Technische und organisatorische Maßnahmen

Eine Übersicht für Kundinnen, Kunden und Kanzleien: wie EaseAcc Ihre Daten schützt. Beschrieben ist nur, was eingerichtet ist.

EaseAcc · Stand 18. November 2026

Standort und Hosting

- Server und Sicherungen bei der Hetzner Online GmbH in Deutschland. Die Rechenzentren des Anbieters sind nach ISO 27001 zertifiziert; das Zertifikat gehört dem Anbieter, nicht EaseAcc.
- PDF-Erzeugung, Virenprüfung, Texterkennung und Belegerkennung laufen auf eigenen Servern, ohne fremde KI und ohne externe Erkennungsdienste.

Verschlüsselung

- Alle Verbindungen sind mit TLS verschlüsselt, Browser werden per HSTS auf verschlüsselte Verbindungen festgelegt.
- Passwörter werden nur als Argon2-Prüfwert gespeichert. Gespeicherte Geheimnisse (zum Beispiel Zwei-Faktor-Schlüssel) sind mit AES-256-GCM verschlüsselt, der Schlüssel liegt nicht in der Datenbank.
- Sicherungen werden verschlüsselt auf einen getrennten Speicher geschrieben. Hochgeladene Dateien tragen eine SHA-256-Prüfsumme.

Trennung der Firmen und unveränderbare Belege

- Jede Firma ist in der Datenbank durch zeilenbasierte Zugriffsregeln (Row-Level Security) von allen anderen getrennt. Die Anwendung greift mit einer eingeschränkten Datenbankrolle zu.
- Ausgestellte Rechnungen und erfasste Zahlungen sind per Datenbank-Trigger gegen Änderung gesperrt; Korrekturen gehen nur per Storno. Rechnungsnummern werden lückenlos vergeben.
- Ein Änderungsprotokoll hält fest, wer wann was getan hat. Es kann nur ergänzt werden, nie geändert oder gelöscht.
- Diese Maßnahmen unterstützen die Nachvollziehbarkeit und Unveränderbarkeit, die Betriebe und Kanzleien für ihre Aufzeichnungen brauchen. Eine Zertifizierung oder Konformitätserklärung ist damit nicht verbunden.

Zugang und Berechtigungen

- Persönliche Konten mit Zwei-Faktor-Anmeldung per Authenticator-App oder Passkey; der Inhaber kann sie für die ganze Firma verpflichtend machen.
- Passwortregeln: mindestens 12 Zeichen ohne, 8 mit Zwei-Faktor-Anmeldung; geprüft wird auch gegen bekannte kompromittierte Passwörter.
- Anmeldeschutz: Nach 5 Fehlversuchen je Konto bzw. 20 je Adresse innerhalb von 15 Minuten wird die Anmeldung vorübergehend gesperrt. Die Registrierung ist ohne externe Dienste gegen automatisierte Anmeldungen geschützt.
- Rollen: Inhaber, Stellvertretung, Buchhaltung, Verkauf, Mitarbeiter. Mitarbeiter sehen nur ihre eigene Arbeit.
- Der EaseAcc-Support sieht Rechnungen, Belege oder Bankdaten nur nach einer zeitlich begrenzten Freigabe durch Sie (nur lesen oder auch ändern, jederzeit beendbar). Jeder Zugriff steht im Protokoll, Sie erhalten eine E-Mail.
- Die Bankverbindung ist nur lesend. EaseAcc kann kein Geld bewegen.

Betrieb und Überwachung

- Jede Version wird vor der Auslieferung automatisch getestet, auch die Mandantentrennung und die Sperren in der Datenbank. Ausgeliefert wird genau das geprüfte Abbild.
- Von außen erreichbar sind nur der Webserver und der Fernwartungszugang mit Schlüssel. Sicherheitsupdates des Betriebssystems werden automatisch eingespielt, wiederholte Fehlversuche am Fernwartungszugang führen zur Sperre.
- Die Anwendung läuft in einem Container mit entzogenen Rechten und schreibgeschütztem Dateisystem. Hochgeladene Dateien werden auf Viren geprüft.
- Stündliche Selbstprüfung des Servers mit Alarm per E-Mail, dazu eine Prüfung von außen. Den aktuellen Stand und die Vorfälle der letzten 30 Tage zeigt die öffentliche Statusseite status.easeacc.com.

Sicherung und Wiederherstellung

- Tägliche Sicherung von Datenbank und Dateien, gestaffelt aufbewahrt (14 Tage, 8 Wochen, 24 Monate, bis zu 7 Jahre), dazu eine Sicherung vor jeder Aktualisierung.
- Die Sicherung wird laufend auf Unversehrtheit geprüft; einmal pro Woche läuft automatisch eine Wiederherstellungsprobe.
- Ihre Daten können Sie jederzeit vollständig exportieren.

Vertragsende und Löschung

- Nach dem Vertragsende bleiben die Bücher 6 Monate lesbar (Lesefrist) und lassen sich als Archiv mit Prüfsummen herunterladen; ein Archiv-Zugang kann gebucht werden.
- Danach wird die Firma nach Ankündigung gelöscht. Das Löschen wird nicht automatisch, sondern bewusst von Hand ausgelöst. Gesetzliche Aufbewahrungsfristen Ihres Betriebs bleiben bei Ihnen.

Dienstleister und Meldeweg

- Die eingesetzten Dienstleister stehen auf easeacc.com/de/subprocessors. Der Auftragsverarbeitungsvertrag liegt in der App zum Abschluss bereit.
- Sicherheitslücken bitte vertraulich an security@easeacc.com melden (Angaben nach RFC 9116 unter easeacc.com/.well-known/security.txt). Wir antworten innerhalb von zwei Werktagen.

Hinweis

Dieses Dokument beschreibt Maßnahmen und ist weder ein Zertifikat noch eine Zusage über Rechts- oder Steuervorschriften. Es kann sich mit der Weiterentwicklung von EaseAcc ändern; die jeweils aktuelle Fassung steht auf easeacc.com/de/security.

Fragen

Zu diesem Dokument und zur Datensicherheit: contact@easeacc.com. Hilfe bei der Nutzung: support@easeacc.com.