Vertrag zur Auftragsverarbeitung (AVV)

gemäß Art. 28 DSGVO

zwischen

_____ (Name der Schule / des Schulträgers)

_____ (Anschrift)

vertreten durch: _____

— nachfolgend **„Verantwortlicher"** —

und

KI-Macht-Lernen GmbH Frankenstraße 22, 71065 Sindelfingen Geschäftsführer: Dr. Robert Bahnsen E-Mail: robertbahnsen@ki-macht-lernen.de

— nachfolgend **„Auftragsverarbeiter"** —

— gemeinsam **„Parteien"** —

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen webbasierte Lern-Apps für den Schulunterricht bereit (nachfolgend „Dienst"). Der Verantwortliche nutzt den Dienst im Rahmen seines Bildungsauftrags.

(2) Gegenstand der Auftragsverarbeitung ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen, wie in **Anlage 1** näher beschrieben.

(3) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags (Nutzungsvertrag / Lizenzvertrag) zwischen den Parteien. Die Verarbeitung beginnt mit der Einrichtung der Kurse und endet mit der Kündigung des Hauptvertrags.

§ 2 Art und Zweck der Verarbeitung

(1) Art und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zum Zweck der Bereitstellung und des Betriebs der Lern-Apps, insbesondere:

- Authentifizierung und Zugangsverwaltung von Lehrkräften und Schülern
- Bereitstellung von Lerninhalten und interaktiven Übungen

- Betrieb eines KI-gestützten Tutors (soweit von der Lehrkraft aktiviert)
- Speicherung von Kurseinstellungen und Modulfreischaltungen
- Speicherung individueller Lernfortschritte und Lernstände (in Apps mit Lernbegleitung)
- Bereitstellung eines schulinternen, gemeinsamen Datenraums für Lehrkräfte derselben Schule (siehe Anlage 1, Abschnitt 6)

(2) Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt.

---

§ 3 Art der personenbezogenen Daten und Kategorien betroffener Personen

(1) Die Arten der verarbeiteten personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** festgelegt.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO ist **nicht Gegenstand** dieses Vertrags.

---

§ 4 Weisungsgebundenheit

(1) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO). Der Hauptvertrag und dieser AVV gelten als allgemeine Weisung. Einzelweisungen sind in Textform (E-Mail genügt) an info@ki-macht-lernen.de zu richten.

(2) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er nach seiner Auffassung eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften der Union oder der Mitgliedstaaten verstößt (Art. 28 Abs. 3 Satz 3 DSGVO).

---

§ 5 Vertraulichkeit

(1) Der Auftragsverarbeiter stellt sicher, dass sich die mit der Verarbeitung befassten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

(2) Die Vertraulichkeitspflicht besteht auch nach Beendigung dieses Vertrags fort.

---

§ 6 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft vor Beginn der Verarbeitung die in **Anlage 2** dargestellten technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO und hält diese während der Vertragslaufzeit aufrecht.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf alternative Maßnahmen umsetzen, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und dem Verantwortlichen auf Anfrage mitzuteilen.

---

§ 7 Unterauftragsverarbeitung

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die **allgemeine schriftliche Genehmigung**, Unterauftragsverarbeiter einzusetzen (Art. 28 Abs. 2 DSGVO). Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern. Der Verantwortliche kann gegen die Änderung innerhalb von **14 Tagen** nach Zugang der Mitteilung aus berechtigten datenschutzrechtlichen Gründen Einspruch erheben.

(3) Legt der Verantwortliche fristgerecht Einspruch ein und kann keine einvernehmliche Lösung gefunden werden, steht dem Verantwortlichen ein Sonderkündigungsrecht zum Zeitpunkt des geplanten Einsatzes des neuen Unterauftragsverarbeiters zu.

(4) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die dem Schutzniveau dieses Vertrags entsprechen (Art. 28 Abs. 4 DSGVO). Die jeweiligen Verträge mit den Unterauftragsverarbeitern werden dem Verantwortlichen auf Anfrage zur Einsicht bereitgestellt.

(5) Der Verantwortliche erkennt an, dass die in Anlage 3 genannten Unterauftragsverarbeiter Standard-DPAs nach eigener Vorlage verwenden, die typischerweise die Anforderungen von Art. 28 DSGVO erfüllen. Der Auftragsverarbeiter prüft bei der Auswahl eines Unterauftragsverarbeiters dessen DSGVO-Konformität und dokumentiert dies.

