SCHOOLANIZER · DATENSCHUTZ

Anlage 1: Hosting, Unterauftragsverarbeiter und TOMs

Allgemeine technische und organisatorische Anlage zum AVV

Version 1.0 · Stand 26.05.2026

1. Zweck der Anlage

Diese Anlage beschreibt die allgemeinen technischen, organisatorischen und infrastrukturellen Rahmenbedingungen, unter denen die Hiller & Selig Technical Solutions GmbH personenbezogene Daten im Auftrag verarbeitet.

Sie ist produktübergreifend angelegt und kann für mehrere Produkte und Dienstleistungen verwendet werden. Produktspezifische Abweichungen oder Ergänzungen sind im jeweiligen Produktblatt festzuhalten.

2. Grundsätzliche Betriebsstruktur

Die Hiller & Selig Technical Solutions GmbH betreibt ihre Anwendungen und zugehörigen Dienste auf selbst administrierten Systemen innerhalb externer Infrastruktur. Zum allgemeinen Betriebsmodell gehören insbesondere:

- getrennte Systeme oder Dienste für Anwendung, Webserver, Datenbank, Administration, Mail, Objektspeicher und Systemüberwachung,
- eigene Härtung und Konfiguration der eingesetzten Systeme,
- getrennte administrative Zugangswege,
- technische und organisatorische Trennung produktiver und nicht produktiver Umgebungen,
- rollenbasierte Zugriffe auf Daten und Funktionen,
- getrennte Fachkomponenten für Hauptanwendung und Chat-/Kommunikationsdienste, soweit das jeweilige Produkt dies vorsieht.

3. Unterauftragsverarbeiter und externe Infrastruktur

3.1 Externe Infrastruktur und Hosting

Anbieter: Hetzner Online GmbH

Rolle: externer Infrastruktur- und Hosting-Dienstleister / Unterauftragsverarbeiter

Zweck: Bereitstellung der zugrunde liegenden Infrastruktur für den produktiven Betrieb

Speicherorte: Nürnberg, Falkenstein

Vertragliche Grundlage: AVV mit Hetzner besteht

Drittlandtransfer: nach aktuellem Kenntnisstand nicht beabsichtigt

> Die Hiller & Selig Technical Solutions GmbH administriert die auf der Hetzner-Infrastruktur betriebenen Server und Systeme selbst. Die Betriebsstruktur sieht getrennte technische Komponenten für Hauptanwendung, Weboberfläche, Kommunikationsdienste, Datenhaltung und dateibasierte Speicherkomponenten vor.

3.2 Objektspeicher / Dateiablagen

Anbieter: Google Cloud

Rolle: externer Speicher- oder Plattformdienst / Unterauftragsverarbeiter, soweit produktiv genutzt

Zweck: Speicherung von Anhängen, Avataren, Dokumenten, Materialien, Aufgabenabgaben, Terminanhängen und weiteren dateibasierten Inhalten

Technischer Rahmen: produktiver dateibasierter Speicher über Google-Objektspeicher im S3-kompatiblen Betriebsmodell

Vertragliche Grundlage: Google Cloud Data Processing Addendum wurde akzeptiert

Regionen: europe-west3 (Frankfurt, Deutschland); perspektivisch zusätzlich europe-west10 (Berlin, Deutschland)

3.3 Google Firebase / Google-Dienste

Anbieter: Google Ireland Ltd. / Google

Rolle: externer Infrastruktur- oder Plattformdienst / Unterauftragsverarbeiter, soweit produktiv genutzt

Zweck:

- Push-Benachrichtigungen über Firebase Cloud Messaging,
- mobile Push-Benachrichtigungen über Firebase Cloud Messaging und Apple Push Notification Service im iOS-Kontext,
- produktiv aktivierte Absturz- und Diagnosedaten über Firebase Crashlytics in der mobilen Haupt-App,
- gegebenenfalls weitere produktbezogene Google-Cloud-Komponenten, wenn diese später eingeführt und in Produktblättern konkretisiert werden.

Vertragliche Grundlage: Google Cloud Data Processing Addendum wurde akzeptiert

Besonderheit: Firebase Cloud Messaging ist produktiv aktiv; Apple Push Notification Service wird für iOS-Push mitgenutzt; Crashlytics ist produktiv aktiv

> Ob und in welchem Umfang einzelne Google-Dienste produktiv genutzt werden, ist im jeweiligen Produktblatt sowie im konkreten Betriebs-Setup zu dokumentieren.

