DATA PROCESSING AGREEMENT

UK General Data Protection Regulation

Cambridge Holdings, LLC (trading as SafeRedact)

1. Parties and Scope

This Data Processing Agreement ("DPA") is entered into between the Controller (as identified in the Order Form or service agreement) and Cambridge Holdings, LLC, trading as SafeRedact, with registered address at Bensenville, Illinois, United States ("Processor"). This DPA supplements the service agreement between the parties.

2. Definitions

"UK GDPR" means the General Data Protection Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended. "Data Protection Laws" means the UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations 2003. All other capitalised terms have the meanings given in the UK 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 the purpose of providing AI-assisted document redaction for DSAR compliance and regulatory purposes, as described in Schedule 1.

4. Technical Architecture

The Processor operates a stateless, zero-storage architecture:

Documents are processed entirely within the Controller's web browser and are never transmitted to Processor servers.

Only extracted text content is transmitted to the Processor's API for AI-based classification.

Text is processed in memory and discarded immediately upon completion of each API request.

No Personal Data is stored at rest on any Processor system.

Processing locations: API hosted on Vercel (AWS US-East-1). AI classification via Anthropic (AWS US). Authentication via Supabase (AWS US-East-1).

5. Obligations of the Processor

5.1 Process Personal Data only on documented instructions from the Controller, unless required by applicable law.

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 appropriate technical and organisational measures as set out in Schedule 2.

5.3 Not engage another sub-processor without prior written authorisation from the Controller. Current sub-processors are listed in Section 7.

5.4 Assist the Controller in responding to Data Subject rights requests under Chapter III of the UK GDPR.

5.5 Assist the Controller with obligations under Articles 32–36 of the UK GDPR.

5.6 At the Controller's choice, delete or return all Personal Data upon termination. Given the zero-retention architecture, no Personal Data persists after each API request.

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

The Processor shall notify the Controller at least 30 days before engaging a new sub-processor or replacing an existing one. The Controller may object within 14 days. The Processor has entered into data processing agreements with each sub-processor that include zero-retention commitments. Copies of relevant sub-processor terms are available upon request.

8. International Transfers

Where Personal Data is transferred from the United Kingdom to a country without an adequacy decision, the Processor shall ensure appropriate safeguards under Article 46 of the UK GDPR. The Processor maintains the International Data Transfer Agreement (IDTA) as issued by the ICO where required. Given the zero-retention architecture, transfers are transient with no data stored at rest outside the United Kingdom.

9. Security Incident Notification

The Processor shall notify the Controller without undue delay, and within 48 hours, of any Security Incident. Notification shall include: the nature of the incident; categories and approximate number of data subjects affected; likely consequences; and measures taken or proposed.

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 and Termination

This DPA remains in effect for the duration of the service agreement. Provisions relating to Personal Data processing survive termination for as long as the Processor processes Personal Data on behalf of the Controller.

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 England and Wales. The parties submit to the exclusive jurisdiction of the courts of England and Wales.

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 identification and redaction of personal data in documents for DSAR compliance.

Duration:

Transient per API request. No persistent storage.

Nature:

Automated classification of text to identify names, emails, phone numbers, national insurance numbers, dates of birth, addresses, bank details, salary data, and other identifiers.

Types of personal data:

Names, email addresses, phone numbers, national insurance numbers, dates of birth, home addresses, postcodes, bank account details, sort codes, employee identifiers, salary information, passport numbers, and any other personal data present in documents processed by the Controller.

Categories of data subjects:

Employees, former employees, contractors, clients, customers, and other individuals whose personal data appears in documents processed by the Controller.

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.