DATA PROCESSING ADDENDUM

ContentRX LLC

Effective May 12, 2026. This Addendum supplements the ContentRX Terms of Service at contentrx.io/terms and applies whenever ContentRX processes Personal Data on behalf of Customer.

Starter template. This Addendum is a Common Paper-derived draft (CC BY 4.0) adapted to ContentRX specifics. It has not yet completed independent legal review. Customer counsel should review the document before relying on any specific clause in a material way. ContentRX welcomes negotiated changes for enterprise agreements. Email privacy@contentrx.io with subject [DPA-COUNTERSIGN] for a counter-signed copy or to propose redlines.

1. Definitions

Capitalised terms used and not otherwise defined in this Addendum have the meanings given in the Agreement (the ContentRX Terms of Service at contentrx.io/terms). The following terms have the meanings below for purposes of this Addendum.

Addendum means this Data Processing Addendum, including the Exhibits.

Agreement means the ContentRX Terms of Service and any order form, statement of work, or other commercial document referencing this Addendum.

Customer means the ContentRX customer that has entered into the Agreement.

Customer Strings means the text content Customer submits to the Service for review, as described in the Agreement. Customer Strings may incidentally contain Personal Data.

Data Protection Laws means all applicable laws governing the processing of Personal Data, including the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), the Personal Information Protection and Electronic Documents Act (PIPEDA), and equivalent state privacy laws in effect from time to time. The EU General Data Protection Regulation (GDPR) and UK Data Protection Act 2018 apply only when ContentRX has opened access in those regions and appointed an Article 27 representative.

Personal Data means any information relating to an identified or identifiable natural person that ContentRX processes on behalf of Customer under the Agreement.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored, or otherwise processed.

Process means any operation performed on Personal Data, including collection, recording, organisation, storage, retrieval, use, disclosure, and erasure.

Service means the ContentRX content design review service as described in the Agreement, accessible through the web dashboard at contentrx.io and through the published API surfaces.

Subprocessor means any third party that ContentRX engages to Process Personal Data in connection with delivery of the Service. The current list of Subprocessors is published at contentrx.io/privacy.

2. Scope and Roles

This Addendum applies whenever ContentRX Processes Personal Data on behalf of Customer in connection with the Agreement. With respect to such Personal Data, Customer acts as the data controller (or business under CCPA) and ContentRX acts as the data processor (or service provider under CCPA). For Personal Data that ContentRX Processes for its own purposes (account administration, billing, fraud prevention, security, and improvement of the Service), ContentRX acts as the controller or business and the ContentRX Privacy Policy at contentrx.io/privacy governs.

3. Compliance with Data Protection Laws

Each party will comply with Data Protection Laws applicable to its Processing of Personal Data under the Agreement. Customer is responsible for ensuring that its instructions to ContentRX, and the Personal Data Customer submits to the Service, comply with Data Protection Laws and with the rights of the individuals whose Personal Data is included.

4. Customer's Instructions

ContentRX will Process Personal Data only in accordance with the Agreement, this Addendum, and Customer's documented instructions. Customer's instructions include the configuration choices Customer makes through the dashboard, the API calls Customer makes through published endpoints, and the Flag-for-Review consent flow described in Section 4 of the Agreement.

If ContentRX believes that an instruction from Customer violates applicable Data Protection Laws, ContentRX will inform Customer promptly and may pause Processing of the affected Personal Data until the conflict is resolved.

5. Confidentiality

ContentRX will treat Personal Data as Customer's Confidential Information under the Agreement. ContentRX will ensure that personnel authorised to Process Personal Data are bound by confidentiality obligations (whether contractual or statutory) and have received training on the secure handling of Personal Data.

6. Security

ContentRX will implement and maintain appropriate technical and organisational measures designed to protect Personal Data against Personal Data Breaches and against unauthorised or unlawful Processing. The measures in effect as of the Effective Date are described in Exhibit C. ContentRX may update these measures over time provided that the level of security is not materially decreased.

7. Subprocessors

Customer authorises ContentRX to engage the Subprocessors listed at contentrx.io/privacy. ContentRX will: (a) impose data protection obligations on each Subprocessor that are no less protective than those in this Addendum, and (b) give Customer at least thirty (30) days notice before adding or replacing a Subprocessor that materially changes the categories of Personal Data shared with third parties.