4. Eigene Systeme des Auftragsverarbeiters

Die folgenden Komponenten werden als eigene, selbst administrierte Systeme betrieben und sind keine eigenständigen Unterauftragsverarbeiter:

- Anwendungs- und Webserver,
- Datenbanksysteme,
- Mailserver bzw. SMTP-Integration auf eigener Betriebsseite,
- Systeme zur Überwachung,
- Administrations- und Zugangsserver,
- eigene GitLab- oder vergleichbare Build- und Bereitstellungskomponenten,
- eigene Chat- und Realtime-Dienste, soweit diese im gleichen Verantwortungs- und Betriebsbereich liegen.

5. Allgemeine technische und organisatorische Maßnahmen

5.1 Zugriffsschutz und Administration

- rollenbasierte Zugriffe auf Daten und Funktionen,
- administrative Zugriffe nur für berechtigte Personen,
- getrennte administrative Oberflächen und interner Zugriffsschutz,
- keine unnötige direkte Exposition interner Verwaltungsdienste nach außen,
- abgesicherte interne Kommunikationswege zwischen Hauptanwendung und gekoppelten Backend-Diensten.

5.2 Authentifizierung und Rollen

- Authentifizierungsmechanismen für Nutzerkonten,
- rollenbasierte Berechtigungskonzepte,
- 2FA-Unterstützung für Nutzerkonten im Hauptsystem,
- Sitzungs- und Tokenverwaltung,
- getrennte Rollenmodelle für schulische Fachnutzer und technische Administrationskontexte.

5.3 Verschlüsselung und Schutz ruhender Daten

- TLS für Datenübertragung,
- verschlüsselte Übertragung zwischen Clients und Backend-Diensten,
- produktbezogene Datei- und Objektablagen über gesonderte Speicherpfade oder externe Speicherdienste,
- Schutz dateibasierter Inhalte außerhalb öffentlich erreichbarer Pfade, soweit lokal oder über Schnittstellen ausgeliefert,
- Backup- und Speicherkonzepte abhängig vom produktiven Betriebs-Setup ergänzbar.

5.4 Netzwerk- und Systemschutz

- Segmentierung und Trennung nach Systemfunktion,
- getrennte Dienste für Datenbank, Realtime, Queueing oder Chat, soweit verwendet,
- Konfiguration nur benötigter Dienste,
- laufende Systemhärtung und Konfiguration der Dienste,
- technische Überwachung der Dienste und interne Dienstgrenzen im Betriebsmodell.

5.5 Logging und Nachvollziehbarkeit

- technische System- und Serverlogs,
- produktbezogene Protokollierung im jeweils verfügbaren Umfang,
- Auth- und Audit-Logs für sicherheitsrelevante oder administrative Vorgänge,
- gesonderte Aufbewahrungslogik für Authentifizierungs-, Protokoll- und Löschdaten vorgesehen,
- eingeschränkter Zugriff auf Logs.

5.6 Backup, Wiederherstellung und Datenlebenszyklus

- Datenbank- und Betriebs-Backups laut Betriebs-Setup vorgesehen,
- gesonderte Aufbewahrungsmechanismen für bestimmte Protokoll- und Logdaten vorhanden,
- Löschprotokollierung für DSGVO-Löschungen vorhanden,

- dateibasierte Inhalte und Chat-Anhänge folgen produkt- und speicherabhängigen Löschlogiken,
- Daten werden nicht selektiv aus bestehenden Backups entfernt, sondern laufen über die jeweilige Backup-Rotation aus.

5.7 Nicht produktive Umgebungen

- Trennung von Produktion, Entwicklung und Test,
- nicht produktive Umgebungen mit separaten oder simulierten Diensten,
- nicht produktive Crash- und Diagnosedatenpfade können in einem stillen No-Op-Modus laufen, wenn produktive Zugangsdaten fehlen.

5.8 Änderungs- und Freigabeprozesse

- kontrollierte Build- und Freigabeprozesse,
- Rollback-Möglichkeiten im Rahmen des technischen Setups,
- produktive Konfigurations- und Secret-Verwaltung über getrennte Betriebsverfahren.

5.9 Sicherheitsvorfälle

- Unterstützung des Verantwortlichen bei Datenschutzvorfällen im Rahmen der Auftragsverarbeitung,
- gesonderte Sicherheits- und Audit-Dokumentation vorhanden,
- weiterer Ausbau formalisierter Vorfallsprozesse möglich und produktunabhängig fortführbar.

6. Produktbezogene Ergänzungen

Diese Anlage bildet die allgemeine technische und organisatorische Grundlage. Produktspezifisch zu ergänzen sind bei Bedarf insbesondere:

- konkrete Datenarten,
- konkrete Betroffenengruppen,
- Rollenmodelle,
- Export- und Downloadfunktionen,
- Archivierungslogiken,
- Chat- und Kommunikationsfunktionen,
- Push-, Diagnose- oder Drittplattformintegration,
- konkrete Nutzung externer Infrastruktur-, Plattform- oder Speicherdienste,
- konkrete produktive Provider und Speicherregionen.