

# Data processing addendum

Version 1.0 | October 5, 2026

This Data Processing Addendum ("DPA") forms part of the agreement governing the Services between Relativity Labs Inc. d/b/a String AI ("String") and the customer identified in that agreement ("Customer"). That agreement, including its applicable order forms, is the "Agreement." This DPA takes effect when both parties execute it or expressly incorporate it into the Agreement.

## 1. Scope and definitions

1.1 This DPA applies to personal data String processes on Customer's behalf in providing the String Web Access API or managed data services ("Customer Personal Data"). It applies to the extent that processing is subject to the EU General Data Protection Regulation (Regulation (EU) 2016/679), the UK GDPR and Data Protection Act 2018, or other applicable data protection law (together, "Data Protection Law").

1.2 "Controller," "processor," "personal data," "processing," "personal data breach" and "data subject" have the meanings given in applicable Data Protection Law. A "Subprocessor" is a third party String engages to process Customer Personal Data on Customer's behalf. The "Services" are the services specified in the Agreement.

1.3 Customer acts as controller, or as processor on behalf of another controller. String acts as processor or subprocessor, respectively. Where Customer is a processor, Customer confirms that its controller has authorized the instructions, subprocessors and transfers contemplated by this DPA. Annex I describes the processing.

1.4 String separately processes account, authentication, billing and business-contact information as an independent controller where it determines the purposes and means of that processing for its own relationship with Customer, as described in String's Privacy Policy. This allocation does not exclude information from this DPA merely because it appears in a log, URL, email or metadata field: information processed on Customer's behalf remains Customer Personal Data.

## 2. Instructions and permitted use

2.1 String shall process Customer Personal Data only on Customer's documented instructions, including instructions concerning transfers. The Agreement, this DPA, Customer's API requests, agreed dataset specifications and subsequent written instructions constitute those instructions. If EU, Member State or UK law requires different processing, String shall inform Customer before processing unless that law prohibits notice on important grounds of public interest.

2.2 String shall immediately inform Customer if, in String's opinion, an instruction infringes Data Protection Law. The parties shall resolve the issue before the affected processing continues. String is not required to provide legal advice to Customer.

## STRING

2.3 Customer shall establish a lawful basis for its instructions and use of the Services, provide required notices and permissions, and limit personal data to what is necessary for the agreed purposes. String remains responsible for its own obligations under Data Protection Law.

2.4 String shall not sell Customer Personal Data, use it for advertising, disclose it to other customers, or use Customer's request URLs or returned content to train machine-learning models. Processing to provide, secure, support and troubleshoot the Services remains subject to Customer's instructions and this DPA.

### 3. Confidentiality and security

3.1 String shall ensure that personnel authorized to process Customer Personal Data are subject to confidentiality obligations or an appropriate statutory duty of confidentiality, and receive training appropriate to their access and responsibilities.

3.2 String shall implement and maintain the technical and organizational measures in Annex II and the measures required by Article 32 of the GDPR, taking into account the state of the art, implementation costs, the processing and its risks to individuals. String may update those measures without materially reducing the overall protection of Customer Personal Data.

3.3 Additional security requirements apply only where agreed in writing. A roadmap, target date or audit in progress is not a representation that a planned control or audit report already exists.

### 4. Subprocessors

4.1 Customer gives general written authorization for the Subprocessors identified in Annex III and the current service-specific list supplied to Customer. String shall provide that list before processing begins and on request. The access page is <https://usestring.ai/subprocessors>; requests may be sent to [support@usestring.ai](mailto:support@usestring.ai).

4.2 String shall give Customer written notice, including by email to Customer's designated contact, at least fifteen days before a new or replacement Subprocessor begins processing Customer Personal Data. The notice shall identify the provider, processing purpose and location. String shall also update its list. Posting an update alone does not replace this notice.

4.3 Customer may object within fifteen days after notice on reasonable data protection grounds. The parties shall work in good faith to resolve the objection. String shall not provide the affected Customer Personal Data to the proposed Subprocessor while the objection remains unresolved. If no reasonable alternative is agreed within thirty days after the objection, either party may terminate the affected Services by written notice. This termination right does not limit rights or remedies that Data Protection Law or the Standard Contractual Clauses make non-waivable.

4.4 Before processing begins, String shall bind each Subprocessor by written terms imposing the applicable data protection obligations required by Article 28(4), including sufficient guarantees of appropriate technical and organizational measures. String remains responsible to Customer for each Subprocessor's performance of those obligations.

