general written authorisation for the Processor to engage Sub-processors, subject to the conditions set out in this Section 5. The Processor's current list of approved Sub-processors is set out in Schedule 4 and maintained at railscloud.co/legal/subprocessors.

5.2 New Sub-processors

Before engaging any new Sub-processor who will process Personal Data, the Processor shall:

7. Give the Controller at least thirty (30) days prior written notice of the intended change, including the Sub-processor's identity, location, and the nature of processing to be performed
8. Provide the Controller with sufficient information to assess whether the new Sub-processor meets the standards required by this DPA
9. Allow the Controller a period of fifteen (15) days from notice to object to the appointment on reasonable data protection grounds

Where the Controller objects and the parties cannot resolve the objection, the Controller may terminate the affected Services upon thirty (30) days written notice without early termination penalties.

5.3 Sub-processor Obligations

The Processor shall impose data protection obligations on each Sub-processor that are no less protective than those set out in this DPA. The Processor remains fully liable to the Controller for the performance of the Sub-processor's obligations.

5.4 Current Sub-processors

Sub-processor	Service Provided	Location	Data Processed
Amazon Web Services (AWS)	Cloud infrastructure, compute, storage	Africa (Cape Town), EU	All Customer Data hosted on Rails Cloud
Payment processor (to be specified)	Payment processing for Rails Pay	Africa / Global	Transaction data, billing details
KYC provider (to be specified)	Identity verification for Rails Pay	Africa	Identity documents, verification results
Support platform	Customer support ticketing	To be confirmed	Support communications

6. Security Incident Notification

6.1 Notification Obligation

The Processor shall notify the Controller without undue delay, and in any event within forty-eight (48) hours of becoming aware of a confirmed Security Incident involving Personal Data processed on behalf of the Controller. Notification shall be made to the Controller's registered account email address and to dpa@railscloud.co.

6.2 Content of Notification

The initial notification shall include, to the extent then known:

- A description of the nature of the Security Incident, including the categories and approximate number of Data Subjects affected
- The categories and approximate volume of Personal Data records concerned
- The name and contact details of the Processor's data protection contact
- A description of the likely consequences of the Security Incident
- A description of the measures taken or proposed to address the Security Incident and to mitigate its possible adverse effects

6.3 Ongoing Communication

Where all required information cannot be provided in the initial notification, it shall be provided in phases without undue delay. The Processor shall cooperate fully with the Controller in investigating the Security Incident and in making any required notifications to supervisory authorities or Data Subjects.

6.4 No Admission

Notification of a Security Incident by the Processor does not constitute an acknowledgement of fault or liability. The Processor's obligation to notify does not prejudice the Controller's independent obligations under Applicable Data Protection Law.

7. International Data Transfers

7.1 Primary Processing Location

The Processor shall primarily process Personal Data within the African continent, using AWS infrastructure in the Cape Town region (af-south-1) where available. The Processor shall not transfer Personal Data outside Africa without the prior written consent of the Controller, except as set out in this Section 7.

7.2 Authorised Transfer Mechanisms

Where transfer of Personal Data outside Zimbabwe or the African Union is necessary for the provision of the Services, the Processor shall ensure that one of the following transfer mechanisms is in place:

- Standard Contractual Clauses (SCCs) as approved by the applicable supervisory authority
- An adequacy decision by the relevant authority recognising the receiving jurisdiction as providing adequate data protection
- Binding Corporate Rules where the transfer is within a group of companies
- Any other lawful transfer mechanism recognised under Applicable Data Protection Law

7.3 Controller Consent for Transfers

By entering into this DPA and selecting Services that involve processing in jurisdictions outside Africa, the Controller provides specific authorisation for such transfers subject to the mechanisms set out in Section 7.2. The Processor shall provide details of applicable transfer mechanisms upon request.

8. Audit and Inspection Rights

8.1 Documentation

The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with the obligations laid down in this DPA, including maintaining records of processing activities as required by Applicable Data Protection Law.

8.2 Audit Rights

The Controller shall have the right to conduct audits or inspections of the Processor's data processing activities under this DPA, subject to the following conditions:

10. The Controller shall give the Processor at least thirty (30) days written notice of an intended audit
11. Audits shall be conducted during normal business hours and in a manner that does not unreasonably disrupt the Processor's operations
12. The Controller may conduct no more than one (1) audit per calendar year unless there are reasonable grounds to suspect a Security Incident or material breach of this DPA
13. The Controller shall bear the costs of any audit unless the audit reveals a material breach of this DPA, in which case the Processor shall bear reasonable audit costs
14. Audit findings shall be treated as Confidential Information by both parties

8.3 Third-Party Audit Reports

In lieu of a direct audit, the Processor may satisfy the Controller's audit rights by providing third-party audit reports, penetration testing summaries, or security certifications, where these adequately address the Controller's audit objectives. The Controller may request such reports at any time upon reasonable notice.

