

Technisch-organisatorische Massnahmen (TOM)

Anlage 1 zum Auftragsverarbeitungsvertrag (AVV)

Stand: April 2026

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Massnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren:

- Server betrieben in professionellem Rechenzentrum (Hetzner Online GmbH, Deutschland)
- Physische Sicherheit (Zutrittskontrolle, Videoüberwachung, Sicherheitspersonal) durch den Rechenzentrumsbetreiber gewährleistet
- Kein physischer Zugang des Anbieters zu den Servern erforderlich (vollständige Remote-Verwaltung)

1.2 Zugangskontrolle

Massnahmen, um Unbefugte an der Nutzung der Systeme zu hindern:

- SSH-Zugang zum Server ausschliesslich ueber SSH-Key-Authentifizierung (Ed25519)
- Kein Passwort-basierter SSH-Login
- Firewall (iptables/nftables) mit restriktiven Regeln
- Alle Dienste (PostgreSQL, Keycloak) nur ueber localhost erreichbar (kein externer Port)
- nginx als Reverse-Proxy mit TLS-Terminierung

1.3 Zugriffskontrolle

Massnahmen, um sicherzustellen, dass Berechtigte nur auf die ihnen zugeordneten Daten zugreifen:

- Authentifizierung ueber Keycloak (OpenID Connect) mit individuellen Benutzerkonten
- Multi-Tenant-Datentrennung: Alle Datenbankabfragen filtern nach user_id
- Rollenbasierte Zugriffskontrolle (@login_required, @admin_required)
- Session-Cookies mit Secure, HttpOnly, SameSite=Lax
- Automatische Session-Invalidierung bei Logout
- Admin-Zugang beschraenkt auf definierte E-Mail-Whitelist

1.4 Trennungskontrolle

Massnahmen zur getrennten Verarbeitung von Daten verschiedener Auftraggeber:

- Strikte Multi-Tenant-Architektur: Alle Daten nach user_id isoliert
- Keine mandantenubergreifenden Abfragen moeglich
- Separate Credentials-Verwaltung pro Nutzer (Bloomest, Miele)
- Display-Links durch kryptographische Token (43 Zeichen, secrets.token_urlsafe(32)) geschuetzt

2. Integritaet (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Massnahmen, um personenbezogene Daten bei Uebertragung zu schuetzen:

- Alle Verbindungen ausschliesslich ueber HTTPS/TLS (Let's Encrypt Zertifikate)

- Automatische Zertifikatserneuerung via certbot

- API-Kommunikation mit Drittanbietern (Bloomest, Miele) ausschliesslich ueber HTTPS

- Keine unverschlüsselten Datenübertragungen

2.2 Eingabekontrolle

Massnahmen zur Nachvollziehbarkeit von Dateneingaben:

- Server-Access-Logs (nginx) mit IP, Zeitstempel, angeforderter Ressource
- Anwendungs-Logging bei relevanten Aktionen
- Datenbankeinträge mit Zuordnung zum jeweiligen Benutzer (user_id)
- Aufbewahrung von Server-Logs fuer 30 Tage

3. Verfuegbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfuegbarkeitskontrolle

Massnahmen zum Schutz gegen Datenverlust:

- VPS bei Hetzner mit redundanter Infrastruktur
- PostgreSQL-Datenbank mit transaktionaler Integritaet
- Angestrebte Verfuegbarkeit: 99% im Jahresmittel
- Systemd-Service mit automatischem Neustart bei Absturz

3.2 Belastbarkeit

Massnahmen zur Gewaehrleistung der Belastbarkeit:

- Gunicorn Application Server mit mehreren Workern (3 Worker, 4 Threads)
- nginx als Load-Balancing Reverse-Proxy
- Caching von Maschinendaten und Umsatzdaten zur Reduzierung von API-Aufrufen
- Miele-Cookie-Cache (55 Min TTL) zur Vermeidung ueberfluessiger Logins

4. Verfahren zur regelmaessigen Ueberpruefung (Art. 32 Abs. 1 lit. d DSGVO)

4.1 Datenschutz-Management

- Dieser AVV und die zugehoerigen TOM werden regelmaessig ueberprueft und bei Bedarf aktualisiert
- Aenderungen werden dem Auftraggeber mitgeteilt

4.2 Incident-Response

- Datenschutzverletzungen werden unverzueglich erkannt und gemeldet (Art. 33 DSGVO)
- Benachrichtigung des Auftraggebers innerhalb von 72 Stunden nach Bekanntwerden
- Dokumentation von Vorfaellen und getroffenen Gegenmassnahmen