4.5 A provider's classification follows the processing it actually performs. This DPA does not exempt a provider that processes Customer Personal Data from the requirements of this section because the provider is described as a proxy, infrastructure service or other vendor.

## **5. Individual rights and assistance**

5.1 Taking into account the nature of processing, String shall assist Customer through appropriate technical and organizational measures, insofar as possible, in responding to requests to exercise data subject rights. String shall forward requests concerning Customer Personal Data to Customer without undue delay, preserve the original receipt date, and respond on the merits only on Customer's instructions or as required by law.

5.2 Taking into account the processing and information available to String, String shall assist Customer with security, breach notifications, data protection impact assessments and prior consultation with supervisory authorities as required by Articles 32 to 36 of the GDPR. Customer may send requests to support@usestring.ai with "PRIVACY" in the subject line.

## **6. Personal data breaches**

6.1 String shall notify Customer without undue delay, and in any event within 72 hours after becoming aware of a personal data breach affecting Customer Personal Data. String shall use the incident or privacy contact designated by Customer. Incomplete information shall not delay the initial notice.

6.2 To the extent available, the notice shall describe the breach, the categories and approximate numbers of affected individuals and records, likely consequences, measures taken or proposed, and a contact for further information. String may provide information in phases and shall provide material updates without undue delay.

6.3 String shall take reasonable steps to contain, investigate and remedy the breach, cooperate with Customer, and provide the assistance required for Customer's own notification obligations. Notification does not itself constitute an admission of liability.

## **7. Retention, return and deletion**

7.1 String shall retain Customer Personal Data only for as long as necessary to provide the agreed Services and carry out Customer's instructions, subject to the retention terms in the Agreement. At the end of the Services, or on Customer's written instruction, String shall, at Customer's choice, return or securely delete Customer Personal Data and delete existing copies without undue delay, unless EU, Member State or UK law requires continued storage.

7.2 Data retained because of a legal requirement remains protected under this DPA and shall be processed only for that requirement. Copies in backups that cannot immediately be selectively deleted shall be put beyond use, remain protected and be deleted on the next applicable deletion cycle. String shall disclose the applicable cycle to Customer on request and shall not extend it to avoid deletion. If a backup is restored for recovery, String shall reapply the required deletions before returning the restored data to normal use.

7.3 String's obligations cover copies under its or its Subprocessors' control, including collection, curation and delivery-staging copies. Customer is responsible for copies delivered to Customer-controlled destinations. String shall revoke delivery access it administers when that access is no longer authorized and, on request, confirm completion of return or deletion in writing.

7.4 Any agreed retention or response period must permit the parties to meet Data Protection Law. Customer may specify additional retention instructions in an order form; a service-specific schedule does not reduce the deletion obligations above.

## **8. Information, audits and inspections**

8.1 String shall provide information necessary to demonstrate compliance with Article 28 and this DPA, and allow and contribute to audits and inspections by Customer or an auditor mandated by Customer.

8.2 The parties shall first use available policies, security questionnaires, independent assessment summaries and audit reports, subject to appropriate confidentiality terms. If those materials do not reasonably answer the relevant compliance questions, Customer may inspect the processing operations through a qualified independent auditor subject to reasonable confidentiality and security arrangements.

8.3 Except where a breach, supervisory authority or Data Protection Law requires otherwise, inspections require thirty days' written notice, occur during business hours, avoid unreasonable disruption and take place no more than once in twelve months. Those arrangements shall not prevent an audit necessary to meet Data Protection Law. Each party bears its own costs unless the Agreement states otherwise.

8.4 String need not disclose another customer's data, legally privileged material or information whose disclosure is prohibited by law. It shall provide an appropriate alternative where necessary to demonstrate compliance without exposing that information.

## **9. International transfers**

9.1 String is established in the United States. Processing locations and applicable Subprocessors are disclosed in the service-specific list. Where a transfer requires safeguards under Data Protection Law, String and Customer shall implement those safeguards before the transfer. Nothing in this DPA states that public availability of source data removes transfer obligations.

9.2 For restricted transfers subject to the EU GDPR for which an adequacy decision or another valid transfer mechanism does not apply, the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 ("EU SCCs") are incorporated by reference, without modification of their mandatory text: [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj).

