KeptPDF Security & Privacy Overview

Version 1.0 · Updated June 2026 · keptpdf.com/security

Summary

KeptPDF runs entirely in your browser. Every tool, from redaction to editing to signing to conversion, processes your file on your own device using WebAssembly and JavaScript. Your document and its contents are never transmitted to KeptPDF and never stored on our servers. There is no upload step to intercept, no copy on our side to breach, log, or subpoena. You can confirm this yourself in about a minute, with no special tools.

How your file is handled

Your file is opened locally in your browser. The processing happens on your device. The finished file is saved by you, to your device. The only things that ever reach our servers are the name of the tool you opened, with a usage count to enforce the free daily limit, and your account and payment details if you choose to create an account. Never your file, its name, or its contents.

Never leaves your device

- Your file's contents
- Its name and size
- The text and images on the page
- Any fingerprint or hash of your file
- The redacted data itself

What we receive, over HTTPS

- Which tool you opened, with a daily usage count
- Your account and sign-in, if you create one
- Payment, handled by Stripe, so we never see your card
- A file you choose to import from Google Drive, where Google's terms apply

No third-party analytics, no advertising pixels, no cross-site trackers.

Subprocessors

These support the account, billing, and hosting layer. None receive your document content.

Subprocessor	What it does	Receives document content
Vercel	Hosts the site and serves the static app code	Never
Stripe	Processes payments. We never see your card either	Never
Resend	Sends account and receipt emails	Never
Neon	Stores accounts, billing, and anonymous usage counts	Never

Data retention

Document content is never collected, so there is nothing to retain or delete on our side. Account details are kept while your account is open and removed on request. Payment records are kept for as long as the law requires. Usage counts are anonymous and sanitized.

Compliance posture

GDPR

No document personal data is transmitted to or processed by KeptPDF, so KeptPDF is not a processor of the personal data inside your files. Account and billing data is processed under our Privacy Policy.

HIPAA

Protected health information never reaches our servers, because the file is processed on your device. There is no third-party processor touching PHI and no server-side breach surface for PHI. Whether a Business Associate Agreement is required is a determination for your counsel. If your policy calls for one, our HIPAA page provides a BAA template based on HHS sample provisions to review and adapt with your own counsel. We describe the architecture and assert no legal conclusion.

FRCP 5.2 and redaction

Redaction flattens each page to an image, so the underlying text is removed from the file, not hidden behind a box that can be copied out or peeled off. Each redaction produces a SHA-256 certificate recording what was scanned and the fingerprint of the finished file.

Certifications

KeptPDF does not currently hold SOC 2 or ISO 27001 certification. The architecture removes the risk those audits exist to manage: there is no server-side store of your documents to secure, because your documents never reach a server. Where a control normally protects data at rest on a vendor's systems, here the data is never at rest on our systems.

You do not have to take our word for it

- **Airplane Mode.** Load the page, turn off wifi, and run any tool. It still works, because the work was never happening on a server.
- **The Network tab.** Open DevTools and watch the requests while you process a file. Your document is never part of a single request. You will see small first-party calls for the daily quota and analytics, never your file.
- **Read the source.** The code that does the work is already in your browser. Inspect it line by line.
- **Verify a redaction.** Check any redacted file against its SHA-256 certificate at keptpdf.com/verify. That check also runs in the browser, so the document is never uploaded to confirm it.

Vendor security questionnaire

The questions a procurement or security review usually asks, answered.

Where is our data hosted, and who processes it?

Your documents are not hosted anywhere. They stay on the device of the person using KeptPDF. The site itself and the account and billing layer are hosted on Vercel. Subprocessors are listed above.

Is data encrypted in transit and at rest?

In transit: every first-party call, for sign-in, payment, and usage counts, uses HTTPS and TLS. Your document is never transmitted, so it is never in transit to us at all. At rest: your document is never at rest on our servers, because we never receive it. Account, billing, and usage data are stored by Neon and Stripe, which encrypt data at rest.

Do you store our documents? What is your retention and deletion policy?

No. We never receive the document, so there is nothing to store, back up, or delete on our side. Account data is kept while your account is open and removed on request. Payment records are kept as required by law.

Who at KeptPDF can access our documents?

No one. There is no copy on our systems for an employee, a contractor, a subpoena, or a breach to reach.

What is our data breach exposure?

Your documents have no server-side breach surface, because they never leave your device. A breach of our systems could expose account and billing data, such as an email and subscription status, the same data any service holds for sign-in and payment. It cannot expose your documents, because we do not have them.

How do users authenticate? Do you support SSO?

Accounts use email-based sign-in, and most KeptPDF tools work with no account at all. Single sign-on and SAML are not currently offered. If this matters for a Practice deployment, contact us.

Will you notify us of subprocessor changes?

The current subprocessor list is above and on keptpdf.com/trust. Material changes are reflected there.

Do you offer a DPA or a BAA?

Account and billing data is processed under our Privacy Policy. If your procurement requires a signed Data Processing Addendum, contact us. For HIPAA, because protected health information never reaches our servers, whether a BAA is required is a determination for your counsel. A BAA template based on HHS sample provisions is provided on our HIPAA page for your counsel to review and adapt. This document is information, not legal advice.

What are the limits of automatic redaction?

Automatic detection scans 45 kinds of sensitive data and is a strong first pass, not a replacement for human review. A text scanner cannot, on its own, catch handwriting, a face in a photo, or text baked into a scanned image. KeptPDF flags those pages for your review. For HIPAA Safe Harbor, 14 of the 18 identifier types are scanned automatically and the rest require a human. Each redaction's certificate records exactly what was scanned, so a reviewer can see the real scope.

How can we independently verify these claims?

Run any tool in Airplane Mode, watch the Network tab while you process a file, read the in-browser source, or verify a redaction's SHA-256 certificate at keptpdf.com/verify. The verification methods are described above.

This overview describes KeptPDF's architecture for vendor and security assessment. It is informational and not legal advice. Questions: support@keptpdf.com · keptpdf.com/trust · keptpdf.com/verify