docuProof.io

Privacy & Data Handling Policy

Effective February 28, 2026

This document describes how docuProof handles user data and privacy. It is timestamped using docuProof to create a permanent, verifiable record of our privacy commitments at the time they were made.

1. CORE PRIVACY PRINCIPLE

docuProof is designed around a fundamental privacy principle: your files never leave your device. When you use docuProof, only a cryptographic hash (a one-way mathematical code) is transmitted. The hash cannot be reversed to reconstruct your file. We cannot see, read, store, or access the content of any file you timestamp.

2. WHAT WE COLLECT

Information we receive:

- SHA-256 hash of your file (computed in your browser, transmitted for anchoring)
- Email address (provided at checkout for certificate delivery)
- Display name (optional — appears on your certificate if provided)
- Filename (optional — appears on your certificate if provided)
- Payment information (processed by Stripe; docuProof does not store card details)

Information we never receive:

- The content of your files
- The names of your files (unless you optionally provide one)
- Metadata embedded in your files
- Any information that could identify what you timestamped

3. HOW WE USE YOUR DATA

Data	Purpose	Retention
Email address	Deliver proof receipts and certificates	Stored for proof delivery and support

Data	Purpose	Retention
SHA-256 hash	Anchor to Bitcoin blockchain via OpenTimestamps	Permanently recorded on blockchain
Proof ID	Allow you to look up and verify your proof	Stored indefinitely for verification
Display name / filename	Print on your Certificate of Proof	Stored with proof record
Payment data	Process transactions via Stripe	Handled entirely by Stripe

4. THIRD-PARTY SERVICES

docuProof uses the following third-party services in the course of normal operation:

- **Stripe** — Payment processing. Stripe handles all payment card data under its own privacy policy.
- **OpenTimestamps** — Open-source timestamping protocol. Only cryptographic hashes are submitted.
- **Bitcoin blockchain** — Public, decentralized ledger. Only hashes (not personal data) are recorded.
- **Netlify** — Web hosting and serverless functions. Standard web server logs may be collected.
- **Postmark** — Transactional email delivery for receipts and certificates.

5. WHAT WE DO NOT DO

- We do not sell, rent, or share your email address with third parties for marketing.
- We do not use tracking pixels or third-party analytics cookies.
- We do not build user profiles or behavioral models.
- We do not store or transmit your files or file contents in any form.
- We do not display ads or allow advertisers to access user data.

6. YOUR RIGHTS

You may request access to, correction of, or deletion of your personal data (email address and associated proof records) by contacting support@docuproof.io. Please note that cryptographic hashes anchored to the Bitcoin blockchain cannot be removed, as they are part of the permanent public record. However, these hashes cannot be used to identify you or reconstruct your files.

7. CHANGES TO THIS POLICY

If we make material changes to this privacy policy, we will publish and timestamp an updated version using docuProof, creating a verifiable record of when the change occurred. The previous version remains independently verifiable on the blockchain.