

RAINFOREST PAY

DATA PROCESSING AND DATA SHARING ADDENDUM

This Data Processing and Data Sharing Addendum (this “Addendum”) is incorporated into, and forms part of, the agreement between Rainforest Pay, Inc. (“Rainforest”) and the counterparty identified in the applicable ordering document or platform agreement (“Platform”). This Addendum governs Rainforest’s Processing of Platform Data (defined below) in connection with the Services.

This Addendum is intended to (i) document the parties’ respective roles with respect to Platform Data, (ii) include the contractual restrictions and assurances required under applicable U.S. state privacy laws where and to the extent those laws apply to the parties and the relevant Processing, and (iii) provide transparency regarding the specific data flows, third-party disclosures, and retention practices that arise in the course of the Services.

1. Definitions

Capitalized terms not defined in this Addendum have the meanings given in the Platform Agreement. The following definitions apply:

“Applicable Privacy Laws” means the privacy, data protection, and data security laws, rules, regulations, and self-regulatory codes that apply to the parties’ Processing of Platform Data, including, where applicable, the California Consumer Privacy Act as amended by the California Privacy Rights Act (“CCPA/CPRA”), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Virginia Consumer Data Protection Act, the Texas Data Privacy and Security Act, and other U.S. state privacy laws as enacted or amended.

“Business,” “Consumer,” “Contractor,” “Personal Information,” “Processing,” “Sale,” “Sell,” “Service Provider,” and “Share” have the meanings given under Applicable Privacy Laws, to the extent applicable.

“End Customer” means an individual who initiates, attempts, or completes a transaction with a Merchant through a Platform-integrated checkout experience, including via Rainforest-hosted payment components (such as embeddable web components or hosted payment fields).

“Merchant” means a seller or sub-merchant that uses the Services through or under a Platform relationship.

“Platform Data” means data (including Personal Information) that Rainforest receives from or on behalf of Platform or Merchants, or collects in connection with providing the Services, including (i) End Customer transaction data, (ii) Merchant onboarding and underwriting data (including beneficial owner information), (iii) Platform user and support data, and (iv) device and behavioral data collected via Rainforest-hosted components or integrated third-party SDKs. Platform Data includes “Customer Data” as that term may be used in the parties’ commercial agreements.

“Payment Processing Services” means the Services required to execute, route, authorize, clear, settle, reconcile, and support payment transactions and related operational functions (including disputes, chargebacks, refunds, account updates, and customer support) as contemplated by the Platform Agreement.

“Risk & Compliance Services” means Services and activities that Rainforest performs to protect the integrity, security, and compliance of the payment ecosystem, including fraud prevention and detection, transaction monitoring, sanctions and politically exposed person (“PEP”) screening and monitoring, identity verification (KYC), business verification (KYB), anti-money laundering screening, platform and merchant risk management, and related model development, testing, tuning, and validation.

“Risk Vendor” means a specialized third-party vendor engaged by Rainforest to provide fraud detection, risk scoring, device intelligence, behavioral biometrics, identity verification, or compliance screening services. As of the Effective Date, Rainforest’s primary Risk Vendor is SardineAI Corp. (“Sardine”).

“Subprocessor” means a third party engaged by Rainforest to Process Platform Data on Rainforest’s behalf in connection with the Services.

2. Roles and Scope

The parties acknowledge that Rainforest’s role depends on the specific Processing activity and category of data, and that a single label (e.g., “service provider”) does not accurately describe the full scope of Rainforest’s operations.

Accordingly, this Addendum applies a dual-role model:

- **Payment Processing Services.** Rainforest Processes Platform Data on behalf of Platform and/or Merchants to execute and support transactions as instructed through the Platform integration.
- **Risk & Compliance Services.** Rainforest Processes Platform Data (including End Customer and Merchant data) as part of Rainforest’s independent fraud, security, and compliance program and in furtherance of Rainforest’s legal and programmatic obligations as a payments infrastructure provider.

Nothing in this Addendum requires Rainforest to provide End Customer-facing consumer experiences. Rainforest is a white-labeled payments infrastructure provider, and End Customers generally interact with Platform or Merchants, not directly with Rainforest.

