Redactly — security and data handling summary

For data protection officers and IT security reviewers · updated 24 November 2026 · current version: redactly.co.uk/security

What Redactly does

Redactly helps UK public bodies redact personal data from documents before disclosure (FOI, EIR, subject access). It suggests redactions using text recognition, pattern rules and an AI model; a person in the customer organisation reviews every suggestion and approves the final redacted PDF.

Where data is stored and processed

Uploaded documents, outputs, database, audit log	Supabase on AWS eu-west-2 (London, UK)
Text recognition (OCR)	Google Cloud Document AI, europe-west2 (London, UK)
AI redaction suggestions	Gemini on Google Cloud Vertex AI, EU multi-region
Application servers	Vercel serverless functions, London (lhr1)
Transactional email	Resend, EU (Ireland) — user names and email addresses only
Payments	Stripe — billing details only, never document content

Document content is not sent outside the UK or EU. Google does not use customer data to train its models under Google Cloud's terms; Redactly never trains AI on customer documents.

Data flow

1. The browser uploads the file directly to encrypted storage in London.
2. The application counts pages and checks the organisation's allowance before any processing.
3. Document AI (London) extracts text, word positions and page images.
4. Gemini (EU) and pattern rules suggest personal data to redact, page by page.
5. A user reviews every suggestion, adds anything missed, and finalises.
6. The redacted PDF is rebuilt from page images with redactions burned in (no hidden text layer); metadata is stripped; intermediate page images are deleted.

Security controls

Encryption	TLS 1.2+ in transit; AES-256 at rest (infrastructure-provided)
Tenant isolation	Postgres row-level security on every table holding customer data
Access	Roles: Admin, Reviewer, Viewer. Users join an organisation only by an admin's time-limited invitation. No shared accounts.
Audit trail	Append-only log of uploads, analysis, every accept/reject/manual redaction, finalisation and user management. Metadata only.
Application security	Upload content-signature validation, size limits, database-backed rate limiting, Content Security Policy and security headers (SSL Labs A+)
Testing	Automated OWASP ZAP scan, March 2026: no high-severity findings

Retention

Unredacted original	Auto-deleted after the period set by the customer's admin (default 3 years after finalisation)
Redacted output and record	Auto-deleted after the period set by the customer's admin (default 6 years after finalisation)
Intermediate page images	Deleted at finalisation
On termination or request	Export offered, then deletion within 30 days, confirmed in writing

Incidents and contacts

Personal data breaches are notified to the customer within 48 hours of discovery (DPA clause 8). Security: security@redactly.co.uk · Data protection and DPA: legal@redactly.co.uk · DPA template: redactly.co.uk/dpa

What we do not yet have. No Cyber Essentials, Cyber Essentials Plus or ISO 27001 certification. No independent (CREST/CHECK) penetration test. No G-Cloud listing or NHS DSPT submission. Database backups are not yet enabled. ICO registration is pending. Redactly is operated by a sole trader.

This summary describes the service as at 24 November 2026. It is provided for assessment purposes and does not form part of any contract; the Data Processing Agreement governs processing.