ANLAGE ZUM AVV — ART. 32 DSGVO

Technisch-organisatorische Maßnahmen

Stand: 25. April 2026 · SchnellPortal · Mindeststandard nach Art. 32 DSGVO

1. Zugriffskontrolle (wer darf was?)

- Rollenbasiertes Berechtigungssystem (Admin, Mitarbeiter, Monteur, Endkunde)
- Need-to-Know-Prinzip: User-bezogener Datenzugriff, beschränkt auf das eigene Konto
- Passwort-Hashing mit Argon2 (modernes, kollisionsresistentes Verfahren)
- Admin-Zugriffe der Anbieterseite auf den Anbieter beschränkt

2. Zugangskontrolle (Schutz gegen unbefugten Systemzugang)

- SSH-Key-Authentifizierung für Server-Zugriff (kein Passwort-Login möglich)
- Firewall auf Server-Ebene (nur HTTPS und SSH erreichbar)
- Cloudflare als vorgelagerter DDoS-Schutz und Rate Limiting

3. Weitergabekontrolle (Schutz bei Datenübertragung)

- TLS 1.3 für alle Browser- und API-Übertragungen
- Content Security Policy (CSP) eingeschränkt auf eigene Domain und freigegebene Ressourcen
- Keine Übertragung an Dritte ohne dokumentierte Rechtsgrundlage

4. Eingabekontrolle (Nachvollziehbarkeit)

- Protokollierung sicherheitsrelevanter Ereignisse auf Anwendungs- und Systemebene (z. B. Login, Passwort-Änderungen, Admin-Aktionen, Datenexporte)
- Code-Änderungen werden nachvollziehbar versioniert (Git, mit zugeordneten Commits und Zeitstempeln)

5. Verfügbarkeitskontrolle (Backup & Recovery)

- Tägliche automatisierte Datenbank-Backups; Vorhalteperiode wird laufend ausgebaut
- Dokumentierter Wiederherstellungsprozess

- Hosting in zertifizierten deutschen Rechenzentren der Hetzner Online GmbH (ISO 27001)

6. Trennungsgebot (Datentrennung)

- Account-basierte Datentrennung auf Anwendungsebene
- Jede Datenbank-Abfrage wird auf den authentifizierten User-Kontext beschränkt
- Keine Cross-Account-Sichtbarkeit zwischen Kundenkonten

7. Integrität (Schutz vor unbefugter Veränderung)

- Berechtigungssystem schützt vor unbefugten Daten-Änderungen
- Versionierte Deployments via Git (vollständige Änderungshistorie)
- Backups erlauben Rollback bei festgestellter Manipulation

8. Löschkonzept

- Bei Account-Löschung: 30 Tage Karenz, danach unwiderrufliche Löschung der operativen Bestandsdaten
- Steuerlich aufbewahrungspflichtige Daten (insbesondere Rechnungen, Buchungsbelege) werden gemäß § 147 AO bis zu 10 Jahre eingeschränkt aufbewahrt und ausschließlich für gesetzliche Zwecke vorgehalten
- Kunden können Daten jederzeit selbst exportieren

9. Incident-Management (Vorfälle)

- Definierter Prozess zur Erkennung, Bewertung und Meldung von Datenschutzvorfällen
- Meldung an die Aufsichtsbehörde gemäß Art. 33 DSGVO innerhalb von **72 Stunden**
- Information betroffener Kunden unverzüglich nach Bekanntwerden gemäß Art. 34 DSGVO
- Vorfallsprotokollierung intern dokumentiert

> **Weiterentwicklung:** SchnellPortal darf TOMs weiterentwickeln, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden Bestandskunden mitgeteilt.

Vollständige Dokumentation unter **schnellportal.com/compliance** · Diese Übersicht ist Anlage 1 zum SchnellPortal-Standard-AVV nach Art. 28 DSGVO.