DaZ Pilot TOM

Softstack GmbH
Schiffbrückstraße 8
24937 Flensburg
hello@softstack.io

Dokument: Technische und organisatorische Maßnahmen
Erstellt: 07. September 2026

Technische und organisatorische Maßnahmen (TOM)

Stand: September 2026

Diese Dokumentation beschreibt die technischen und organisatorischen Maßnahmen der **Softstack GmbH** gemäß Art. 32 DSGVO für den Betrieb der cloudbasierten SaaS-Variante von **DaZ Pilot**. Sie bildet Anlage 2 zum Auftragsverarbeitungsvertrag und orientiert sich an den Bausteinen des BSI IT-Grundschutzes.

Hosting-Standort: zertifiziertes Rechenzentrum der **IONOS SE** in Frankfurt am Main (ISO 27001, BSI C5, BSI IT-Grundschutz).

1. Vertraulichkeit

1.1 Zutrittskontrolle

Physischer Zugang zu den Verarbeitungssystemen ist auf das Rechenzentrum der IONOS SE beschränkt. Nachweislich umgesetzt werden unter anderem:

- 24/7-Zugangskontrolle und Videoüberwachung
- biometrische und/oder chipkartenbasierte Zutrittssicherung
- protokollierte Zutritte und Besuchermanagement
- physische Trennung und abgesicherte Serverräume gemäß den IONOS-Zertifizierungen

Softstack-Mitarbeitende haben keinen physischen Zutritt zu den Serverräumen; der Zugang erfolgt ausschließlich remote über gesicherte Verwaltungswege.

1.2 Zugangskontrolle

- Authentifizierung über Session-Tokens (SHA-256-gehasht) bzw. OpenID Connect (Moodle)
- Passwort-Policy und Session-Timeouts
- Multi-Faktor-Authentifizierung für privilegierte Admin-Zugänge zur Infrastruktur
- Super-Admin-API-Schlüssel mit Mindestlänge von 64 Zeichen
- keine Weitergabe von Zugangsdaten; Zugang nur für autorisierte Mitarbeitende

1.3 Zugriffskontrolle

Rollenbasiertes Zugriffssystem (RBAC) mit den Rollen Super-Admin, Lehrkraft und Schüler:in

Prinzip der geringsten Rechte (Least Privilege)

schulbezogene Mandantentrennung: Datenbankabfragen sind über `school_id` scoped

getrennte Qdrant-Collections und Classifier-Blobs (`school_classifiers`) je Schule

Audit-Logs für kritische Vorgänge (Rechteänderungen, Löschungen, Vertragsbezogene Aktionen)

1.4 Trennungskontrolle

logische Mandantentrennung auf Anwendungsebene (schuleigene Datensätze)

getrennte Entwicklungs-, Test- und Produktionsumgebungen

Produktivdaten werden nicht in Entwicklungs- oder Testsystemen verwendet

1.5 Pseudonymisierung

Schüler:innen-Profile werden pseudonymisiert gespeichert; personenbezogene Zuordnung erfolgt über die Moodle-OIDC-Kennung der jeweiligen Bildungseinrichtung

Session-Tokens werden ausschließlich gehasht gespeichert

Kamerabilder/Frames werden nur temporär zur Klassifikation verarbeitet und nicht dauerhaft als Rohbild dem Nutzerprofil zugeordnet

2. Integrität

2.1 Weitergabekontrolle

externe Kommunikation ausschließlich über TLS 1.3

der ML-Service (SigLIP 2 / LinearSVC) ist nur im privaten Netzwerk erreichbar und nicht öffentlich exponiert

keine Übermittlung personenbezogener Daten in Drittländer außerhalb der EU/des EWR

verschlüsselte administrative Zugänge (SSH/VPN) zur Infrastruktur

2.2 Eingabekontrolle

Protokollierung kritischer Eingaben und Änderungen (Audit-Logs)

strukturiertes Logging (Pino) mit nachvollziehbaren Zeitstempeln und Akteursbezug

nachvollziehbare Lösch- und Rechteänderungsvorgänge

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

angestrebte monatliche Verfügbarkeit von 99 % (vgl. § 7 AGB), exklusive geplanter Wartung

Health-Checks für Backend, ML-Service und abhängige Dienste

containerisierter Betrieb (Docker) mit Orchestrierung und automatischem Neustart bei Ausfällen

Schutz vor Überlastung durch Ressourcenlimits und Monitoring

3.2 Wiederherstellbarkeit

tägliche Backups der Datenbank mit 30-Tage-Rotation

dokumentierte Recovery-Verfahren

Wiederanlauf der Services über Infrastructure-as-Code / Docker-Compose

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Management

Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO

regelmäßige Überprüfung der TOM und des Löschkonzepts (mindestens jährlich)

Datenschutz-Ansprechpartner: hello@softstack.io (kein benannter Datenschutzbeauftragter nach § 38 BDSG erforderlich)

4.2 Incident-Response

dokumentierter Prozess zur Erkennung, Bewertung und Behandlung von Sicherheitsvorfällen

Benachrichtigung des Verantwortlichen innerhalb von 72 Stunden nach Kenntnis einer Verletzung des Schutzes personenbezogener Daten (vgl. § 10 AVV)

Koordination mit dem Hosting-Partner IONOS SE bei infrastrukturellen Vorfällen

4.3 Auftragskontrolle

Verarbeitung ausschließlich auf dokumentierte Weisung (vgl. AVV)

Register genehmigter Sub-Auftragsverarbeiter (Anlage 3 AVV)

vertragliche Weitergabe der Datenschutzpflichten an Sub-Auftragsverarbeiter

5. Weitere Maßnahmen

5.1 Verschlüsselung

Datenübertragung: TLS 1.3

Speicherung: Verschlüsselung at-rest gemäß den Standardmaßnahmen des Rechenzentrums; Session-Tokens gehasht (SHA-256)

5.2 Nachhaltigkeit und Transparenz

klimaneutraler Betrieb und Green-Coding-Standards bei der Softwareentwicklung

Quelloffenheit unter EUPL 1.2 – öffentliches Repository auf OpenCoDE

Diese TOM werden bei wesentlichen Änderungen der Architektur oder der eingesetzten Infrastruktur aktualisiert. Die jeweils aktuelle Fassung ist unter dieser URL abrufbar.

Softstack GmbH · Schiffbrückstraße 8 · 24937 Flensburg
hello@softstack.io