9. Processing Instructions and Changes

9.1 Standard Instructions

The Controller's instructions to the Processor for the processing of Personal Data are set out in Schedule 2 and embodied in the Customer's use of the Rails Cloud Services in accordance with the applicable documentation. These instructions authorise the Processor to:

- Store and back up Personal Data on Rails Cloud infrastructure
- Replicate Personal Data for redundancy and disaster recovery purposes
- Access Personal Data for the purposes of providing technical support where authorised by the Controller
- Process Personal Data as necessary to detect, prevent, and respond to Security Incidents
- Perform routine maintenance and updates that incidentally involve access to stored Personal Data

9.2 Changes to Instructions

The Controller may issue updated or additional processing instructions at any time by written notice to dpa@railscloud.co. The Processor shall implement updated instructions within a reasonable timeframe and shall notify the Controller if it believes any instruction infringes Applicable Data Protection Law.

9.3 Processor's Right to Object

Where the Processor reasonably believes that a Controller instruction would cause the Processor to breach Applicable Data Protection Law or this DPA, the Processor shall notify the Controller in writing before implementing the instruction. The parties shall work together in good faith to resolve the issue.

10. Records of Processing Activities

The Processor shall maintain complete and accurate records of all processing activities carried out on behalf of the Controller, including:

- The name and contact details of the Processor and each Sub-processor
- The categories of processing carried out on behalf of each Controller
- Transfers of Personal Data to third countries and the transfer mechanisms relied upon
- A general description of the technical and organisational security measures implemented

These records shall be made available to the Controller and to supervisory authorities upon request.

11. Post-Termination Data Handling

11.1 Deletion or Return

Upon termination or expiry of the Services, the Processor shall, at the Controller's choice and within sixty (60) days of the effective termination date:

- Return all Personal Data to the Controller in a standard, portable format (as specified in the Rails Cloud Data Portability & Exit Policy); or
- Securely delete or destroy all Personal Data, including all copies and backups, and provide written certification of deletion within ten (10) business days of completion

11.2 Retention Exceptions

Notwithstanding Section 11.1, the Processor may retain Personal Data to the extent required by applicable law. Where the Processor retains Personal Data pursuant to a legal obligation, it shall:

- Notify the Controller of the retention and the legal basis for it
- Continue to apply all security and confidentiality obligations under this DPA to the retained data
- Delete the retained data as soon as the legal obligation permitting retention expires

11.3 Survival

Sections 3.2 (Confidentiality), 6 (Security Incident Notification), 10 (Records), 11 (Post-Termination), and 12 (Liability) shall survive termination or expiry of this DPA.

12. Liability

12.1 Each Party's Liability

Each party shall be liable for the damage caused by processing that infringes Applicable Data Protection Law. The Processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

12.2 Allocation Between Parties

Where both the Controller and the Processor are responsible for damage caused by a breach of this DPA or Applicable Data Protection Law, liability shall be allocated between the parties according to their respective degree of responsibility.

12.3 Cap on Liability

Subject to applicable law, the Processor's total aggregate liability to the Controller under or in connection with this DPA (whether in contract, tort, or otherwise) shall not exceed the total fees paid by the Controller for the affected Services in the twelve (12) months preceding the event giving rise to the claim. This cap does not apply to liability arising from willful misconduct or gross negligence.

12.4 Mutual Indemnification

Each party shall indemnify the other against claims, damages, fines, and costs arising from that party's breach of this DPA or Applicable Data Protection Law, subject to the liability cap in Section 12.3.

13. General Provisions

13.1 Governing Law

This DPA is governed by the laws of the Republic of Zimbabwe. Any disputes arising under this DPA shall be resolved in accordance with the dispute resolution provisions of the Rails Cloud Master Subscription Agreement.

13.2 Entire Agreement

This DPA, including its Schedules, constitutes the entire agreement between the parties with respect to data processing and supersedes all prior agreements, understandings, and representations relating to the subject matter hereof.

13.3 Amendments

This DPA may be amended by mutual written agreement of both parties. The Processor reserves the right to update this DPA to reflect changes in Applicable Data Protection Law, providing thirty (30) days written notice of material changes.