2.1 Payment Processing Services: Processor / Service Provider

With respect to Platform Data Processed solely to provide the Payment Processing Services, Rainforest will act as a processor (where those concepts apply) and as a service provider or contractor (as applicable) for Platform under Applicable Privacy Laws, subject to Section 3 of this Addendum.

2.2 Risk & Compliance Services: Independent Business / Controller

With respect to Platform Data Processed to provide the Risk & Compliance Services, Rainforest acts as an independent controller/business (as applicable) under Applicable Privacy Laws.

Platform acknowledges that Rainforest:

- determines certain purposes and means of such Processing, including the selection of Risk Vendors, the creation and tuning of risk rules, and the decisioning applied to transactions;
- may use Platform Data for system integrity, fraud prevention, compliance screening, dispute management, and related analytics and model improvement across Merchants and Platforms; and
- when performing cross-merchant and cross-platform analytics for Risk & Compliance Services, may use transaction-level and pseudonymous data (including stable identifiers such as card hashes, device fingerprints, and hashed contact information) that remains linkable across Merchants and Platforms within Rainforest's internal systems, rather than solely aggregated or deidentified data.

Limitation on Use. Rainforest will not use Platform Data for consumer marketing or advertising to End Customers, and Rainforest does not provide cross-context behavioral advertising using Platform Data. Rainforest's use of Platform Data for Risk & Compliance Services is limited to fraud, security, compliance, transaction integrity, and closely related analytics and model validation.

2.3 No "Sale" or "Share" for Cross-Context Behavioral Advertising

Rainforest does not Sell or Share Platform Data for cross-context behavioral advertising, and Rainforest will not authorize any Subprocessor to do so on Rainforest's behalf.

2.4 Data Minimization and Integration Discipline

Platform will not provide Rainforest with data that is not reasonably necessary for the Services, and Platform will not include sensitive or special-category data in free-form metadata fields (e.g., "custom" JSON blobs) except where explicitly required for a supported Service feature and documented by the parties. Platform remains responsible for ensuring it has the legal right to disclose Platform Data to Rainforest and Rainforest's Subprocessors for the purposes described in this Addendum, including providing any required End Customer notices and obtaining any required consents.

2.5 Data Ownership

Platform retains ownership of Platform Data, subject to the licenses and rights granted in this Addendum and the Platform Agreement. Platform grants Rainforest a non-exclusive, worldwide, royalty-free right to host, Process, transmit, disclose, and otherwise use Platform Data as necessary to provide the Services and for the purposes described in this Addendum.

2.6 Deidentified and Aggregated Data

Rainforest may create and use deidentified or aggregated data derived from Platform Data for analytics, benchmarking, product improvement, and reporting, provided such data does not identify (and is not reasonably linkable to) an individual End Customer. Deidentified and aggregated data is not Platform Data for purposes of confidentiality or deletion obligations, to the extent permitted by law.

3. Terms Applicable to Rainforest as Processor / Service Provider (Payment Processing Services)

This Section 3 applies only to Platform Data Processed solely to provide the Payment Processing Services on behalf of Platform.

3.1 Instructions and Permitted Processing

Platform instructs Rainforest to Process Platform Data as necessary to provide the Payment Processing Services under the Platform Agreement, including to (i) execute and support transactions, (ii) provide transaction records and reconciliation, (iii) handle disputes, chargebacks, and refunds, (iv) provide customer support to Platform and Merchants, (v) maintain the security and reliability of the Services, (vi) to enhance and improve services, (vii) to identify and contact potential new clients, and (viii) comply with applicable law, card network rules, and sponsor bank requirements.

3.2 Confidentiality

Rainforest will ensure that personnel authorized to Process Platform Data are subject to appropriate confidentiality obligations, whether by contract or applicable professional duty.

3.3 Security

Rainforest will implement and maintain reasonable administrative, technical, and physical safeguards designed to protect Platform Data against unauthorized access, acquisition, disclosure, alteration, and destruction. Without limiting the foregoing, Rainforest maintains security controls aligned with payment industry requirements (including PCI DSS where applicable) and uses encryption and key management controls appropriate to the sensitivity of the data being processed.