---

§ 8 Rechte der betroffenen Personen

(1) Soweit möglich, unterstützt der Auftragsverarbeiter den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflichten nach Art. 12–22 DSGVO (Betroffenenrechte).

(2) Wendet sich eine betroffene Person mit einem Antrag nach Art. 15–21 DSGVO — d. h. Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17), Einschränkung der Verarbeitung (Art. 18), Mitteilungspflicht bei Berichtigung/Löschung/Einschränkung (Art. 19), Datenübertragbarkeit (Art. 20) oder

Widerspruch gegen die Verarbeitung (Art. 21) — direkt an den Auftragsverarbeiter, leitet dieser den Antrag unverzüglich an den Verantwortlichen weiter.

§ 9 Meldung von Datenschutzverletzungen

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen **unverzüglich** (spätestens innerhalb von **48 Stunden**) nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 2 DSGVO).

(2) Die Meldung enthält mindestens: - Beschreibung der Art der Verletzung - Betroffene Datenkategorien und ungefähre Anzahl der betroffenen Personen - Wahrscheinliche Folgen der Verletzung - Ergriffene oder vorgeschlagene Maßnahmen

(3) Die Meldung erfolgt an: _____ (Kontaktperson des Verantwortlichen)

§ 10 Unterstützung bei Folgenabschätzung und Konsultation

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung seiner Pflichten aus Art. 35 DSGVO (Datenschutz-Folgenabschätzung) und Art. 36 DSGVO (vorherige Konsultation).

§ 11 Löschung und Rückgabe personenbezogener Daten

(1) Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter sämtliche personenbezogenen Daten, die im Auftrag des Verantwortlichen verarbeitet wurden, innerhalb von **90 Tagen** bei Schul-Lizenz- und Klassen-Abo-Verträgen bzw. **30 Tagen** bei Eltern-Abos (AGB § 10 Abs. 2a für Schul-Lizenzen, Abs. 3a für Klassen-Abos, Abs. 1a für Eltern-Abos), es sei denn, eine längere Speicherung ist nach Unionsrecht oder dem Recht der Mitgliedstaaten vorgeschrieben. Die längere Frist für Schul-Lizenz- und Klassen-Abo-Verträge trägt schulischen Ferienzeiten und etwaigem Verwaltungs-Vorlauf der Schulleitung Rechnung.

(2) Auf Verlangen des Verantwortlichen gibt der Auftragsverarbeiter die Daten vor der Löschung in einem gängigen, maschinenlesbaren Format zurück.

(3) Der Auftragsverarbeiter bestätigt die Löschung auf Anfrage schriftlich.

§ 12 Kontroll- und Auditrechte

(1) Der Verantwortliche hat das Recht, die Einhaltung dieses Vertrags zu überprüfen, einschließlich durch Inspektionen vor Ort oder Audits (Art. 28 Abs. 3 lit. h DSGVO). Inspektionen sind mit einer Frist von **4 Wochen** vorab anzukündigen.

(2) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

(3) Aktuelle Zertifizierungen oder Audit-Berichte (z.B. SOC 2 der Unterauftragsverarbeiter) können als Nachweis anstelle einer Vor-Ort-Inspektion akzeptiert werden.

§ 13 Haftung

Die Haftung der Parteien richtet sich nach den gesetzlichen Vorschriften, insbesondere Art. 82 DSGVO.

§ 14 Schlussbestimmungen

(1) Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform.

(3) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

(4) Ergänzend zu diesem AVV und dem Hauptvertrag gelten die Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters (KIM-Suite-AGB, abrufbar unter https://ki-macht-lernen.de/agb.html) als Bestandteil des Vertragsverhältnisses zwischen den Parteien. Soweit Bestimmungen dieses AVV von den Allgemeinen Geschäftsbedingungen oder dem Hauptvertrag abweichen oder ihnen widersprechen, haben die Regelungen dieses AVV Vorrang, insbesondere soweit sie den Schutz personenbezogener Daten betreffen.