9.3 Customer is the exporter and String the importer. Module Two applies where Customer is controller; Module Three applies where Customer is processor. Clause 7 does not apply. Clause 9(a), Option 2 applies with the fifteen-day prior-notice period in section 4.2. The optional language in Clause 11(a) does not apply. Clause 17 uses Option 1 and Irish law; Clause 18 names the courts of Ireland. The competent supervisory authority is determined under Clause 13 based on the exporter and transfer, as recorded in Annex I. Annexes I and II below complete the corresponding EU SCC annexes; Annex III and the list supplied under section 4 identify the authorized Subprocessors.

9.4 For restricted transfers subject to the UK GDPR, the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner, version B1.0 in force on March 21, 2022 ("UK Addendum"), is incorporated with its mandatory clauses: <https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf>. Table 1 uses the parties, contacts and effective date in this DPA and the Agreement. Table 2 uses the EU SCCs and applicable module selected in section 9.3. Table 3 uses Annexes I and II and the Subprocessor list. In Table 4, the importer may end the Addendum as permitted by section 19 of the UK Addendum.

9.5 The parties shall provide information and cooperation required by the applicable transfer mechanism, including assessment of relevant destination-country laws and additional safeguards where necessary. If the mechanism becomes unavailable, the parties shall implement a valid alternative or suspend the affected transfer until lawful safeguards are in place.

## **10. Liability, priority and term**

10.1 The Agreement's liability provisions apply to this DPA, except where Data Protection Law, the EU SCCs or UK Addendum prohibit a limitation. Nothing limits an individual's rights or a party's obligations under those instruments.

10.2 In a conflict, the EU SCCs and UK Addendum prevail for the transfers they govern, followed by this DPA and then the Agreement. Except for the transfer instruments' mandatory elections, this DPA follows the Agreement's governing law and dispute provisions.

10.3 This DPA remains effective until Customer Personal Data has been returned or deleted as required above. Confidentiality and protection obligations continue for any lawfully retained data. Neither party's execution of this DPA constitutes a claim that a supervisory authority or auditor has approved the Services.

## Annex I: Processing details and parties

| Item                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exporter                   | Customer, with its legal name, address and privacy contact as stated in the Agreement or signature block below.                                                                                                                                                                                                                                                                                                                                                                      |
| Importer                   | Relativity Labs Inc. d/b/a String AI, 651 North Broad Street, Suite 201, Middletown, DE 19709, United States. Privacy contact: support@usestring.ai, subject "PRIVACY".                                                                                                                                                                                                                                                                                                              |
| Roles                      | Customer is controller or processor as specified in the Agreement and section 1.3; String is processor or subprocessor.                                                                                                                                                                                                                                                                                                                                                              |
| Subject matter and purpose | Providing the purchased Web Access API or managed data services, including retrieval, collection, extraction, structuring, delivery, support and protection of the Services on Customer's instructions.                                                                                                                                                                                                                                                                              |
| Nature of processing       | Receipt, retrieval, transmission, organization, analysis, temporary or continuing storage as instructed, access control, delivery, return and deletion. LLM-assisted extraction may be used where applicable to the purchased service.                                                                                                                                                                                                                                               |
| Data subjects              | People whose personal data appears in customer-directed requests, public source content, agreed datasets or related communications processed on Customer's behalf.                                                                                                                                                                                                                                                                                                                   |
| Personal-data categories   | Public-source information selected by Customer or within the agreed dataset specification, which may include names, professional contact details, roles, profile information and other information in the source; request content, URLs, metadata and communications to the extent they contain personal data processed on Customer's behalf. The order form may narrow the categories.                                                                                              |
| Sensitive data             | The Services are not directed at special-category data or criminal-offence data. Customer shall not deliberately submit or instruct collection of such data without prior written agreement on scope and additional safeguards. Incidental data receives the same access restrictions, security and deletion protections as other Customer Personal Data, with additional measures where its risk requires them. PHI requires a separate signed BAA and an approved scoped workflow. |
| Frequency                  | Continuous as Customer invokes the API, or at the delivery frequency in the managed-services order form.                                                                                                                                                                                                                                                                                                                                                                             |

## STRING

| Item                            | Description                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Duration and retention          | The service term and the time necessary to complete return or deletion under section 7. Retention follows Customer's instructions and any agreed schedule, subject to legally required storage.                                                                                                                         |
| Competent supervisory authority | The authority determined by EU SCC Clause 13: the authority for the exporter's relevant EU establishment; where applicable, the authority for its EU representative; or an authority in a Member State where affected data subjects are located. The Customer identifies that authority in the execution details below. |

For the Web Access API, Customer selects the target URLs and requests. For managed data services, processing follows the agreed dataset specification and source-selection requirements. Independent-controller account processing under section 1.4 remains separate.