3.4 Subprocessors

Platform authorizes Rainforest to engage Subprocessors to Process Platform Data for the Payment Processing Services, subject to the following:

- Rainforest will conduct reasonable diligence prior to engaging a Subprocessor to Process Platform Data.

- Rainforest will enter into a written agreement with each Subprocessor that includes data protection obligations no less protective than those set out in this Addendum (to the extent applicable to the service provided).
- Rainforest remains responsible for its Subprocessors' acts and omissions to the same extent Rainforest would be responsible if performing the Subprocessor's services directly, subject to the Platform Agreement's limitations of liability.
- Rainforest will make available an up-to-date list of Subprocessors in Schedule 2 and will provide reasonable prior notice of material changes to the list where practicable.

3.5 Assistance with Consumer Requests and Regulatory Inquiries

To the extent required under Applicable Privacy Laws and applicable to the Payment Processing Services, Rainforest will provide reasonable assistance to Platform in responding to verified consumer requests relating to Platform Data Processed by Rainforest as a service provider, including requests to access, delete, or correct Personal Information. Rainforest may require that Platform route requests through Platform as the primary interface with End Customers; Rainforest will cooperate with Platform to the extent reasonably necessary to support Platform's response.

If Rainforest receives a consumer request directly that relates to Platform-controlled data, Rainforest may direct the consumer to Platform (or the relevant Merchant) as the primary point of contact, unless applicable law requires a different approach.

3.6 Retention; Return / Deletion

Rainforest retains Platform Data for as long as necessary to provide the Services and for additional periods as required to comply with law, card network rules, sponsor bank requirements, accounting and audit obligations, and fraud and dispute management.

3.7 CCPA/CPRA Service Provider / Contractor Terms

Where CCPA/CPRA applies and Rainforest is acting as a service provider or contractor for Platform with respect to Payment Processing Services, Rainforest agrees and certifies that it will not:

- Sell or Share Personal Information;
- retain, use, or disclose Personal Information for any purpose other than for the specific purpose of performing the Payment Processing Services described in this Addendum and as otherwise permitted for service providers/contractors under CCPA/CPRA;
- retain, use, or disclose Personal Information outside of the direct business relationship between Platform and Rainforest, except as otherwise permitted by CCPA/CPRA; or
- combine Personal Information received from Platform with Personal Information received from or on behalf of another person, or collected from Rainforest's own

interaction with a consumer, except to the extent permitted for service providers/contractors under CCPA/CPRA for purposes such as security, fraud prevention, and compliance.

Rainforest will notify Platform if Rainforest determines that it can no longer meet its obligations under this Section 3.7 with respect to the Payment Processing Services. Upon Platform's written notice, Rainforest will take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information.

At Platform's reasonable request (not more than once per twelve-month period), Rainforest will make available information reasonably necessary to demonstrate compliance with this Section 3.7 and will cooperate with reasonable and appropriate compliance reviews (including written questionnaires or similar diligence), subject to confidentiality obligations and reasonable limitations on scope, timing, and access.

4. Terms Applicable to Rainforest as Independent Business / Controller (Risk & Compliance Services)

This Section 4 applies to Platform Data Processed in connection with Risk & Compliance Services, including fraud prevention and detection, transaction monitoring, KYC/KYB, sanctions/PEP screening and monitoring, AML screening, and related system integrity functions.

4.1 Purpose; Permitted Uses

Platform acknowledges that Rainforest's Risk & Compliance Services are operated as part of Rainforest's independent payments risk and compliance program. Rainforest may Process Platform Data for the following purposes:

- detecting, preventing, and investigating fraud, attempted fraud, and other suspicious activity;
- screening and monitoring for sanctions, PEPs, adverse media, and other compliance-related signals;
- performing identity verification (KYC) and business verification (KYB) and ongoing portfolio monitoring;
- managing payment risk, chargebacks, disputes, refunds, account updates, and transactional integrity;
- maintaining the security, reliability, and integrity of Rainforest systems and the payment ecosystem; and
- developing, testing, tuning, and improving risk and compliance models, rules, and controls, including across Merchants and Platforms, subject to the restrictions in this Addendum (including Section 2.3).