If Customer reasonably objects to a new Subprocessor on data protection grounds, Customer may terminate the Agreement under Section 6 of the Agreement (Refunds and cancellation) without penalty, with a prorated refund of any prepaid annual Subscription fee covering the unused portion of the Term.

8. Data Subject Rights

ContentRX provides Customer with the tools described in the ContentRX Privacy Policy at contentrx.io/privacy that allow Customer to respond to requests from individuals to exercise rights under Data Protection Laws (access, rectification, erasure, restriction, portability, objection, and withdrawal of consent). If ContentRX receives a request directly from a Customer end user regarding Personal Data ContentRX Processes on behalf of Customer, ContentRX will redirect the request to Customer and provide reasonable cooperation as needed to enable Customer to respond.

9. Personal Data Breach

ContentRX will notify Customer of any Personal Data Breach affecting Customer's Personal Data without undue delay, and in any event within seventy-two (72) hours of becoming aware of the breach. The notification will include the information required by Article 33(3) of the GDPR (when applicable) and by PIPEDA's breach reporting framework (for Canadian Personal Data). ContentRX will cooperate with Customer's investigation and remediation efforts.

10. Cross-Border Transfers

ContentRX Processes Personal Data on infrastructure located in the United States. As of the Effective Date, ContentRX does not offer the Service to data subjects located in the European Union, the European Economic Area, or the United Kingdom (see contentrx.io/privacy under "Regional availability"). When ContentRX opens access to those regions, the Standard Contractual Clauses adopted by the European Commission (Module Two, controller-to-processor) will apply by reference and will be incorporated as Exhibit D to this Addendum without further action by the parties.

For Personal Data of Canadian residents (outside Quebec), ContentRX complies with PIPEDA's cross-border transfer requirements by imposing contractual safeguards on Subprocessors equivalent to those required by PIPEDA Principle 4.1.3.

11. Deletion and Return of Personal Data

Upon termination or expiration of the Agreement, ContentRX will delete Personal Data Processed on behalf of Customer within thirty (30) days, except to the extent retention is required by applicable law (in which case ContentRX will preserve confidentiality and isolate the data from active Processing). Customer may request earlier deletion of specific Personal Data at any time through the in-product flows described at contentrx.io/privacy or by emailing privacy@contentrx.io.

12. Audits

On reasonable written request, and no more than once per twelve (12) month period absent a Personal Data Breach, ContentRX will make available to Customer information reasonably necessary to demonstrate ContentRX's compliance with this Addendum. ContentRX may satisfy this obligation through summary reports, the published security disclosures at contentrx.io/security, or third-party audit reports as they become available. On-site audits require thirty (30) days advance notice and are conducted at Customer's expense.

13. Liability

Each party's liability arising out of or in connection with this Addendum is subject to the limitations and exclusions in Section 7 of the Agreement (Warranty disclaimer and liability cap). For clarity, Personal Data Breach claims, regulatory fines, and indemnification obligations under Data Protection Laws are subject to the same overall

liability cap as other claims under the Agreement, except where Data Protection Laws prohibit such limitation.

14. Term and Termination

This Addendum takes effect on the Effective Date and continues for the term of the Agreement. Sections that by their nature should survive termination (including Sections 5, 9, 11, 12, 13, and 15) survive termination of the Addendum and the Agreement.

15. Governing Law

This Addendum is governed by the same law and venue as the Agreement (California law, Sacramento County). Nothing in this Section limits any rights individuals or regulators have under applicable Data Protection Laws.

16. Order of Precedence

In the event of a conflict between this Addendum and the Agreement with respect to the Processing of Personal Data, this Addendum controls. In the event of a conflict between this Addendum and any executed Standard Contractual Clauses, the Standard Contractual Clauses control.

EXHIBIT A

Description of Processing

Subject matter.

Delivery of the ContentRX content design review Service to Customer.

Duration.

The term of the Agreement, plus the deletion window described in Section 11 of this Addendum.

Nature and purpose of Processing.

Receipt of Customer Strings through ContentRX endpoints, forwarding of the strings to the evaluation engine for review, return of Service Output to Customer, retention of hashed and metadata records for billing and dashboard history, optional calibration use of Customer Strings affirmatively flagged through the Flag-for-Review consent flow.

Categories of Personal Data.

(a) Account data submitted by Customer (name, email, billing information). (b) Personal Data incidentally contained in Customer Strings submitted to the Service (placeholder names, example email addresses, sample personal identifiers in microcopy under review). ContentRX does not collect Sensitive Personal Information as defined by CPRA.