4.3 Software-Sicherheit

- Regelmaessige Updates des Betriebssystems (Debian 13)
- Aktuelle Versionen aller eingesetzten Software-Komponenten (Flask, PostgreSQL, Keycloak, nginx)
- Passwort-Verschluesselung: Miele-Passwoerter mit Fernet (AES-128-CBC), Bloomest-Passwoerter als SHA1-Hash (API-Vorgabe des Drittanbieters, nicht beeinflussbar)

5. Zertifizierungen und Audits des Rechenzentrumsbetreibers

5.1 Hetzner Online GmbH -- Zertifizierungen

Der Rechenzentrumsbetreiber Hetzner Online GmbH verfügt ueber folgende Zertifizierungen:

Zertifizierung	Gultig bis	Bemerkung
ISO 27001	September 2028	Zertifiziert seit Oktober 2016, regelmassig erneuert
BSI C5 Typ 2	--	Erteilt seit Dezember 2025

5.2 TUEV-Audit der technisch-organisatorischen Massnahmen

Die TOM von Hetzner Online GmbH werden jaehrlich durch den TUEV Rheinland geprueft. Das letzte Audit umfasste folgende Standorte:

Standort	Pruefungsdatum
Helsinki / Tuusula (Finnland)	19.02.2026
Nuernberg (Deutschland)	07.02.2024
Falkenstein (Deutschland)	11.02.2025

Ergebnis: Bei der Pruefung wurden keine Abweichungen festgestellt.

Der aktuelle Pruefbericht ist ueber das Hetzner-Kundenportal abrufbar unter: <https://accounts.hetzner.com/account/dpa>

5.3 AVV mit Hetzner Online GmbH

Ein Auftragsverarbeitungsvertrag (AVV) gemaess Art. 28 DSGVO wurde mit Hetzner Online GmbH geschlossen:

- **Vertragsnummer:** K0401256926
- **Unterzeichnet am:** 21.04.2026
- **Datenverarbeitung:** Ausschliesslich innerhalb der EU (bei Wahl eines EU-Serverstandorts)

5.4 Verantwortlichkeiten bei Cloud-Server-Produkten

Gemaess der Hetzner-Produktdokumentation und dem TUEV-Audit obliegen dem Auftragnehmer (Dynkhues GmbH) als Betreiber des Cloud Servers folgende Massnahmen:

Massnahme	Verantwortlich	Umsetzung
Datensicherung / Backup	Auftragnehmer	PostgreSQL-Backups (regelmassig, automatisiert)
Firewall-Konfiguration	Auftragnehmer	iptables/nftables mit restriktiven Regeln
Verschluesselung ruhender Daten	Auftragnehmer	Fernet-Verschluesselung sensibler Credentials
Virenschutz	Auftragnehmer	Regelmassige Sicherheitsupdates, gehaertete Serverkonfiguration

Hetzner stellt die physische Infrastruktur, Netzanbindung und Stromversorgung mit Redundanz bereit. Die logische Sicherheit des Servers liegt vollstaendig in der Verantwortung des Auftragnehmers.

6. Verschluesselung

Kontext	Methode
Datenuebertragung (Browser <-> Portal)	TLS 1.2+ (HTTPS via Let's Encrypt)
Datenuebertragung (Portal <-> APIs)	TLS 1.2+ (HTTPS)

Kontext	Methode
Datenuebertragung (Portal <-> DeepL)	TLS 1.2+ (HTTPS), nur Textinhalte, keine Kontodaten
Miele-Passwoerter (Speicherung)	Fernet-Verschluesselung (AES-128-CBC + HMAC)
Bloomest-Passwoerter (Speicherung)	SHA1-Hash (API-Vorgabe, nicht aenderbar)
Flask-Sessions	Signiert mit FLASK_SECRET_KEY
Keycloak-Passwoerter	bcrypt (Keycloak-internes Hashing)

7. Eingesetzte Infrastruktur-Komponenten

Komponente	Version	Funktion
Debian	13 (Trixie)	Betriebssystem
nginx	aktuell	Reverse Proxy, TLS-Terminierung
Keycloak	26.2	Identity & Access Management
PostgreSQL	16	Datenbank
Flask + Gunicorn	aktuell	Application Server
Playwright + Chromium	aktuell	Miele Move Login (Headless Browser)
Docker	aktuell	Keycloak + PostgreSQL Container

Letzte Aktualisierung: April 2026