## Annex II: Technical and organizational measures

1. String maintains documented security policies, named security and compliance owners, risk assessments, personnel confidentiality obligations and security-awareness training.
2. Access uses managed identities, MFA requirements, role-based permissions and documented provisioning and removal procedures. Access rights and privileged roles are reviewed periodically.
3. Public API and web endpoints use TLS 1.2 or higher. Cloud data at rest uses provider-managed encryption. Secrets are held in managed secret storage with restricted access.
4. Personnel devices must use FileVault, macOS firewall, automatic updates, password-protected screen locks and built-in Gatekeeper/XProtect protection. Current device compliance uses annual, joiner and device-change self-attestation. Mosyle is a planned control, with rollout targeted by November 30, 2026; it is not represented as deployed at the date of this template.
5. Cloud controls restrict administrative access and network exposure. Offboarding revokes relevant credentials, sessions, system permissions and private-network membership. Devices are personally owned; String does not represent that it can remotely erase them.
6. Source code is version-controlled. Changes follow documented review, testing and deployment procedures, with records retained for review. Security checks and dependency review support remediation according to risk.
7. Centralized cloud logging and selected automated alerts support investigation of security and availability events. String maintains incident-response procedures and the notification obligations in section 6.
8. Backups and provider recovery features support documented business-continuity and recovery procedures. String evaluates recovery controls and retains evidence; no untested recovery-time guarantee is created by this Annex.
9. Data handling follows classification, authorized-storage and retention requirements. Access is limited by purpose and role; deletion and return follow section 7.
10. String maintains a vendor inventory and risk-review process and contracts with Subprocessors under section 4. Independent assessment summaries and policies are available subject to reasonable confidentiality arrangements. A SOC 2 audit in progress is not an issued report or certification.

## Annex III: Providers supporting the Services

The following providers are disclosed for transparency across String's services. A provider is a Subprocessor under this DPA to the extent it processes Customer Personal Data on Customer's behalf. Service applicability and processing locations are recorded in the list supplied under section 4.1; that list forms part of this Annex. Providers used solely for String's independent-controller activities remain subject to String's separate vendor agreements.

| Provider                           | Purpose                                                                |
|------------------------------------|------------------------------------------------------------------------|
| Google Cloud Platform (Google LLC) | Cloud compute, storage, analytics, logging and secrets management      |
| Amazon Web Services                | S3 dataset delivery                                                    |
| Snowflake                          | Dataset delivery and warehousing                                       |
| DigitalOcean                       | Managed PostgreSQL and backups                                         |
| Anthropic                          | LLM inference for extraction and processing                            |
| OpenAI                             | LLM inference                                                          |
| Langfuse                           | LLM tracing and observability                                          |
| Resend (Plus Five Five, Inc.)      | Transactional email, including recipient addresses and message content |
| Clerk                              | Portal authentication                                                  |
| Stripe                             | Payments and subscription billing                                      |
| Sentry                             | Error monitoring and masked session replay                             |
| PostHog                            | Product analytics and session recording                                |
| HubSpot                            | CRM and customer communications                                        |
| Google Workspace (Google LLC)      | Email, documents and identity                                          |

**STRING**

String shall identify any additional provider that processes Customer Personal Data under section 4 before that processing begins. The applicable list must be supplied with the execution copy; this Annex does not authorize undisclosed providers.

**Execution details**

Customer legal name: \_\_\_\_\_

Customer address: \_\_\_\_\_

Customer privacy and incident-notification contact: \_\_\_\_\_

Agreement / order form and date: \_\_\_\_\_

Customer role: Controller / Processor (select applicable role)

Competent EU supervisory authority, where applicable under Annex I: \_\_\_\_\_

Service-specific Subprocessor list version/date supplied with this DPA: \_\_\_\_\_

Effective date: \_\_\_\_\_

| For Relativity Labs Inc. d/b/a String AI | For Customer                |
|------------------------------------------|-----------------------------|
| Authorized signatory: _____              | Authorized signatory: _____ |
| Name and title: _____                    | Name and title: _____       |
| Date: _____                              | Date: _____                 |