Categories of data subjects.

(a) Customer's authorised users of the Service. (b) Natural persons whose Personal Data Customer chooses to include in Customer Strings.

Special categories of data.

None expected. Customer represents in Section 2 of the Agreement that strings submitted to the Service do not include personal data of any individual without that individual's consent.

EXHIBIT B

Subprocessor List

The current list of Subprocessors engaged by ContentRX is published and maintained at contentrx.io/privacy under "Who else sees it (subprocessors)". The list as of the Effective Date includes the parties named in the table below. ContentRX updates the published list within thirty (30) days of any change and notifies Customer at least thirty (30) days in advance of material additions.

Subprocessor	Purpose	Data accessed
Anthropic, PBC	LLM evaluation	Customer Strings for the duration of the evaluation call.
Stripe, Inc.	Payments	Customer billing email, card details, subscription history.
Clerk Inc.	Authentication	Account email, hashed password, session tokens.
Supabase, Inc.	Database hosting	Account metadata, hashed Customer Strings, verdicts, usage.
Vercel Inc.	Application hosting	HTTP requests in transit.
Resend.com Inc.	Transactional email	Recipient email address and message body.
Functional Software, Inc. dba Sentry	Error tracking	Stack traces and scrubbed request metadata.
Plausible Insights OU	Analytics	Anonymous page-view counts. No cookies.
Upstash, Inc.	Rate limiting	Short-lived counters keyed by user id.
Figma, Inc.	Plugin distribution	Plugin install metadata under Figma's own policy.

EXHIBIT C

Technical and Organisational Measures

ContentRX maintains the technical and organisational measures described below. The published security disclosures at contentrx.io/security are the operating record and supersede this Exhibit if the two disagree.

Access control. Production access is limited to authorised personnel. Multi-factor authentication is required for all admin consoles (Vercel, Stripe, Clerk, Supabase, Anthropic). Account credentials are not shared.

Encryption in transit. All traffic between Customer browsers, ContentRX endpoints, and Subprocessors uses TLS 1.2 or higher.

Encryption at rest. Supabase Postgres encrypts data at rest. Stripe stores payment details under PCI-DSS Level 1 controls. Sentry encrypts stored events.

Pre-screening of inbound text. Every public endpoint that accepts a Customer String runs a regex pre-screen rejecting obvious credentials and PII patterns (credit card numbers, US Social Security Numbers, AWS / Stripe / OpenAI / Anthropic / GitHub API keys) before forwarding the string to the evaluation engine.

Error redaction. Sentry events have request bodies, authorisation headers, cookies, and query strings stripped before send. Exception messages are truncated to two hundred (200) characters.

Logging hygiene. User-facing routes use a structured logger that hand-shapes the payload to {kind, message, status?} so error objects do not serialise transitive properties.

Rate limiting. Sixty (60) requests per minute per authenticated user, enforced by Upstash Redis with a sliding-window counter.

Backups. Supabase performs daily encrypted backups with seven (7) days of point-in-time recovery.

Personnel training. All ContentRX personnel with access to production systems complete annual data-handling and security training.

Vendor management. Each Subprocessor is bound by a written data processing agreement or equivalent terms with data protection obligations no less protective than this Addendum.

EXHIBIT D

Standard Contractual Clauses

Not applicable as of the Effective Date.

ContentRX does not offer the Service to data subjects located in the European Union, the European Economic Area, or the United Kingdom. When ContentRX opens access to those regions, the European Commission Standard Contractual Clauses (Module Two, controller-to-processor, dated 4 June 2021) and the UK Information Commissioner's Office International Data Transfer Addendum will be incorporated into this Exhibit D by reference. Customer's signature on this Addendum constitutes Customer's signature on the Standard Contractual Clauses to take effect on the date ContentRX opens access to the relevant region.

SIGNATURES

Acceptance of the Addendum

Customer accepts this Addendum by checking the corresponding box in the ContentRX dashboard, by signing and returning a counter-signed copy of this document, or by using the Service after the Effective Date with knowledge of this Addendum.

CONTENTRX LLC	**CUSTOMER**
Signature: _____	Signature: _____
Printed name: _____	Printed name: _____
Title: _____	Title: _____
Date: _____	Date: _____

ContentRX LLC
2520 Venture Oaks Way, Suite 120
Sacramento, CA 95833
United States
privacy@contentrx.io