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 sowie ergänzende Organisations-Apps für den Schulbetrieb (z. B. Raumbuchung für Räume und Geräte, Anmeldung zu schulischen Betreuungsangeboten, Projektwahl und -zuteilung, Planung von Veranstaltungen mit Wahlangeboten, Bestell- und Rückmeldelisten) sowie Werkzeuge zur Unterrichtsdokumentation für Lehrkräfte (z. B. Sitzplan mit Notizen zur mündlichen Beteiligung und zur Anwesenheit) bereit (nachfolgend zusammen „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 (Schulvertrag, auch bei Bestellung über eine Schul-App-Plattform, oder Klassen-Abo). Schaltet der Verantwortliche den Dienst auf einer von ihm eingesetzten Schul-App-Plattform für seine Lehrkräfte sowie Schülerinnen und Schüler frei, ohne dass ein Lizenzvertrag besteht (kostenfreier Zugang, Probephase), so dauert die Verarbeitung, solange die Freischaltung besteht; sie endet mit deren Rücknahme, spätestens mit der Löschung nach Anlage 1 Abschnitt 5 Abs. 0d. Die Verarbeitung beginnt mit der ersten Anmeldung oder der Einrichtung von Kursen.

§ 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 und ergänzenden Organisations-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)
- Verwaltung und Buchung schulischer Räume und Geräte durch Lehrkräfte (Organisations-App Raumbuchung; siehe Anlage 1)
- Planung schulischer Veranstaltungen mit Wahlangeboten (Projekt-, Studien- und Fortbildungstage, Tagungen): Wahl der Teilnehmenden, Verteilung auf Tage und Zeitblöcke, persönlicher Plan — auch für Lehrkräfte und externe Gäste als Teilnehmende (siehe Anlage 1, Abschnitt 4, Modell C)
- Dokumentation von Unterrichtsbeobachtungen durch die Lehrkraft (Sitzordnung, Notizen zur mündlichen Beteiligung, Anwesenheitsnotizen); die Zuordnung dieser Notizen zu den Namen der Schülerinnen und Schüler speichert der Auftragsverarbeiter ausschließlich verschlüsselt und kann sie nicht auflösen (siehe Anlage 1, Abschnitt 4, Modell D)
- Anlage und Führung pseudonymer Benutzerkonten bei Anmeldung über einen Identitätsdienst der Schule sowie Übernahme der dort gepflegten Gruppen als Klassen (siehe Anlage 1, Abschnitt 7)

(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 Zweck** dieses Vertrags und wird vom Auftragsverarbeiter weder angestrebt noch ausgewertet.

(3) In einzelnen Organisations-Apps stellt der Auftragsverarbeiter Freitextfelder bereit, deren Inhalt allein der Verantwortliche bestimmt (z. B. die Begründung, warum zwei Schüler nicht derselben Gruppe zugeteilt werden sollen, oder ein Notizfeld zu einem Sonderstatus). Trägt der Verantwortliche dort Angaben ein, die unter Art. 9 Abs. 1 DSGVO fallen, verarbeitet der Auftragsverarbeiter sie im

Rahmen dieses Vertrags mit; die Entscheidung darüber und die Prüfung ihrer Zulässigkeit liegen beim Verantwortlichen. Der Auftragsverarbeiter empfiehlt, solche Felder auf das für den Zweck Erforderliche zu beschränken und auf Angaben zu Gesundheit oder vergleichbare Kategorien zu verzichten.

(4) In der Betreuungsanmeldung stammt der Inhalt eines Freitextfeldes nicht vom Verantwortlichen, sondern von den **Erziehungsberechtigten selbst** (Mitteilungen zum Kind, etwa ein Geschwisterkind, der Schulbus oder eine Allergie). Der Auftragsverarbeiter weist im Formular darauf hin, dass die Mitteilung ausschließlich den betreuenden Lehrkräften zugänglich ist, und beschränkt die Länge des Feldes. Absatz 3 gilt entsprechend: Über die Zulässigkeit der dort gemachten Angaben entscheidet der Verantwortliche im Rahmen seiner Aufgabe.

---

§ 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 unterschrit-

ten 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. Für Konten, die ohne Lizenzvertrag über einen Identitätsdienst des Verantwortlichen entstanden sind, gilt die Frist aus Anlage 1 Abschnitt 5 Abs. 0d.

(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. Setzt der Verantwortliche eine Schul-App-Plattform ein, auf deren Angebotsseite dieser AVV hinterlegt ist, so kommt der AVV in der dort hinterlegten Fassung zustande, sobald der Verantwortliche den Dienst auf der Plattform für seine Lehrkräfte sowie Schülerinnen und Schüler freischaltet; er gilt auch für eine spätere Bestellung über die Plattform. In beiden Fällen kann dieser AVV alternativ oder zusätzlich als Dokument ausgefüllt und in Textform bestätigt werden. Beide Parteien können die geschlossene Fassung archivieren.

Unterschriften

Wird dieser AVV nach § 14 Abs. 5 im Abschlussvorgang des Schul-Verwaltungsportals oder durch die Freischaltung auf einer Schul-App-Plattform geschlossen, ist keine Unterschrift erforderlich. Die folgenden Felder sind nur für den Abschluss als ausgefülltes Dokument bestimmt.

