PROJECT DATA PROCESSING AGREEMENT

UK General Data Protection Regulation — Single DSAR Engagement

Cambridge Holdings, LLC (trading as SafeRedact)

Template. Executed versions contain project-specific terms.

PROJECT DETAILS

Project Reference	
Controller	
Controller Contact	
Data Subject Name	
Estimated Items	
Project Fee	
Completion Deadline	
Effective Date	

1. PARTIES

This Project Data Processing Agreement ("DPA") is entered into between:

The Controller: The entity identified in the Project Details table above.

The Processor: Cambridge Holdings, LLC, trading as SafeRedact, with registered address at Bensenville, Illinois, United States.

This DPA governs the processing of Personal Data for the specific project identified above and no other purpose.

2. DEFINITIONS

"UK GDPR" means the General Data Protection Regulation as retained in UK law. "Data Protection Laws" means the UK GDPR and the Data Protection Act 2018. All 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. Unsuccessful attempts (failed logins, port scans, denial of service) are excluded.

"Project" means the single Data Subject Access Request identified in the Project Details, including all documents processed and redacted in connection with that request.

3. SCOPE AND PURPOSE

The Processor shall process Personal Data solely for the purpose of providing AI-assisted document redaction for the DSAR identified in the Project Details. Processing is limited to:

Receiving extracted text from documents uploaded by the Controller via the SafeRedact web application;

Analysing extracted text using AI to identify personal data for redaction;

Returning detection results to the Controller's browser for review and approval.

Processing shall not extend beyond the scope of the identified Project. No Personal Data shall be used for any other purpose.

4. TECHNICAL ARCHITECTURE

The Processor operates a stateless, zero-storage architecture:

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

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

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

Retention: The Processor does not store document content or extracted text at rest. Extracted text is retained by the AI sub-processor for no longer than 30 days for abuse monitoring and is never used to train models. Account, authentication, billing and audit records, and any saved data-subject reference records, are deleted within 30 days of termination or on written request.

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

No per-job, per-file, or per-detection records are retained by the Processor. Audit trails, per-decision logs, and processing summaries are generated client-side in the Controller’s browser and bundled into the deliverable ZIP that the Controller downloads. The Processor retains only the Controller’s account record (email, billing) and a minimal usage indicator consisting of one record per Authorised User per calendar day on which the User accessed the service. The Processor does not retain Data Subject identifiers, document contents, detection counts, geographic data, or any record of which specific redaction jobs the Controller processed. Because the Processor holds no copy of the Controller’s audit records, the Processor cannot reproduce them on the Controller’s behalf or in response to legal process; the Controller is the sole holder of its compliance evidence.

5. OBLIGATIONS OF THE PROCESSOR

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

5.2 Ensure all personnel with access to systems are bound by confidentiality obligations. Access restricted to personnel necessary for service delivery.

5.3 Implement technical and organisational measures as described in Schedule 1.

5.4 Not engage additional sub-processors beyond those listed in Section 7 without the Controller's prior written consent.

5.5 Assist the Controller in responding to the Data Subject's rights request that is the subject of this Project.

5.6 Upon Project completion, the Processor shall confirm in writing that no document content or extracted text has been retained. Account, authentication, billing and audit records, and any saved data-subject reference records, shall be deleted within 30 days of Project completion or on written request.

6. CUSTOMER DATA AND AI

The Controller retains all rights, title, and interest in Customer Data. Nothing in this DPA transfers ownership.

The Processor shall not use Customer Data, Personal Data, or extracted text to train, fine-tune, improve, or evaluate AI models. Equivalent commitments have been obtained from all sub-processors including Anthropic, PBC.

7. SUB-PROCESSORS

Sub-processor	Purpose	Location	Certifications	Retention
Anthropic, PBC	AI text classification	US (AWS)	SOC 2 Type II	No model training; deleted within 30 days
Vercel Inc.	Application hosting	US (AWS)	SOC 2 Type II	No data stored
Supabase Inc.	User authentication	US (AWS)	SOC 2 Type II	Auth tokens only

The Processor shall give the Controller at least 30 days' notice before engaging or replacing a sub-processor; the Controller may object within 14 days. Each sub-processor is engaged under a written data processing agreement incorporating the Standard Contractual Clauses where applicable. The current sub-processor list, with roles and processing locations, is published at saferedact.app/enterprise/legal/subprocessors.

8. INTERNATIONAL TRANSFERS

Where Personal Data is transferred from the United Kingdom to the United States, the Processor maintains the International Data Transfer Agreement (IDTA) as issued by the ICO, together with the sub-processor agreements referenced above. Document content is never transferred. Extracted text is transferred transiently for classification and is retained by the AI sub-processor for no longer than 30 days.

9. SECURITY INCIDENT NOTIFICATION

The Processor shall notify the Controller within 48 hours of becoming aware of any Security Incident, including: nature of the incident; approximate data subjects affected; likely consequences; measures taken.

If the Processor receives a law enforcement or government request for Personal Data, it shall redirect the authority to the Controller and notify the Controller promptly unless legally prohibited.

10. AUDIT

The Processor shall make available information necessary to demonstrate compliance. The Controller may conduct one audit during the Project term, with 14 days' written notice, at the Controller's cost. Audits shall not require access to source code or trade secrets. The Processor may satisfy requests by providing SOC 2 reports or penetration test summaries.

11. REDACTION ACCURACY

The Processor provides automated detection tools. The Controller is solely responsible for reviewing, approving, and correcting all detections before export. The Processor makes no warranty as to completeness or accuracy of automated detection. The review step within the service exists specifically to enable the Controller to exercise this responsibility.

12. LIABILITY

Each party's aggregate liability under this DPA shall not exceed £[●]. This limitation does not apply to wilful misconduct or gross negligence, or to any liability that cannot be limited or excluded under applicable law.

The Processor shall not be liable for indirect, incidental, special, consequential, or punitive damages.

13. TERM AND TERMINATION

This DPA is effective from the Effective Date in the Project Details and terminates upon the earlier of: (a) delivery of the redacted document package to the Controller; (b) the Completion Deadline; or (c) written termination by either party with 7 days' notice.

Upon termination, the Processor shall confirm that no Personal Data has been retained. Sections 6, 11, and 12 survive termination.

14. GOVERNING LAW

This DPA shall be governed by and construed in accordance with 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: TECHNICAL AND ORGANISATIONAL MEASURES

Encryption in transit: TLS 1.2 or higher for all data transmitted between Controller's browser and Processor's API.

Retention: No Personal Data stored at rest. Text processed in memory and discarded per API request.

No document storage: Documents processed in Controller's browser. Never transmitted to Processor servers.

Access controls: Multi-factor authentication for system access. Administrative access logged.

Infrastructure: SOC 2 Type II certified hosting (Vercel) and authentication (Supabase).

AI processing: Text classification is performed by Anthropic PBC (Claude API) acting as a sub-processor under Anthropic's Commercial Terms and Data Processing Addendum, which incorporate the Standard Contractual Clauses. Anthropic does not train models on customer content. Inputs and outputs are deleted within 30 days. Anthropic maintains ISO 27001:2022, ISO 42001 and SOC 2 Type II certification.

Penetration testing: Annual penetration testing of application and API infrastructure.

Incident response: Documented procedures, tested annually.