

# Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

---

Zwischen

dem Kunden der Plattform YasaEdu – nachfolgend „Verantwortlicher“ genannt –  
und

yasa-it, vertreten durch Yazan Sadieh, Alhausstr. 6, 42281 Wuppertal – nachfolgend „Auftragsverarbeiter“  
genannt –

## § 1 Gegenstand, Dauer und Zweck der Verarbeitung

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen die cloudbasierte Software-as-a-Service-Plattform „YasaEdu“ zur Nutzung bereit. Im Rahmen der Vertragserfüllung verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen.

(2) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages.

## § 2 Art der Daten und Kreis der Betroffenen

(1) Kreis der Betroffenen: Kunden, Schüler sowie deren gesetzliche Vertreter (Eltern) des Verantwortlichen; Angestellte, freie Lehrkräfte (Tutoren/Freelancer) des Verantwortlichen.

(2) Art der personenbezogenen Daten: Stammdaten (Namen, Anschriften), Kontaktdaten (E-Mail, Telefon), Vertrags- und Abrechnungsdaten (Lektionen, Rechnungsbeträge, Bankverbindung), Leistungsdaten (Noten, Fächer, Lernfortschritte), visuelle & kryptografische Daten (digitale Signaturen nebst SHA-Prüfsummen).

## § 3 Pflichten des Auftragsverarbeiters

(1) Weisungsgebundenheit: Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen.

(2) Vertraulichkeit: Der Auftragsverarbeiter sichert zu, dass die von ihm mit der Verarbeitung der Daten betrauten Personen zur Vertraulichkeit verpflichtet wurden.

(3) Sicherheit: Der Auftragsverarbeiter setzt die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen um (siehe Anlage 1).

(4) Datenlöschung: Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter alle personenbezogenen Daten nach Ablauf einer Kulanfrist von drei Monaten nach Beendigung des Hauptvertrages unwiderruflich, es sei denn, gesetzliche Pflichten verbieten dies.

## § 4 Unterauftragsverhältnisse (Subunternehmer)

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter hinzuzuziehen.

(2) Zum Zeitpunkt des Abschlusses dieser Vereinbarung setzt der Auftragsverarbeiter folgende Unterauftragnehmer ein:

1. STRATO AG, Berlin – Zweck: Serverinfrastruktur (VPS) und Mailserver. Rechenzentren in Deutschland.

2. Hetzner Online GmbH, Gunzenhausen – Zweck: Optionale/Zukünftige Cloud-Infrastruktur. Rechenzentren in Deutschland.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen über jede Änderung bezüglich der

Unterauftragnehmer per E-Mail oder Systembenachrichtigung. Dem Verantwortlichen steht ein Widerspruchsrecht innerhalb von 14 Tagen aus wichtigen datenschutzrechtlichen Gründen zu.

## **§ 5 Kontrollrechte des Verantwortlichen**

- (1) Der Verantwortliche hat das Recht, die Einhaltung dieser Vereinbarung zu überprüfen. Der Auftragsverarbeiter stellt hierfür notwendige Nachweise (z. B. Sicherheitsdatenblätter, Zertifikate) bereit.
- (2) Eine physische Vor-Ort-Kontrolle ist nur nach rechtzeitiger Anmeldung (mindestens 4 Wochen im Voraus), während der regulären Geschäftszeiten und auf Kosten des Verantwortlichen zulässig.

## **Anlage 1: Technische und organisatorische Maßnahmen (TOM)**

### **1. Vertraulichkeit:**

- Zutrittskontrolle: Hosting in zertifizierten Hochsicherheits-Rechenzentren von Strato/Hetzner in Deutschland mit biometrischer Zugangskontrolle und 24/7-Überwachung.
- Zugangskontrolle: Administrativer Zugriff auf Server ausschließlich via verschlüsseltem SSH mit SSH-Keys. Passwort- und direkter Root-Login sind deaktiviert.
- Zugriffskontrolle: Striktes, rollenbasiertes Berechtigungskonzept in der Applikation (Administratoren, Lehrer, Schüler sehen jeweils nur ihre freigegebenen Datenbereiche).

### **2. Integrität:**

- Weitergabekontrolle: Verschlüsselte Datenübertragung über das HTTPS-Protokoll mit aktuellen TLS-Standards.
- Manipulationsschutz: Digitale Signaturen aus dem Frontend werden im Backend mittels SHA-Kryptoverfahren (Prüfsumme) untrennbar mit dem Dokument verknüpft.

### **3. Verfügbarkeit und Belastbarkeit:**

- Datensicherung: Automatisierte, tägliche und verschlüsselte Backups der Datenbanken auf getrennten Speichersystemen.
- Wiederherstellbarkeit: Infrastruktur-Deployment via Ansible-Playbooks zur schnellen und fehlerfreien Wiederherstellung auf alternativen Serverinstanzen.

### **4. Regelmäßige Überprüfung:**

- Automatisierte Pipelines für zeitnahe Einspielung von Sicherheitsupdates (Java, Spring Boot, Angular) und System-Hotfixes.