Aveldra

TRUST CENTER · SELBSTAUSKUNFT

Security Self-Assessment Summary

Aveldra · Stand 1. August 2026 · Version 1.1 · Daniel Acar (§19 UStG)

Diese Zusammenfassung beschreibt die Sicherheits- und Datenschutzkontrollen von Aveldra in der Struktur des CAIQ (Cloud Security Alliance). Aveldra erhält privilegierten, überwiegend lesenden Zugriff auf Microsoft-365-Mandanten – deshalb legen wir offen, was wir tun und was wir bewusst nicht tun. Alle Angaben sind zum genannten Stand codebelegt.

Selbstauskunft – keine externe Zertifizierung. Dieses Dokument ist eine ehrliche Selbsteinschätzung des Betreibers, kein SOC-2-/ISO-27001-Bericht und kein externer Penetrationstest. Ein Pentest ist geplant, sobald er von Kundenseite gefordert wird.

1 · Governance & Risiko-Management

Wer betreibt Aveldra und wie wird Sicherheit gesteuert?
Aveldra wird von Daniel Acar (Einzelunternehmen, §19 UStG) betrieben. Sicherheit ist im Entwicklungsprozess verankert: strenge CI-Gates (Ruff-Lint, Bandit-SAST, Gitleaks-Secret-Scan, >970 automatisierte Tests, ~83 % Backend-Coverage mit Coverage-Floors) und ein fail-closed Produktions-Boot-Gate, das den Start mit unsicheren Default-Secrets verweigert.

Gibt es externe Zertifizierungen (SOC 2, ISO 27001) oder einen Pentest?
Nein. Dies ist eine Selbstauskunft, keine externe Zertifizierung. Ein externer Penetrationstest ist geplant, sobald ein Kunde ihn anfordert. Wir weisen diesen Reifegrad bewusst offen aus.

2 · Datenschutz / DSGVO

Wo werden personenbezogene Daten verarbeitet?
Verarbeitung und Speicherung in der EU (Frankfurt, Fly.io). Einzelne Sub-Prozessoren können in den USA verarbeiten – abgesichert über EU-Standardvertragsklauseln (SCC) bzw. EU-US Data Privacy Framework (DPF).

Welche Daten werden verarbeitet – und welche nie?
Ausschließlich Sicherheits-Metadaten (App-Namen/-IDs, Berechtigungen, Anmelde-Metadaten wie IP/Land/Zeit/Risikostufe, Weiterleitungsregel-Metadaten). Niemals E-Mail- oder Dateiinhalte, keine Passwörter.

Gibt es einen AVV und eine offene Sub-Prozessoren-Liste?
Ja. Eine öffentliche, datierte Sub-Prozessoren-Liste (aveldra.de/subprozessoren) und ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO (unterschriftsfertig auf Anfrage).

3 · Zugriffskontrolle & Identität

Wie authentifizieren sich Nutzer?
Anbindung per einmaligem Microsoft-365-Admin-Consent (OAuth). Das id_token wird JWKS-signaturgeprüft. Sessions laufen über HttpOnly-/Secure-Cookies mit SameSite=lax – kein Token in localStorage/URL.

Gilt das Least-Privilege-Prinzip?

Ja. Laufende Analyse nutzt nur lesende Graph-Berechtigungen (Application.Read.All, AuditLog.Read.All, User.Read.All, Domain.Read.All). Schreibende Aktionen (Security Defaults, Gegenmaßnahmen) laufen ausschließlich auf explizite Nutzeraktion – nie automatisch im Hintergrund.

Wie wird bei Rollen-Unsicherheit entschieden?
Fail-closed: kann eine Admin-Rolle im Token nicht sicher bestimmt werden (Group-Overage), wird im Zweifel KEIN Admin-Zugriff gewährt. Die App-Authentifizierung gegen Microsoft nutzt ein Zertifikat statt eines Client-Secrets.

4 · Verschlüsselung & Schlüssel

Wie werden Daten in Transit und at Rest geschützt?
In Transit ausschließlich TLS/HTTPS. At Rest werden OAuth-Zugriffstokens symmetrisch verschlüsselt (Fernet / AES-128-CBC + HMAC-SHA256). Schlüssel-Rotation wird unterstützt (MultiFernet); ein fehlerhafter Schlüssel wird bereits beim Start abgewiesen (fail-closed).