(5) **Abschluss und Form.** Für diesen AVV nach Art. 28 DSGVO genügt die Textform (§ 126b BGB); eine qualifizierte elektronische Signatur ist nicht erforderlich. Der AVV wird gemeinsam mit dem Hauptvertrag geschlossen: Beim Abschluss des Schulvertrags im Schul-Verwaltungsportal des Auftragsverarbeiters bestätigt die zeichnungsberechtigte Person der Schule die Zustimmung zu diesem AVV in seiner jeweils aktuellen Fassung elektronisch im Abschlussvorgang; alternativ wird dieser AVV als Dokument ausgefüllt und in Textform bestätigt. Beide Parteien können die geschlossene Fassung archivieren.

Unterschriften

Für den Verantwortlichen (Schule):	Für den Auftragsverarbeiter:
Ort, Datum	Ort, Datum
Name, Funktion	Dr. Robert Bahnsen, Geschäftsführer KI-Macht-Lernen GmbH
Unterschrift	Unterschrift

Anlage 1: Gegenstand der Verarbeitung

1. Zweck der Verarbeitung

Bereitstellung und Betrieb webbasierter Lern-Apps für den Schulunterricht (fachübergreifend, mit Schwerpunkt Chemie und Physik) einschließlich eines fächerübergreifenden, optionalen KI-gestützten Tutors.

2. Art der Verarbeitung

- Erhebung und Speicherung von Anmeldedaten (Lehrkräfte und ggf. Schüler)
- Authentifizierung von Schülern über Kurscode und Passwort (anonymer Zugang) oder über individuelle Benutzerkonten (E-Mail + Passwort bzw. temporäres Erst-Passwort, das beim ersten Login geändert werden muss)
- Anlage eines Kind-Accounts durch die Eltern im Rahmen des Eltern-Abos und Versand eines temporären Erst-Passworts an die Kind-E-Mail-Adresse
- Speicherung von Kurseinstellungen und Modulfreischaltungen
- Speicherung individueller Lernfortschritte (in Apps mit Lernbegleitung)
- Verarbeitung von Schüler-Eingaben im KI-Chat (in Apps mit KI-Tutor)
- Speicherung von Chat-Nachrichten und Schüler-Anhängen (Bilder, PDFs) während der Laufzeit einer Lern-Session
- Erzeugung und Verwaltung App-spezifischer Zugangslinks (UUID-Token) durch die Lehrkraft, die ohne eigenen Schüler-Account verwendet werden können (zum Beispiel im Säure-Base-Trainer für volljährige Schülerinnen und Schüler zur Abitur-Vorbereitung; bei diesem App-Typ erfolgt keine Speicherung des Chat-Verlaufs)

- Protokollierung von KI-Nutzung zu Abrechnungszwecken (anonymisiert)
- Versand vertragsbezogener und transaktionaler E-Mails (z. B. Lehrer-Einladung, Erst-Passwort, Lizenz-Hinweise) primär über Resend (Plus Five Five, Inc., USA) mit aktivierter „Enforce TLS"-Domain-Einstellung; bei Ausfall der primären Versandstrecke automatischer Fallback auf IONOS SMTP (Deutschland) mit STARTTLS-Aushandlung
- Sofern der Hauptvertrag über den Online-Bezahldienst des Auftragsverarbeiters abgerechnet wird: Übermittlung von Vertragspartner-Daten (Name und Anschrift der zeichnungsberechtigten Person, Schulanschrift, ggf. USt-IdNr.) an die Stripe Payments Europe Ltd. zur Rechnungsstellung. Schülerdaten werden in keinem Fall an Stripe übermittelt.

3. Kategorien betroffener Personen

Kategorie	Beschreibung
Lehrkräfte	Lehrerinnen und Lehrer, die Kurse erstellen und verwalten
Schülerinnen und Schüler	Lernende, die über Kurscode (anonym) oder über individuelle Benutzerkonten auf die Apps zugreifen (ca. 15–19 Jahre)

4. Arten personenbezogener Daten

Lehrkräfte

Datenkategorie	Erhoben?	Anmerkung
E-Mail-Adresse	Ja	Für Authentifizierung (Clerk)
Klar-Name (Vor- und Nachname)	**Nein**	Wird nicht erhoben — Datensparsamkeit nach Art. 5 Abs. 1 lit. c DSGVO
Benutzername / Kürzel	Ja, optional	Bei Bedarf zur Anzeige in der App (z. B. Lehrer-Kürzel in der Raumbuchung)
Kurs-Zugehörigkeit	Ja	Erstellte Kurse und Einstellungen
Schul-Zugehörigkeit	Ja	Mandantentrennung über `school_id`
IP-Adresse	Ja	Server-Logs (automatisch)
Nutzungsdaten	Ja	Anzahl KI-Anfragen (Abrechnung)

