Saldoblick

Technische und organisatorische Maßnahmen

Version 1.0 · Veröffentlicht am 6. November 2026

Diese Maßnahmen treffen wir nach Art. 32 DSGVO für Saldoblick. Rechenzentren betreiben wir nicht selbst, sondern nutzen die unserer Subdienstleister.

1. Vertraulichkeit

Zutritt zu Räumen und Rechenzentren

Die Daten liegen ausschließlich in Rechenzentren der Subdienstleister, die den physischen Zutritt regeln.

Zugang zu den Systemen

- Nutzer melden sich mit E-Mail-Adresse und Passwort an. Passwörter speichern wir nur als nicht umkehrbaren Hash.
- Jeder Nutzer kann einen zweiten Faktor (Einmalcode) einrichten. Danach verlangt ihn jede Anmeldung. Für unsere eigenen Betreiberzugänge ist er Pflicht.
- Sitzungen laufen höchstens zwölf Stunden. Ändert ein Nutzer sein Passwort oder schaltet er den zweiten Faktor ab, beenden wir seine anderen Sitzungen.
- Das Sitzungs-Cookie ist versiegelt und für Skripte nicht lesbar.
- Anmeldeversuche begrenzt die Firewall des Hosting-Anbieters.

Zugriff auf Daten

- Jeder Nutzer hat eine Rolle (Inhaber, Administrator, Controller, Betrachter). Die Rolle bestimmt, was er sehen und ändern darf.
- Arbeiten wir zur Unterstützung in der Anwendung eines Kunden, geschieht das in einer eigenen Sitzung, die wir protokollieren.

Trennung

- Jedes Unternehmen ist ein eigener Mandant mit eigener Adresse.
- Die Datenbank erzwingt die Trennung zusätzlich zur Anwendung: Die Anwendung greift mit einer Rolle zu, die an die Zeilenregeln der Datenbank (Row-Level-Security) gebunden ist und sie nicht umgehen kann. Jede Anfrage arbeitet in einer Transaktion, die nur die Daten ihres Mandanten sieht.
- Auf Anfrage betreiben wir ein Unternehmen mit eigener Datenbank und eigenem Deployment.

Verschlüsselung

- Die Übertragung zwischen Browser und Anwendung ist mit TLS verschlüsselt.
- Zugangsdaten zu angebundenen Systemen speichern wir mit AES-256-GCM verschlüsselt. Der Schlüssel liegt nicht in der Datenbank.
- Der Datenbankanbieter verschlüsselt die gespeicherten Daten.

2. Integrität

Weitergabe

- Wir geben Daten nur an die Subdienstleister und nur zu dem dort genannten Zweck weiter.
- Die Anwendung setzt Sicherheits-Header, darunter eine strenge Content-Security-Policy. Sie lädt keine Skripte und Schriften von Dritten.
- Der Assistent verarbeitet Daten ausschließlich in Rechenzentren der Europäischen Union.

Eingabe

- Anmeldungen und Änderungen werden mit Zeitpunkt, Nutzer, IP-Adresse und Browser protokolliert. Das gilt auch für Änderungen, die der Assistent nach Bestätigung vornimmt.
- Passwörter, Zugangsschlüssel und Tokens landen nicht im Protokoll.
- Der Assistent ändert Daten erst, nachdem ein Nutzer es bestätigt hat.

3. Verfügbarkeit und Belastbarkeit

- Anwendung und Datenbank laufen in Frankfurt am Main.
- Der Datenbankanbieter hält Wiederherstellungspunkte vor, mit denen sich ein früherer Stand der Datenbank herstellen lässt.
- Änderungen an der Datenbank spielen wir mit versionierten Migrationen ein, bevor der Code veröffentlicht wird, der sie braucht.

4. Überprüfung und Bewertung

- Mandantentrennung, Rollen, Sitzungen und Verschlüsselung sind durch automatisierte Tests abgedeckt. Sie laufen bei jeder Änderung am Code, bevor sie veröffentlicht wird.

5. Auftragskontrolle

- Subdienstleister setzen wir nur mit Vertrag zur Auftragsverarbeitung ein.
- Wir verarbeiten Daten nur nach Weisung des Kunden.

- Wer bei uns Zugang zu Kundendaten hat, ist zur Vertraulichkeit verpflichtet.