DATA PROCESSING AGREEMENT

California Consumer Privacy Act / California Privacy Rights Act and Applicable US State Privacy Laws

Cambridge Holdings, LLC (trading as SafeRedact)

1. Parties and Scope

This Data Processing Addendum ("DPA") is entered into between the Business (as identified in the Order Form) and Cambridge Holdings, LLC, trading as SafeRedact, with principal offices at Bensenville, Illinois, United States ("Service Provider"). This DPA applies to processing governed by the CCPA/CPRA and, to the extent applicable, the Virginia CDPA, Colorado CPA, Connecticut CTDPA, Utah UCPA, and other US state privacy laws.

2. Definitions

"CCPA" means the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100–1798.199) as amended by the CPRA. "Personal Information", "Business", "Service Provider", "Consumer", "Sell", "Share", and "Business Purpose" have the meanings given in the CCPA.

"Security Incident" means any 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 by the Processor. A Security Incident does not include unsuccessful attempts or activities that do not compromise the security of Personal Data, such as failed login attempts, pings, port scans, denial of service attacks, or similar incidents.

3. Service Provider Obligations

3.1 SafeRedact shall not sell or share Personal Information.

3.2 SafeRedact shall not retain, use, or disclose Personal Information for any purpose other than the Business Purpose of providing AI-assisted document redaction services, or as otherwise permitted by the CCPA.

3.3 SafeRedact shall not combine Personal Information received from the Business with Personal Information from other sources except as permitted by the CCPA.

3.4 SafeRedact shall comply with applicable CCPA obligations and provide the same level of privacy protection as required by the CCPA.

3.5 SafeRedact shall notify the Business if it determines it can no longer meet its CCPA obligations.

3.6 The Business has the right to take reasonable steps to ensure SafeRedact uses Personal Information consistent with the Business's CCPA obligations.

3.7 SafeRedact shall notify the Business of any Consumer rights requests (access, deletion, correction, opt-out) and assist in responding.

4. Technical Architecture

Zero-storage architecture. Documents processed in browser. Only extracted text transmitted for AI classification. No Personal Information stored at rest. Processing location: United States (AWS US-East-1).

5. Customer Data

The Controller retains all rights, title, and interest in and to all Customer Data, including all Personal Data. Nothing in this DPA transfers any ownership rights in Customer Data to the Processor.

The Processor shall not use Customer Data, Personal Data, or any text extracted from documents submitted to the service to train, fine-tune, improve, or evaluate machine learning or artificial intelligence models. The Processor has obtained equivalent contractual commitments from all sub-processors, including Anthropic, PBC.

6. Sub-contractors

Sub-processor	Purpose	Location	Certifications	Retention
Anthropic, PBC	AI text classification	United States (AWS US)	SOC 2 Type II	Zero retention
Vercel Inc.	Application hosting, serverless API	United States (AWS US-East)	SOC 2 Type II	No data stored
Supabase Inc.	User authentication only	United States (AWS US-East)	SOC 2 Type II	Auth tokens only

Each sub-contractor is bound by contractual obligations consistent with this DPA, including zero-retention commitments. Terms available on request.

7. Security

Technical and Organisational Measures:

Encryption in transit: All data transmitted between the Controller's browser and the Processor's API is encrypted using TLS 1.2 or higher.

Zero retention: No Personal Data is stored at rest on any Processor system. Text is processed in memory and discarded upon completion of each API request.

No document storage: Documents are processed entirely within the Controller's browser and are never transmitted to or stored on Processor servers.

Access controls: System access is restricted to authorised personnel using multi-factor authentication. Administrative access is logged.

Infrastructure: Application hosting and API infrastructure are provided by SOC 2 Type II certified partners (Vercel, Supabase).

AI processing: Text classification is performed by Anthropic's Claude API under contractual zero-retention terms (Anthropic SOC 2 Type II certified).

Penetration testing: The Processor conducts or commissions annual penetration testing of its application and API infrastructure.

Incident response: The Processor maintains documented incident response procedures, tested at least annually.

8. Security Incident

SafeRedact shall notify the Business without unreasonable delay, and within 48 hours, of any Security Incident.

If the Processor receives a request from a law enforcement authority or government body for disclosure of Personal Data processed on behalf of the Controller, the Processor shall (a) redirect the requesting authority to the Controller, (b) promptly notify the Controller of the request unless legally prohibited from doing so, and (c) not disclose the Personal Data unless compelled by applicable law.

9. Confidentiality

The Processor shall ensure that all personnel authorised to process Personal Data are bound by appropriate confidentiality obligations, whether contractual or statutory. Access to systems capable of processing Personal Data is restricted to personnel who require such access for the performance of the services.

10. Audit

The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA. The Controller may conduct or commission an audit of the Processor's compliance, subject to the following conditions:

(a) Audits may be conducted no more than once per twelve-month period, unless required by a Supervisory Authority or following a confirmed Personal Data breach.

(b) The Controller shall provide at least 30 days' written notice of any audit.

(c) Audits shall be conducted during normal business hours and shall not unreasonably interfere with the Processor's operations.

(d) The Controller shall bear the costs of any audit.

(e) Audits shall not require access to source code, trade secrets, security architecture details beyond what is documented, or systems of other customers. The Processor may satisfy audit requests by providing relevant SOC 2 reports, penetration test summaries, or other third-party audit documentation.

11. Redaction Accuracy

The Processor provides automated tools for the detection and redaction of personal data. The Controller is solely responsible for reviewing, approving, and where necessary correcting all detections before exporting redacted documents. The Processor makes no warranty as to the completeness or accuracy of automated detection. The review step within the service is designed to enable the Controller to exercise this responsibility.

12. Liability

The Processor's aggregate liability under this DPA shall not exceed the fees paid by the Controller to the Processor in the twelve (12) months preceding the event giving rise to the claim. This limitation shall not apply to liability arising from the Processor's wilful misconduct or gross negligence.

The Processor shall not be liable for any indirect, incidental, special, consequential, or punitive damages arising under this DPA.

13. HIPAA

SafeRedact's zero-retention architecture minimises PHI exposure by design. Documents never leave the browser and extracted text is processed with no-log headers.

14. Term

Effective for the duration of the service agreement.

15. Governing Law

This DPA shall be governed by the law governing the underlying service agreement between the parties. In the absence of a governing law provision in the service agreement, this DPA shall be governed by the laws specified below.

Fallback: the laws of the State of Delaware.

16. Signatures

For and on behalf of the Business:

Signature: _____

Name: _____

Title: _____

Date: _____

For and on behalf of the Service Provider (SafeRedact / Cambridge Holdings, LLC):

Signature: _____

Name: _____

Title: _____

Date: _____