Schülerinnen und Schüler

Je nach App gibt es zwei Zugangsmodelle:

Modell A — Anonymer Zugang (z. B. KI-Lernassistent): Schüler greifen über einen Kurscode und ein Kurspasswort zu, ohne individuelles Konto.

Datenkategorie	Erhoben?	Anmerkung
Name	**Nein**	Kein individuelles Konto
E-Mail-Adresse	**Nein**	Zugang nur über Kurscode + Passwort
Alter / Geburtsjahr	**Nein**	Wird nicht erhoben
Kurs-Zugehörigkeit	Ja	Nur Kurscode
IP-Adresse	Ja	Server-Logs (automatisch)
KI-Chat-Eingaben	Ja	Gespeichert während Session-Laufzeit; bei Anthropic: Zero Data Retention
Chat-Anhänge (Bilder, PDFs)	Ja	Gespeichert während Session-Laufzeit
Nutzungsdaten	Ja	Anzahl KI-Anfragen (anonymisiert)

Modell B — Individueller Zugang (z. B. Vokabeltrainer): Schüler registrieren sich mit E-Mail-Adresse und Passwort und erhalten ein eigenes Benutzerkonto. Im Rahmen des Eltern-Abos können auch die Eltern den Kind-Account anlegen; das initiale Erst-Passwort wird an die Kind-E-Mail-Adresse versandt und ist beim ersten Login zwingend zu ändern.

Datenkategorie	Erhoben?	Anmerkung
E-Mail-Adresse	Ja	Für Authentifizierung (Clerk)
Klar-Name (Vor- und Nachname)	**Nein**	Wird nicht erhoben — Datensparsamkeit nach Art. 5 Abs. 1 lit. c DSGVO
Benutzername	Ja, optional	Bei Bedarf für Anzeige; kein Klar-Name
Kurs-/Klassenzugehörigkeit	Ja	Zuordnung zu Lehrkraft-Klassen
Lernfortschritt	Ja	Gelernte Fachbegriffe, Übungsergebnisse, Lernlevel
KI-Chat-Verläufe	Ja, soweit aktiviert	Gespeichert während der Laufzeit der Lern-Session bzw. des Projekts
IP-Adresse	Ja	Server-Logs (automatisch)

Hinweise: - **Datensparsamkeit (Modell A und B):** Der Auftragsverarbeiter erhebt und speichert **grundsätzlich keine Klar-Namen (Vor- oder Nachnamen) von Schülern**. Die Authentifizierung erfolgt entweder anonym über Kurscode (Modell A) oder über E-Mail-Adresse plus Benutzernamen (Modell B). Trägt eine Schule oder ein Schulträger nach eigener Namens-Konvention Vor- und/oder Nachnamen im lokalen Teil der E-Mail-Adresse (z. B. `vorname.nachname@schule.de`), so liegt dies in

der Verantwortung des Verantwortlichen. - **Modell A:** Schüler werden nicht namentlich erfasst. Es werden weder Alter noch Geburtsjahr erhoben. Die Lehrkraft trägt die Verantwortung für den altersgerechten Einsatz der KI-gestützten Lernhilfen im Unterricht. Chat-Nachrichten und Anhänge werden automatisch gelöscht (Schnell-Sessions: 24 Stunden, Projekt-Sessions: 14 Tage nach Ende). Lehrkräfte können Chat-Verläufe und Anhänge einsehen (pädagogische Begleitung/Aufsichtspflicht). - **Modell B:** Lehrkräfte können den individuellen Lernfortschritt ihrer Schüler einsehen (pädagogische Begleitung und gezielte Förderung). Es werden keine Noten gespeichert.

5. Dauer der Verarbeitung

(1) Die Verarbeitung entspricht grundsätzlich der Laufzeit des Hauptvertrags. Nach Kündigung des Hauptvertrags werden alle Daten gelöscht — bei Schul-Lizenz- und Klassen-Abo-Verträgen innerhalb von **90 Tagen**, bei Eltern-Abos innerhalb von **30 Tagen** (siehe § 11 sowie Absatz 2 dieses Abschnitts).