Limitation. Rainforest will not use Platform Data to build advertising profiles or for cross-context behavioral advertising. Rainforest's use of Platform Data for Risk & Compliance

Services is limited to fraud, security, compliance, transaction integrity, and closely related analytics and model validation.

4.2 Disclosures to Risk Vendors and Third Parties

In connection with Risk & Compliance Services, Rainforest may disclose Platform Data to:

- Risk Vendors and specialized fraud/compliance vendors (including Sardine) engaged by Rainforest;
- payment processors, gateways, sponsor banks, and card networks as required to execute transactions and manage risk; and
- regulators, law enforcement, and other parties where required by law or where reasonably necessary to protect the Services and the payment ecosystem.

Stable Identifiers and Linkability. Platform acknowledges that Rainforest transmits stable identifiers to Risk Vendors (including session keys, internal transaction and merchant identifiers, card number hashes, and device fingerprints) that enable the Risk Vendor to link data across transactions, merchants, and platforms for fraud detection and compliance monitoring purposes. Additionally, fields such as name, address, email, phone, tax identifiers, and bank account information transmitted as part of risk and KYC/KYB payloads may be used by the Risk Vendor for identity resolution and ongoing monitoring.

4.3 End Customer Notices and Transparency

Because End Customers generally interact with Platform or Merchants, Platform is responsible for providing End Customer-facing notices and choices required under Applicable Privacy Laws for the collection and disclosure of Platform Data to Rainforest and Rainforest's vendors for the purposes described in this Addendum. This includes, without limitation, disclosing the collection and use of device intelligence and behavioral biometrics by third-party SDKs integrated into Rainforest-hosted payment components.

4.4 Data Subject Requests

Each party is responsible for responding to data subject requests applicable to Personal Information for which it acts as a business/controller, subject to Applicable Privacy Laws. Rainforest will make commercially reasonable efforts to coordinate with Platform where a request relates to Platform Data and where Platform is the primary point of contact for End Customers.

5. Security Incidents

5.1 Rainforest Notification

Rainforest will notify Platform without undue delay after Rainforest confirms a security incident involving unauthorized access to, acquisition of, or disclosure of Platform Data in Rainforest's direct control that has a material impact on Platform, Merchants, or related data subjects' rights

(“Security Incident”). Rainforest’s notification will describe, to the extent known, the nature of the incident, the categories and approximate volume of data affected, and the measures taken or proposed to mitigate adverse effects.

Rainforest’s obligation to report a Security Incident is not and will not be construed as an acknowledgement of fault or liability. Except as required by law, Rainforest will not issue any public notice of a Security Incident that names Platform without first consulting Platform.

5.2 Platform Notification

Platform will notify Rainforest without undue delay if Platform becomes aware of any unauthorized access to, disclosure of, or loss of Platform Data or Rainforest credentials on Platform’s systems. Platform will not issue any public notice of such incident that names Rainforest without first consulting Rainforest.

6. Cooperation and Audit

At a party’s request and at the requesting party’s expense, the parties will provide each other reasonable assistance (taking into account the nature of Processing and the information available) with respect to data protection impact assessments, regulatory inquiries, and notifications to regulators, to the extent required by Applicable Privacy Laws.

As required to comply with Applicable Privacy Laws, in the event that a regulator conducts an investigation, audit, or review of Platform which requires additional information regarding Rainforest’s operations, Rainforest will cooperate reasonably with the same at Platform’s expense. Rainforest may satisfy audit requests through the provision of relevant certifications, audit reports (such as SOC 2 Type II), or written responses to reasonable questionnaires, in lieu of on-site inspections, to the extent permitted by law.

7. Limitation of Liability and Indemnity

7.1 Limitation of Liability

Rainforest will not be liable in connection with this Addendum, under any legal theory (whether in contract, tort, or otherwise), for any indirect, special, incidental, consequential, exemplary, or punitive damages, or for any loss of data, revenues, or profits, even if Rainforest knew or should have known of the possibility of such damages. Rainforest’s aggregate liability under this Addendum will be limited according to the terms of the Platform Agreement.