13.4 Severability

If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

13.5 Priority

In the event of conflict between this DPA and the Rails Cloud Terms of Service on data protection matters, this DPA shall prevail. In the event of conflict between this DPA and any Schedule, the body of this DPA shall prevail unless the Schedule expressly states otherwise.

SCHEDULES

Schedule 1 — Controller Details

To be completed by the Customer and returned to dpa@railscloud.co upon execution of this DPA.

Field	Controller Details
Legal Entity Name	
Registration Number	
Country of Incorporation	
Principal Address	
Data Protection Contact Name	
Data Protection Contact Email	
Rails Cloud Account ID	
Industry / Sector	

Field	Controller Details
Applicable Data Protection Regulation(s)	e.g. ZDCPA, GDPR, POPIA, NDPR

Schedule 2 — Processing Details

Nature and Purpose of Processing

Rails Cloud processes Personal Data on behalf of the Controller for the following purposes:

- Hosting, storing, and providing access to Customer Data on Rails Cloud infrastructure
- Backing up Customer Data for disaster recovery and business continuity
- Providing technical support and resolving service issues where access to Customer Data is required
- Monitoring platform performance and availability
- Processing financial transactions through Rails Pay on behalf of the Controller

Categories of Personal Data

The categories of Personal Data processed under this DPA are determined by the Controller. Typical categories include:

Category	Examples	Sensitivity
Identity data	Names, usernames, profile information	Standard
Contact data	Email addresses, phone numbers	Standard
Transaction data	Payment records, order history	Standard / Financial
Technical data	IP addresses, device IDs, logs	Standard
Special category data	Only if explicitly instructed by Controller	High — requires explicit consent

Categories of Data Subjects

The categories of Data Subjects whose Personal Data is processed under this DPA are determined by the Controller and may include:

- The Controller's customers and end users
- The Controller's employees and authorised users of the Rails Cloud account
- Third-party individuals whose data the Controller processes through Rails Cloud infrastructure

Schedule 3 — Security Measures

Rails Cloud implements the following technical and organisational security measures as part of its obligations under this DPA:

Control Area	Measures
Encryption at rest	AES-256 encryption for all data stored in Rails Cloud infrastructure, including databases, object storage, and backup snapshots
Encryption in transit	TLS 1.2 minimum for all data transmitted between Customer and Rails Cloud; TLS 1.3 supported and preferred
Access control	Role-based access control (RBAC); principle of least privilege; MFA mandatory for all privileged internal access; quarterly access reviews
Network security	Virtual Private Cloud (VPC) isolation; firewall rules; DDoS protection; intrusion detection and prevention systems
Vulnerability management	Automated dependency scanning on all production dependencies; patch management policy with critical patches applied within 48 hours; periodic third-party penetration testing
Physical security	Physical infrastructure hosted in AWS data centres with ISO 27001 / SOC 2 certifications; 24/7 physical access controls
Backup and recovery	Automated daily backups with point-in-time recovery; backup encryption; recovery testing performed quarterly
Incident response	Documented incident response plan; 24/7 monitoring with automated alerting; defined escalation paths; post-incident review for all P1/P2 events
Personnel security	Background checks for all personnel with access to production systems; mandatory privacy and security training; signed confidentiality agreements
Audit logging	All access to production systems and Customer Data logged with immutable audit trails; logs retained for minimum 12 months

Schedule 4 — Approved Sub-processors

The following Sub-processors are approved at the date of this DPA. The current and up-to-date list is maintained at railscloud.co/legal/subprocessors.

Sub-processor	Country	Service	Data Protection Basis
Amazon Web Services (AWS)	USA / South Africa	Infrastructure	AWS DPA + SCCs where applicable
Payment Processor (TBC)	To be confirmed	Payments	PCI-DSS + Data Processing Agreement
KYC Provider (TBC)	Africa	Identity verification	Data Processing Agreement

Execution

This Data Processing Agreement is entered into by the authorised representatives of each party as set out below. By signing, each party confirms that they have the authority to bind their respective organisations to the terms of this Agreement.

FOR RAILS NET (PRIVATE) LIMITED (Data Processor)

Signature:

Name:

Title:

Date:

FOR THE CUSTOMER / CONTROLLER

Signature:

Name:

Title:

Date:

Executed copies of this DPA should be returned to dpa@railscloud.co. This DPA forms part of the Rails Cloud legal framework. All legal documents available at railscloud.co/legal. Rails Net (Private) Limited, Registration 84172A0722026, TIN 2002425765, Zimbabwe.