Wie werden Secrets verwaltet?
Als plattformverwaltete Secrets (Fly.io), nie im Repository. Der Produktionsstart wird abgebrochen, wenn Pflicht-Secrets fehlen oder auf unsicheren Defaults stehen.

5 · Mandantenisolation

Wie wird verhindert, dass ein Kunde Daten eines anderen sieht?
Strikte Isolation auf Datenbankebene: jede Abfrage ist auf den jeweiligen Mandanten begrenzt, es gibt keine mandantenübergreifenden Abfragen. Die Isolation ist testabgedeckt (inkl. Schutz gegen Time-of-check/Time-of-use-Lücken).

Werden Kundendaten je zusammengeführt?
Nein. Daten werden zwischen Mandanten weder zusammengeführt noch weitergegeben.

6 · Hosting & Sub-Prozessoren

Welche Auftragsverarbeiter kommen zum Einsatz?
Fly.io (Compute/PostgreSQL, Frankfurt EU) · Vercel (Frontend-Hosting) · Stripe (Zahlungen) · Resend (Benachrichtigungs-E-Mails) · Sentry (Fehler-Monitoring). Off-Site-Backups auf EU-Objektspeicher (Backblaze EU Central) mit Immutability – in Einführung.

Ist Microsoft ein Sub-Prozessor?
Nein, nicht im engeren Sinne: die Microsoft-365-Daten stammen aus dem eigenen Tenant des Kunden; Aveldra liest sie über die Graph API (nur Metadaten).

7 · Backup & Notfallwiederherstellung

Wie werden Backups erstellt und geschützt?
Täglicher, verschlüsselter pg_dump (GPG/AES-256, client-seitig vor dem Upload verschlüsselt) zusätzlich zu Volume-Snapshots. Jedes Backup wird verifiziert (nicht leer, entschlüsselbar, integer) bevor es als Erfolg zählt.

Gibt es Off-Site-Redundanz und wurde Restore getestet?
Off-Site-Spiegelung auf immutable EU-Objektspeicher (Object-Lock) – in Einführung. Ein Restore-Drill mit exaktem Prod-Gegencheck wurde bestanden; Wiederholung quartalsweise.

8 · Incident Response & Monitoring

Wie werden Ausfälle und Vorfälle erkannt?
Dead-Man's-Switch-Monitoring (healthchecks.io) für alle 14 Hintergrund-Jobs und den Backup-Lauf: bleibt ein Heartbeat aus, alarmiert der externe Monitor. Fehler-Monitoring via Sentry mit PII-Scrubbing. Ein append-only Audit-Log hält sicherheitsrelevante Ereignisse unveränderbar fest.

Gibt es einen Kanal für Schwachstellenmeldungen?
Ja: verantwortungsvolle Offenlegung mit Safe-Harbor-Zusage (aveldra.de/sicherheit) und maschinenlesbarer Kontakt unter /.well-known/security.txt (RFC 9116). Zusätzlich automatischer Missbrauchsschutz (IP-Bann bei wiederholten Fehlversuchen).

9 · Datenaufbewahrung & -löschung

Wie lange werden Daten aufbewahrt?
Automatisierte, überwachte Löschjobs erzwingen die Fristen: gekündigte Mandanten werden 30 Tage nach Vertragsende vollständig gelöscht; Bedrohungsereignisse nach 24 Monaten; Nutzungsmetriken nach 12 Monaten; Snapshots nach 90 Tagen.

Wie kann ein Kunde Zugriff und Daten beenden?
Der Zugriff wird jederzeit selbstständig über den Microsoft-Admin-Consent entzogen – ohne Rücksprache. Nach Kündigung erfolgt die Löschung automatisch; auf Wunsch löschen wir auch vorher.

Ehrliche Grenzen (Stand heute)

- Solo-Betrieb; keine SOC-2-/ISO-27001-Zertifizierung.
- Noch kein externer Penetrationstest (geplant bei Kundenbedarf).
- Single-Region-Betrieb; Hochverfügbarkeit/Failover auf der Roadmap.

Kontakt für Rückfragen & AVV: kontakt@aveldra.de · Schwachstellen: aveldra.de/.well-known/security.txt