DATA PROCESSING AGREEMENT

General Data Protection Regulation (EU) 2016/679

Cambridge Holdings, LLC (trading as SafeRedact)

1. Parties and Scope

This Data Processing Agreement ("DPA") is entered into between the Controller and Cambridge Holdings, LLC, trading as SafeRedact, with registered address at Bensenville, Illinois, United States ("Processor"). This DPA supplements the service agreement and complies with Article 28 GDPR.

2. Definitions

"GDPR" means Regulation (EU) 2016/679. "Standard Contractual Clauses" or "SCCs" means the clauses adopted by European Commission Decision 2021/914. All other capitalised terms have the meanings given in the GDPR.

"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. Purpose of Processing

The Processor processes Personal Data solely for AI-assisted document redaction for DSAR and regulatory compliance, as described in Schedule 1.

4. Technical Architecture

The Processor operates a stateless, zero-storage architecture. Documents are processed in the Controller's browser. Only extracted text is transmitted for AI classification. Text is processed in memory and discarded immediately. No Personal Data is stored at rest. Processing locations: Vercel (AWS US-East-1), Anthropic (AWS US), Supabase (AWS US-East-1).

5. Obligations of the Processor

5.1 Process Personal Data only on documented instructions from the Controller.

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.

5.2 Implement technical and organisational measures per Article 32 GDPR (Schedule 2).

5.3 Sub-processor engagement subject to Section 7.

5.4 Assist with Data Subject rights (Articles 15–22 GDPR).

5.5 Assist with DPIA and prior consultation (Articles 35–36 GDPR).

5.6 Delete or return Personal Data upon termination (no data persists under zero-retention architecture).

6. 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.

7. Sub-processors

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

30 days' notice for sub-processor changes. Controller may object within 14 days. Sub-processor agreements with zero-retention commitments available on request.

8. International Transfers

Where Personal Data is transferred outside the EEA to a country without an adequacy decision, the parties incorporate the Standard Contractual Clauses (Module Two: Controller to Processor) adopted by Commission Decision 2021/914. The SCCs form an integral part of this DPA. Completed annexes reflect Schedule 1. Given zero-retention, transfer risk is structurally minimised.

9. Security Incident Notification

Notification within 48 hours. Details as required by Article 33(3) GDPR.

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.

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. Term

Effective for the duration of the service agreement.

14. 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 Member State in which the Controller is established.

15. Signatures

For and on behalf of the Controller:

Signature: _____

Name: _____

Title: _____

Date: _____

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

Signature: _____

Name: _____

Title: _____

Date: _____

Schedule 1: Processing Details

Subject matter:

AI-assisted PII detection and document redaction for DSAR and regulatory compliance.

Duration:

Transient per API request. No persistent storage.

Types of personal data:

Names, emails, phones, national ID numbers, dates of birth, addresses, bank details, employee identifiers, salary data.

Categories of data subjects:

Employees, former employees, contractors, clients, and other individuals in processed documents.

Schedule 2: Technical and Organisational Measures

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.

Annex: Standard Contractual Clauses

The Standard Contractual Clauses (Module Two: Controller to Processor) adopted by European Commission Implementing Decision (EU) 2021/914 are incorporated by reference. The completed annexes reflect Schedule 1 and Schedule 2 above.