(2) Wird die Lern-App im Rahmen eines **Eltern-Abos** zur KIM-Suite (Privatkunden-Vertrag der Eltern mit dem Auftragsverarbeiter) genutzt und ist der Schüler-Account einer Klasse oder einem Kurs der Schule zugeordnet, so gelten zusätzlich die Aufbewahrungsfristen der Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters (KIM-Suite-AGB, Stand 07.06.2026): Nach Storno des Eltern-Abos werden Kind-Account-Daten (Lernfortschritte, KI-Chat-Verläufe) **30 Tage** lang aufbewahrt und anschließend gelöscht (AGB § 10 Abs. 1a). Für schul- bzw. klassenlizenzierte Schüler-Daten beträgt die analoge Aufbewahrungsfrist nach Vertragsende **90 Tage** (AGB § 10 Abs. 2a für Schul-Lizenzen bzw. Abs. 3a für Klassen-Abos).

6. Schulinterner gemeinsamer Datenraum für Lehrkräfte (interner Datenfluss)

(1) Für mehrere Lern-Apps (insbesondere ChemBuddy und PhysBuddy) führt der Auftragsverarbeiter pro Schule einen **gemeinsamen schulinternen Datenraum** für Lehrkräfte derselben Schule (technisch realisiert als Tabellen `cb_school_terms` bzw. `pb_school_terms` mit Mandantentrennung über `school_id`).

(2) In diesem Datenraum gilt für Lehrkräfte derselben Schule eine **Lese-Berechtigung für alle Einträge** der eigenen Schule und eine **Schreib- und Änderungs-Berechtigung ausschließlich für selbst erstellte Einträge** (technische Umsetzung via Row Level Security, Art. 32 DSGVO). Lehrkräfte anderer Schulen haben keinerlei Zugriff auf diese Daten.

(3) Inhalte dieses Datenraums sind ausschließlich **Lehrmaterialien** (z. B. Fach-Vokabeln, Karteikarten-Sets, Modul-Konfigurationen). **Personenbezogene Schülerdaten werden in diesem schulinternen Datenraum nicht verarbeitet.** Verfasser-Information (`created_by`) eines Eintrags ist die interne Lehrkraft-Kennung — nicht der Klar-Name.

(4) Der Datenraum dient ausschließlich der pädagogischen Zusammenarbeit innerhalb der Schule (Bildungsauftrag des Verantwortlichen) und ist Bestandteil der vom Verantwortlichen erteilten Verarbeitungs-Weisung.

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

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

Maßnahme	Umsetzung
Zutrittskontrolle	Cloud-Infrastruktur bei zertifizierten Anbietern (ISO 27001, SOC 2)
Zugangskontrolle	Authentifizierung über Clerk (MFA verfügbar); API-Keys ausschließlich serverseitig; JWT-basierte Session-Authentifizierung (Clerk → Supabase, HS256-signiert)
Zugriffskontrolle	Row Level Security (RLS) in der Datenbank (PostgreSQL); Lehrkräfte sehen nur eigene Kurse, Schüler nur eigene Lerndaten
Trennungskontrolle	Mandantentrennung pro Schule über `school_id`-Fremdschlüssel und RLS-Policies; separate Kurs- und Schul-Datenräume
Verschlüsselung Transit	TLS 1.2+ für sämtliche Verbindungen zwischen Browser, Edge Functions und Datenbank. Versand transaktionaler E-Mails primär über Resend mit aktivierter „Enforce TLS"-Domain-Einstellung (Resend setzt TLS 1.3+ ein und unterbindet den Versand, wenn der Empfänger-Mailserver keine TLS-gesicherte Verbindung anbietet); Fallback-Versand über IONOS mit STARTTLS-Aushandlung nach RFC 3207
Verschlüsselung at Rest	Festplattenverschlüsselung auf Datenbank- und Storage-Ebene bei Supabase (AES-256)
Passwort-Sicherheit	Kurs-Passwörter mit bcrypt gehasht (pgcrypto); Benutzer-Passwörter werden ausschließlich vom Identity Provider Clerk gespeichert (bcrypt/scrypt); Erst-Passwörter für Kind-Accounts und neue Lehrkräfte sind 12-stellig und müssen beim ersten Login geändert werden

