



Sicherheitserklärung

VERSION 1.0 · GÜLTIG AB 1. SEPTEMBER 2026 · ZULETZT GEPRÜFT 24. JULI 2026

Hinweis: Diese deutsche Fassung ist eine maschinelle Übersetzung und dient nur der Vereinfachung. Rechtlich maßgeblich ist die englische Originalfassung.

Diese Erklärung fasst die technischen und organisatorischen Maßnahmen zusammen, mit denen wir die CashXChain-Plattform und die darauf befindlichen Daten schützen. Es handelt sich um eine öffentliche Zusammenfassung; interne Verfahren werden dabei nicht offengelegt.

- 1. Unser Ansatz.** Sicherheit ist fester Bestandteil der Art und Weise, wie wir die Plattform konzipieren, entwickeln und betreiben. Wir treffen dem Risiko angemessene Maßnahmen im Einklang mit Artikel 32 [DSGVO](#) und überprüfen diese regelmäßig.
- 2. Verschlüsselung.** Der gesamte Datenverkehr zu und von unserer Plattform wird bei der Übertragung mit TLS 1.3 verschlüsselt und an Cloudflares Edge terminiert. Ruhende Daten werden mit AES-256 verschlüsselt.
- 3. Authentifizierung und Zugriff.** Wir schützen Konten mit Mehr-Faktor-Authentifizierung, einschließlich Unterstützung für Passkeys (WebAuthn), sowie optionaler Anmeldung über etablierte Identitätsanbieter. Die Authentifizierung erfolgt über unseren selbst gehosteten Authentifizierungsdienst. Der interne Zugriff auf Systeme und Daten erfolgt über eine rollenbasierte Zugriffskontrolle, erzwingt Mehr-Faktor-Authentifizierung auf allen internen Systemen, folgt dem Grundsatz der geringsten Rechte und wird durch Audit-Protokollierung erfasst.
- 4. Netzwerk- und Infrastruktursicherheit.** Unsere Plattform arbeitet hinter Cloudflare, das TLS, eine Web Application Firewall, DDoS-Schutz, Bot-Management und eine datenschutzfreundliche Herausforderung (Turnstile) bereitstellt. Die Plattform wird bei Amazon Web Services in der Region eu-central-1 (Frankfurt) gehostet.
- 5. Sichere Entwicklung.** Wir folgen sicheren Entwicklungspraktiken, einschließlich Code-Review und Abhängigkeitsverwaltung. Eine unabhängige Sicherheitsdesign-Überprüfung wurde im Q2 2026 von Certora durchgeführt und deckte die Rust/Axum-Backend-Architektur und die Blockchain-Integration ab.
- 6. Überwachung und Reaktion auf Vorfälle.** Wir überwachen unsere Systeme im Hinblick auf Sicherheit und Verfügbarkeit. Wie und wann wir Kunden und Behörden über Sicherheitsvorfälle und Verletzungen des Schutzes personenbezogener Daten benachrichtigen, ist in unserer [Richtlinie zur Meldung von Vorfällen](#) (Incident Notification Policy) festgelegt. Sicherheitsforscher können Probleme über unsere Seite zur [verantwortungsvollen Offenlegung \(Responsible Disclosure\)](#) melden.
- 7. Datenschutz.** Wie wir personenbezogene Daten verarbeiten, einschließlich Aufbewahrung und Ihrer Rechte, ist in unserer [Datenschutzerklärung](#) festgelegt.
- 8. Ausfallsicherheit und Backups.** Wir erstellen täglich automatisierte Backups mit einer Aufbewahrungsdauer von 30 Tagen, halten für kritische Datenbanken eine Point-in-Time-Wiederherstellung vor und nutzen regionenübergreifende Replikation für Produktionsdaten, damit wir Verfügbarkeit und Zugriff nach einem Vorfall zeitnah wiederherstellen können.

9. Zertifizierungen und Roadmap. Die ISO-27001-Zertifizierung und die SOC-2-Attestierung befinden sich im Rahmen eines zweigleisigen Umsetzungsprogramms in aktiver Vorbereitung. Zeitpläne für Zertifizierung und Attestierung werden veröffentlicht, sobald sie bestätigt sind.

10. Kontakt. Sicherheitsfragen können an security@cashxchain.com gesendet werden; um eine Schwachstelle zu melden, siehe unsere Seite zur verantwortungsvollen Offenlegung (Responsible Disclosure).