Wo deine Belege liegen, und warum sie dort sicher sind

Rechnungskit trägt kein eigenes Zertifikat (etwa ISO 27001 oder SOC 2). Was es stattdessen gibt: ein ISO-27001-zertifiziertes Rechenzentrum in Deutschland, technische Schutzmaßnahmen, die sich prüfen lassen, und GoBD- und DATEV-Anforderungen, die direkt im System umgesetzt sind. Diese Seite fasst zusammen, was das konkret bedeutet.

100 % EU
Server in Deutschland, Backup in Finnland, kein US-Cloud-Anbieter

ISO 27001
Zertifiziertes Rechenzentrum (Hetzner, Falkenstein)

WORM + SHA-256
Unveränderbares Belegarchiv, Prüfsumme bei jedem Abruf

DATEV EXTF
Festschreibbare Exporte, byte-identisch nachweisbar

Hosting und Datenstandort

EU ONLY

Produktivsystem in Deutschland: Hetzner Online, Rechenzentrum Falkenstein, nach ISO/IEC 27001 zertifiziert.

Kein US-Cloud-Anbieter in der Verarbeitungskette: Anwendung, Datenbank, Belegarchiv und Backups laufen ausschließlich bei EU-Anbietern.

Backup in Helsinki (Finnland, EU): Alles, was Deutschland verlässt, wird vor der Übertragung clientseitig verschlüsselt (AES-256). Der Backup-Standort sieht nur Chiffrat.

Schutzschicht: Web Application Firewall und Bot-Schutz über einen europäischen Anbieter (Bunny, Slowenien).

Auftragsverarbeitung: AV-Vertrag nach Art. 28 DSGVO unter rechnungskit.de/avv. Alle Unterauftragsverarbeiter sitzen in der EU.

GoBD-Archiv

UNVERÄNDERBAR

WORM-Speicher: Jeder finalisierte Beleg (ZUGFeRD PDF/A-3 mit EN-16931-XML) liegt in versioniertem Objektspeicher mit Object Lock. Überschreiben oder Löschen ist technisch gesperrt, auch für Rechnungskit selbst.

Integritätsnachweis: SHA-256-Prüfsumme je Beleg, verifiziert bei jedem Abruf. Ein manipulierter Beleg würde sofort auffallen.

Datenbank-seitige Sperren: Archivierte Belege, Positionen, Vorlagen-Versionen und Protokoll sind gegen UPDATE und DELETE gesperrt (Trigger). Korrekturen nur über Storno und Neuausstellung.

Lückenlose Nummernkreise: Nummernvergabe und Archivschreibvorgang sind eine Transaktion. Ein Beleg, der die Validierung nicht besteht, verbraucht keine Nummer.

Aufbewahrung 8 Jahre (§ 147 AO, Frist für Buchungsbelege seit 2025). Der komplette Archiv-Export steht dir jederzeit offen, auch 90 Tage nach Vertragsende kostenlos.

DATEV-Export und Steuerkanzlei

FESTSCHREIBUNG

Standardformat DATEV EXTF (Buchungsstapel, SKR03/SKR04): deine Steuerkanzlei importiert die Datei ohne Zusatzsoftware direkt in DATEV.

Festschreibung: Ein festgeschriebener Export ist unveränderlich, jeder spätere Download byte-identisch (SHA-256-geprüft). Festschreiben dürfen nur Inhaber und Steuerkanzlei-Rolle.

Kanzlei-Zugang mit Protokoll: Die Kanzlei arbeitet in einem eigenen Bereich, sieht Belege und Exporte, pflegt Konten-Zuordnungen. Jede Aktion wird unveränderlich protokolliert, der Zugriff ist mit einem Klick widerrufbar.

Keine stillen Fehlbuchungen: Fehlt eine Konten-Zuordnung, wird die Zeile mit Warnung übersprungen, nie falsch gebucht.

Anwendung und Zugriff

MEHRSCHICHTIG

Mandantentrennung auf Datenbankebene: Row-Level-Security in PostgreSQL, erzwungen auf allen Mandanten-Tabellen. Ohne gültigen Mandantenkontext liefert die Datenbank keine Zeile (fail-closed).

Rollen und Rechte: Inhaber, Buchhaltung, Steuerkanzlei, Betriebsprüfung (befristeter Lesezugriff), Lesen. Die Rechtematrix wird zentral erzwungen und durch automatisierte Tests abgesichert: die Lese-Rolle kann nichts ändern und nichts herunterladen.

Befristete Fremdzugriffe: Support- und Agenturzugänge laufen nach 30 Tagen automatisch ab.

Transport und Speicherung: TLS für alle Verbindungen, Belege im Archiv zusätzlich AES-256-verschlüsselt, Passwort-Mindestlänge und Rate-Limiting gegen Brute-Force.

Server-Härtung: Firewall default-deny, SSH nur per Schlüssel, automatische Sicherheitsupdates. Sicherheits-Audit des Quellcodes im Juli 2026, alle Findings behoben.

Backup und Wiederherstellung

3-2-1

Drei Kopien, zwei Speichersysteme, ein zweiter Standort: Datenbank kontinuierlich gesichert (max. ca. 1 Minute Datenverlust) plus tägliche unabhängige Dumps; Belegarchiv und Volumes nächtlich verschlüsselt nach Helsinki gespiegelt; wöchentlicher Server-Snapshot.

Ransomware-resistent: Die Anwendung besitzt keine Zugangsdaten für den Backup-Standort. Ein kompromittierter Server könnte Backups weder lesen noch löschen. Das Archiv ist durch Versionierung und Object Lock zusätzlich geschützt.

Geübt, nicht nur geplant: Wiederherstellungs-Übungen werden regelmäßig durchgeführt und protokolliert (Datenbank-Restore, Stichproben-Belege mit Prüfsummenabgleich). Ein unabhängiges Monitoring alarmiert, wenn ein Backup ausbleibt.

Ehrlich benannt: Was Rechnungskit nicht hat, und warum das in Ordnung ist

TRANSPARENZ

Gibt es ein GoBD-Zertifikat?

Nein, und das gibt es für keine Software: Die Finanzverwaltung erteilt keine Testate (GoBD Rz. 179 ff.), Zertifikate Dritter sind nicht bindend. Entscheidend sind die tatsächlichen Maßnahmen (oben) und deine Verfahrensdokumentation. Die technische Beschreibung dafür liefert Rechnungskit.

Ist Rechnungskit eine „DATEV-zertifizierte Schnittstelle"?

Nein. Rechnungskit erzeugt das offene DATEV-Standardformat EXTF, das jede Kanzlei ohne Freischaltung importiert. Eine Zertifizierung ist dafür nicht erforderlich.

Ist Rechnungskit selbst ISO-27001-zertifiziert?

Nein. Eine eigene Zertifizierung ist ein mehrmonatiges Verfahren, das erst ab einer gewissen Unternehmensgröße sinnvoll ist. Zertifiziert ist die Infrastruktur, die deine Daten physisch hält; die Maßnahmen darüber sind dokumentiert und auf Nachfrage im Detail einsehbar.

Wer trägt die Verantwortung?

Die Aufbewahrungspflicht nach § 147 AO liegt bei dir als Unternehmen. Rechnungskit stellt Archiv, Integritätsnachweis und jederzeitigen Export bereit, damit du diese Pflicht erfüllen kannst, unabhängig davon, ob du Kunde bleibst.