Technisch-organisatorische Maßnahmen (TOM)

AKI.IO GmbH · Marienburger Str. 1 · 10405 Berlin

Stand: 01.09.2026 · Version 1.3 (DE)

Geltungsbereich: alle Verarbeitungen personenbezogener Daten der AKI.IO GmbH (B2B-AI-API **auf deutscher HPC-Infrastruktur, kein Einsatz von Hyperscalern oder öffentlicher Cloud**).

1. Vertraulichkeit

1.1 Zutrittskontrolle

- Personalisierte Schlüssel für die Geschäftsräume in der Marienburger Str. 1, 10405 Berlin;
- Home Office mit separater Richtlinie und VPN / TLS
- Alarmanlage mit Bewegungs- und Fenstersensoren (24/7);
- Besucher werden empfangen, registriert und begleitet, Besucher nur in Ausnahmefällen und eher auf Dienstleister beschränkt;
- Trennung der WLAN-Netze: dedicated internes WLAN (WPA2-Enterprise/WPA3) und separates Gäste-WLAN ohne Zugriff auf interne Ressourcen;
- Hardware ist bei AIME GmbH (Subprozessor) gemietet und von dieser in Rechenzentren untergebracht;
- Rechenzentren sind nach ISO 27001 zertifiziert und erfüllen DIN EN 50600.

1.2 Zugangskontrolle (Authentifizierung)

- Individuelle Benutzerkonten in allen Systemen; Shared Accounts sind ausgeschlossen;
- Starke Passwortrichtlinie (Mindestlänge 12 Zeichen, Komplexitätsregeln, Passwort-Manager-Empfehlung);
- Multi-Faktor-Authentifizierung (MFA) für privilegierte Administrationszugänge;
- Keypass als Passwort Container
- API-Zugriffe nur über individuelle, jederzeit widerrufbare API-Keys; jeder Aufruf wird mit der Key-ID protokolliert;
- Administrative Zugriffe ausschließlich über VPN bzw. SSH mit Schlüssel-basierter Authentifizierung;
- Endgeräte sind disk-verschlüsselt (FileVault / BitLocker / LUKS); Privatgeräte sind im produktiven Zugriff ausgeschlossen.

1.3 Zugriffskontrolle (Berechtigungen)

- Rollenbasiertes Berechtigungsmodell (RBAC) nach dem Need-to-know-Prinzip;
- Vier-Augen-Prinzip für produktionsverändernde Aktionen (Berechtigungserteilung, Infrastruktur-Änderungen);
- Trennung von Entwicklungs-, Operations- und Administrationsrollen;
- Quartalsweise Re-Zertifizierung der Zugriffsrechte;
- Sichere Datenträgerlöschung defekter Disks im AIME-RZ nach NIST 800-88 / DIN 66399.

1.4 Pseudonymisierung und Verschlüsselung

- Transportverschlüsselung TLS (state-of-the-art) für alle externen und internen Verbindungen;
- Disk-Encryption auf Endgeräten;

- Aufbewahrung von Backups innerhalb Deutschlands;
- Pseudonymisierung in Logs (API-Key-ID anstelle direkter Nutzeridentifikatoren).

1.5 Verpflichtung der Beschäftigten und von Unterauftragnehmern

- Alle Beschäftigten werden vor Aufnahme ihrer Tätigkeit in Textform zur Verschwiegenheit verpflichtet und bestätigen dies mit ihrer Unterschrift;
- die Verpflichtung enthält eine ausdrückliche Belehrung nach § 203 Abs. 4 Satz 1 StGB sowie über die Pflichten nach Art. 28 Abs. 3 lit. b, Art. 29 und Art. 32 Abs. 4 DSGVO;
- sie gilt zeitlich unbeschränkt und über das Ende des Beschäftigungsverhältnisses hinaus;
- Unterauftragnehmer werden entsprechend verpflichtet.

2. Integrität

- Audit-Trails für administrative Zugriffe auf Code-Base über Git;
- Code-Review-Pflicht vor Deployment (Pull-Request-Workflow, Required Approvals by CTO);
- Change- und Release-Management; Rollback-Verfahren dokumentiert;
- Datenintegrität durch Mandantentrennung und konsequente Trennung von Produktiv-, Staging- und Entwicklungsumgebungen;

3. Verfügbarkeit und Belastbarkeit

- Tägliche Backups operativer Konfigurations- und Geschäftsdaten;
- Periodische Restore-Tests; Recovery-Ziele (RPO/RTO) sind in Finalisierung;
- USV und Klimatisierung im Rechenzentrum (AIME / RZ-Betreiber nach DIN EN 50600);
- Incident-Response-SOP;
- Notfall- und Wiederanlaufkonzept (BCM) als Bestandteil des ISMS in Aufbau;

4. Datenminimierung und Speicherbegrenzung

- **Inferenzdaten (Prompts, Outputs) werden transient im RAM bzw. GPU-Speicher verarbeitet und weder auf Datenträgern noch in Datenbanken, Logs, Swap oder temporären Dateien persistiert;**
- Zugriff auf den flüchtigen Speicher der Inferenz-Verarbeitung ist nicht möglich und wird auch zur Fehleranalyse, Monitoring oder Support nicht durchgeführt;
- Analyse, Monitoring und Support finden ausschließlich auf der abstrakten Ebene der Metadaten von Requests statt;
- **Keine Trainingsnutzung von Kundenpayloads; keine sekundäre Nutzung;**
- Logging beschränkt sich auf technische Metadaten; keine Payload-Inhalte;
- Aufbewahrungsfristen sind je Datenkategorie definiert (siehe Lösch- und Aufbewahrungskonzept).

5. Nichtverkettung

- Mandantentrennung pro Company-Account (Daten- und Schlüssel-Scoping);
- Strikte Trennung Test- / Staging- / Produktionsumgebungen;
- Datenverarbeitung der Inferenz ist organisatorisch und technisch von Account-/Billing-Daten getrennt.

6. Intervenierbarkeit

- Prozess Betroffenenrechte (Art. 15–22) etabliert; Anlaufstelle privacy@aki.io;
- Löschpflicht auch in Backups (Lifecycle dokumentiert);
- Datenportabilität (Art. 20): Exportfunktion für Account-Daten;
- Widerruf von Einwilligungen jederzeit über Cookie-Settings;

7. Transparenz

- Datenschutzhinweise erfüllen Art. 13/14 DSGVO;
- DPA (Standardvertrag für Kunden) im Backend abrufbar;
- AUP und ToU sind Bestandteil des Sign-up-Flows;
- Subprozessor-Liste ist Bestandteil der DPA und wird bei Änderungen aktiv kommuniziert;

8. Physische Sicherheit Office Berlin und Rechenzentren

Office: personalisierte Schlüssel, Alarmanlage, Fenstersensoren, WLAN-Trennung intern/Gast, abgeschlossene Schränke für sensible Unterlagen, Aktenvernichter DIN 66399 (Stufe P-4 oder höher).

Rechenzentren (Subprozessor der AIME GmbH): ISO 27001-zertifiziert, DIN EN 50600, USV, Klimatisierung, redundante Stromversorgung, personalisierte Zutrittskontrolle, kontinuierliche Überwachung.

9. Überprüfung und kontinuierliche Verbesserung

Maßnahme	Frequenz	Verantwortlich
TOM-Review	jährlich	Engineering + GF (bis Bestellung eines DSB)
Restore-Test Backup	halbjährlich	Engineering
Quartalsweise Access Review	quartalsweise	Engineering + GF
DSFA-Review	quartalsweise + anlassbezogen	GF (bis Bestellung eines DSB)