7.2 Platform Indemnity

Platform will indemnify, defend, and hold harmless Rainforest and its affiliates from any claims, actions, suits, demands, losses, liabilities, damages, costs, and expenses (including reasonable attorney’s fees) arising from or in connection with: (i) breaches of this Addendum by Platform or its Merchants; (ii) acts or omissions of Platform or its Merchants relating to Platform Data or the Services; (iii) Platform’s failure to provide required notices or obtain required consents under

Applicable Privacy Laws; (iv) Rainforest's use of Platform Data in accordance with this Addendum and the Platform Agreement; and (v) Platform's or its Merchants' breach of any applicable laws or regulations.

8. Miscellaneous

8.1 Order of Precedence

In the event of a conflict between this Addendum and the Platform Agreement with respect to Platform Data, this Addendum will control. In the event of a conflict between this Addendum and the Rainforest Processing Terms and Conditions as they relate to Platform or Merchant data, this Addendum will control as between Rainforest and Platform. Except as expressly modified by this Addendum, the Platform Agreement remains in full force and effect.

8.2 Changes in Law

If any variation to this Addendum is required as a result of a change in Applicable Privacy Laws, either party may provide written notice to the other of the required change. No additional terms will be effective unless agreed by both parties in a signed writing.

8.3 No Third-Party Beneficiaries

This Addendum is between the parties only. No third-party beneficiaries are intended or created by this Addendum.

8.4 Governing Law

This Addendum is governed by the governing law and dispute resolution provisions of the Platform Agreement.

8.5 Severability

If any provision of this Addendum is held invalid or unenforceable, it will be reformed only insofar as necessary to make it lawful and enforceable, or severed without effect on the remaining terms.

Schedule 1 — Description of Processing

Subject matter: provision of Payment Processing Services and Risk & Compliance Services as described in the Platform Agreement and this Addendum.

Duration: for the term of the Platform Agreement and any additional retention periods as described in Section 3.6 and Schedule 3.

Categories of data subjects: (i) End Customers; (ii) Merchant representatives and beneficial owners; (iii) Platform and Merchant users and administrators; (iv) individuals screened for sanctions, PEP, or adverse media in connection with onboarding and ongoing monitoring.

Categories of Personal Information (non-exhaustive) may include:

- Identifiers and contact information (e.g., name, email, phone, mailing address, billing and shipping address);
- Government identifiers and verification attributes (e.g., SSN/EIN, date of birth, identity document verification results);
- Transaction and commercial information (e.g., transaction ID, amount, currency, MCC, items, shipping address);
- Payment method information (e.g., card BIN/last4/hash/brand, expiry, bank account and routing numbers, digital wallet identifiers/tokens);
- Device and network information (e.g., IP address, language, user agent, device and session identifiers, browser type, operating system);
- Device intelligence and behavioral biometrics collected via third-party SDKs (e.g., Sardine SDK) embedded in Rainforest-hosted payment components;
- Fraud, risk, and compliance signals and scores (including rule triggers, risk levels, and vendor response data);
- KYC/KYB and sanctions screening data (including beneficial owner information, ownership percentages, and screening configuration);
- Customer support communications; and
- Platform-provided merchant risk indicators (e.g., historical volume, average ticket, subscription data).

Schedule 2 — Subprocessors (as of June 30, 2026)

Rainforest may update this list from time to time

Subprocessor	Services	Data Categories
Amazon Web Services (AWS)	Hosting, storage, logging, and infrastructure supporting the Services.	All Platform Data categories
SardineAI Corp.	Fraud detection and risk scoring; device intelligence and behavioral biometrics; KYC/KYB; sanctions/PEP screening and portfolio monitoring.	Transaction, identity, device, payment, and compliance data
Hubspot	Customer support ticketing and communications (as applicable).	Contact information, support communications

Note: Payment processors, gateways, sponsor banks, and card networks are generally independent third parties involved in transaction execution and oversight, and are not treated as Rainforest Subprocessors for purposes of this Addendum.