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

Maßnahme	Umsetzung
Eingabekontrolle	Server-seitige Validierung aller Eingaben; CORS-Beschränkung auf autorisierte Domains
Weitergabekontrolle	Keine Weitergabe personenbezogener Schülerdaten an Dritte; Zero Data Retention bei KI-Anbieter (Anthropic)
Brute-Force-Schutz	Max. 5 Fehlversuche pro Kurscode in 15 Minuten
Rate Limiting	Max. 30 KI-Anfragen pro Stunde pro Nutzer

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO)

Maßnahme	Umsetzung
Hosting	Netlify (CDN, DDoS-Schutz), Supabase (automatische Backups)
Wiederherstellbarkeit	Tägliche automatische Datenbank-Backups bei Supabase

4. Regelmäßige Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

Maßnahme	Umsetzung
Sicherheitsüberprüfung	Regelmäßige Prüfung der Abhängigkeiten (npm audit), Dependency-Updates
Zertifizierungen Unterauftragsverarbeiter	Clerk: SOC 2 Type II, DPF-zertifiziert; Supabase: SOC 2 Type II; Anthropic: SOC 2 Type II

Anlage 3: Unterauftragsverarbeiter

Der Auftragsverarbeiter setzt folgende Unterauftragsverarbeiter ein:

Unterauftragsverarbeiter	Sitz	Zweck	Transfer-Mechanismus	Zertifizierungen
Clerk, Inc.	USA	Authentifizierung und Nutzerverwaltung (Lehrkräfte)	EU-US DPF + SCCs	SOC 2 Type II, DPF
Supabase, Inc.	USA	Datenbank (Kursdaten, Einstellungen)	SCCs	SOC 2 Type II
Anthropic, PBC	USA	KI-Tutor (Chat-Verarbeitung, Zero Data Retention)	SCCs	SOC 2 Type II
Netlify, Inc.	USA	Hosting der Web-App, Serverless Functions	EU-US DPF + SCCs	DPF
Plus Five Five, Inc. (d/b/a Resend)	USA	Versand transaktionaler E-Mails (primär)	SCCs (Modul 2, Bestandteil der Resend-ToS / DPA: https://resend.com/legal/dpa)	SOC 2 Type II
Amazon Web Services, Inc.	USA	Resend-Subprozessor: Hosting und Versand-Infrastruktur	Abgedeckt über Resend-DPA (vollständige Resend-Subprozessoren-Liste: https://resend.com/legal/subprocessors)	SOC 2, ISO 27001
IONOS SE	Deutschland	DNS, Domain-Verwaltung, Mail-Empfang, Versand transaktionaler E-Mails (SMTP-Fallback)	— (EU)	ISO 27001
Stripe Payments Europe Ltd. *(nur falls per Stripe abgerechnet)*	Irland (EU)	Zahlungsabwicklung der Lizenzgebühr, Rechnungsstellung an die Schule	DSGVO (EU); SCCs für Konzern-Datenflüsse zur US-Konzernmutter	SOC 2, EU-US DPF (Konzern)

Hinweis zu Anthropic (KI-Tutor): Die Verarbeitung erfolgt mit **Zero Data Retention (ZDR)**. Schüler-Eingaben im KI-Chat werden von Anthropic nicht gespeichert und nicht zum Training von KI-Modellen verwendet. Es erfolgt keine dauerhafte Speicherung personenbezogener Daten bei Anthropic.

Hinweis zu Stripe (Zahlungsabwicklung): Stripe wird nur eingesetzt, wenn der Hauptvertrag über den Online-Bezahldienst des Auftragsverarbeiters abgerechnet wird (Alternative: manuelle Rechnungsstellung). An Stripe übermittelt werden ausschließlich Vertragspartner-Daten der Schule (Name und Anschrift der zeichnungsberechtigten Person, Schulanschrift, ggf. USt-IdNr.) sowie Zahlungsmittel-

Daten, die direkt im Stripe-Checkout eingegeben werden. **Daten der Schülerinnen und Schüler werden in keinem Fall an Stripe übermittelt.**

Stand: 07.06.2026