PolicyProof
Data Handling Commitment

Last updated: May 2026 — Version 1.0

This document describes in plain English how PolicyProof handles your organization's compliance data. It is designed to answer the questions insurance compliance and legal teams typically ask before using a new tool.

Your data belongs to you — always

The compliance policies, AI decision records, and organizational information you enter into PolicyProof are yours. We have no claim to it. You can export it or delete it at any time. We will never monetize your data.

We never train AI on your data

Your compliance policies, underwriting guidelines, claims procedures, and decision records will never be used to train any AI model — ours or anyone else's. This is an absolute commitment, not a setting that could be changed in terms and conditions.

Current phase — data stays in your browser

The current version of PolicyProof stores all data locally in your browser session. Nothing you enter is transmitted to or stored on our servers. When you close your browser, the data clears. This means: no data breach risk from our servers, no unauthorized access to your compliance information.

Production phase — encrypted US servers

When we move to production database storage, your data will be stored on servers located in the United States, encrypted at rest using AES-256, transmitted only over TLS 1.2+ encrypted connections, and accessible only to authorized personnel under strict access controls. We will notify you before this transition and update this document accordingly.

No third-party data sharing

We do not share your compliance data with any third parties. Ever. Not for analytics, not for marketing, not for any purpose. The only data that leaves your browser in the current phase is your email address if you submit the access request form.

You control deletion

You can delete your data at any time. In the current pilot phase, closing your browser clears all data. In the production phase, we will provide a self-service deletion tool. We will confirm deletion within 30 days of request.

No sensitive personal data in current phase

The current version of PolicyProof is designed for compliance policy documentation and AI decision audit trails. Please do not enter personally identifiable information about policyholders, claimants, or employees into the current pilot version. The production version will include appropriate controls for sensitive data handling.

Security incident notification

In the unlikely event of a security incident affecting your data, we will notify you within 72 hours of becoming aware of the incident, consistent with applicable breach notification requirements.

Questions and requests

For data handling questions, access requests, or deletion requests: Email: suneel@policyproof.ai Website: policyproof.vercel.app We respond to all data handling requests within 5 business days.

Summary — The Five Commitments

1. Your data belongs to you — we have no claim to it

2. We never train AI models on your data — absolute commitment

3. Current phase — data stays in your browser, never transmitted to our servers

4. Production phase — encrypted US servers, AES-256, TLS 1.2+

5. You control deletion — we confirm within 30 days