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 sowie ergänzender Organisations-Apps für den Schulbetrieb (z. B. Raumbuchung für Räume und Geräte, Anmeldung zu schulischen Betreuungsangeboten, Projektwahl und -zuteilung, Planung von Veranstaltungen mit Wahlangeboten, Bestell- und Rückmeldelisten, Rückmeldungen aus dem Unterricht, Inventarverwaltung schulischer Sammlungen) sowie von Werkzeugen zur Unterrichtsdokumentation für Lehrkräfte (Sitzplan mit Notizen zur mündlichen Beteiligung und zur Anwesenheit).

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, zu dessen Änderung beim ersten Login aufgefordert wird)
- Anlage eines Kind-Accounts durch die Eltern im Rahmen des Eltern-Abos und Versand eines temporären Erst-Passworts an die Kind-E-Mail-Adresse
- Anlage pseudonymer Benutzerkonten bei Anmeldung über einen Identitätsdienst der Schule (pseudonyme Kennung, Pseudonym als Anzeigename, Rolle, Schule, Gruppen), Übernahme der Gruppen als Klassen sowie Rückmeldung an den Identitätsdienst, ob ein Zugang besteht (Abschnitt 7)
- 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)
- Speicherung von Raum- und Geräte-Buchungen der Lehrkräfte in der Organisations-App Raumbuchung (Datum, Zeitslot, Raum bzw. Gerät, optionale Beschreibung, Lehrer-Kürzel); der per QR-Code am Raum abrufbare Belegungsstatus ist anonym und enthält keine personenbezogenen Daten
- Speicherung von Inhalten, die Schülerinnen und Schüler in kollaborativen Lern-Apps selbst beitragen (Sachinformationen zu Unterrichtsgegenständen mit Pflicht-Quellenangabe). Im anonymen Sitzungsbetrieb ohne Personenbezug; im angemeldeten Klassenbetrieb mit Zuordnung zum Benutzerkonto der beitragenden Person, damit die Lehrkraft ihrer Moderationsaufgabe nachkommen kann (siehe Anlage 1 Abschnitt 6 B)
- Namentliche Verwaltung in Organisations-Apps, soweit der Name Zweck der Anwendung ist: Anmeldung zu Betreuungsangeboten (Kind, Erziehungsberechtigte, Kontaktdaten, Betreuungstage, daraus abgeleitete Raumzuteilung, tagesbezogene Anwesenheit einschließlich des Grundes einer Abwesenheit, Nachweis der von den Betreuungskräften gehaltenen Nachmittage sowie eine freiwillige Mitteilung der Erziehungsberechtigten im Freitextfeld des Anmeldeformulars), Projektwahl und -zuteilung (Klassenlisten, Wünsche, Zuteilungen, Anwesenheit und Fehlzeiten, Einverständniserklärungen als Datei-Upload), Planung von Veranstaltungen mit Wahlangeboten (Teilnehmerliste mit Name und Gruppe, persönlicher Zugangslink, Wünsche, Zuteilung zu Angeboten und Zeitblöcken; eine E-Mail-Adresse nur, soweit angegeben, für den Versand des Zugangslinks und des persönlichen Plans; Teilnehmende können neben Schülerinnen und Schülern auch Lehrkräfte und externe Gäste sein, Letztere auch über eine offene Anmeldung mit Veranstaltungscode), Bestell- und Rückmeldelisten (Klassenliste, persönliche Zugangs-PIN, Rückmeldung Ja/Nein)
- Verwaltung der eingesetzten Betreuungs- und Projektleitungspersonen sowie der Referentinnen und Referenten einer Veranstaltung (Name, Kontaktdaten, Einsatzzeiten bzw. Verfügbarkeit, Abrechnungsgrundlage) — auch soweit diese nicht dem Kollegium des Verantwortlichen angehören
- Erfassung von Rückmeldungen aus dem Unterricht: Antworten von Schülerinnen und Schülern auf Fragen der Lehrkraft, **von ihnen mit dem Finger oder Stift angefertigte Zeichnungen** sowie eine automatisch (KI-gestützt) erzeugte Rückmeldung zu diesen Antworten. Der Zugang erfolgt entweder pseudonym über ein selbst gewähltes Kürzel ohne Konto oder über das individuelle Benutzerkonto; die Lehrkraft sieht die Rückmeldungen ihrer Klasse
- Führung eines Inventars schulischer Sammlungen: Räume, Schränke und Geräte mit Bezeichnung, Zustand, Prüfdatum und Fotos **der Geräte**, dazu optional ein Vermerk, wer ein Gerät für den Unterricht reserviert hat. Personenbezogene Daten von Schülerinnen und Schülern entstehen dabei nicht
- Dokumentation von Unterrichtsbeobachtungen durch die Lehrkraft: Sitzordnung (Raum und Platz), Notizen zur mündlichen Beteiligung (Zeitpunkt, Platz, Art des Beitrags — gemeldet,

aufgerufen oder Sorgfalt beim Arbeiten — sowie eine Wertung der Lehrkraft) und Anwesenheitsnotizen (anwesend, fehlt, verspätet mit Ankunftszeit). Die Notizen werden ausschließlich unter einer **Nummer** gespeichert; die Zuordnung der Nummer zum Namen liegt beim Auftragsverarbeiter nur **verschlüsselt** und ist für ihn nicht auflösbar (siehe Anlage 2 Nr. 1). **Fotos der Schülerinnen und Schüler werden nicht an den Auftragsverarbeiter übermittelt** und verbleiben auf dem Endgerät der Lehrkraft. Die Anwesenheitsnotiz ersetzt kein Fehlzeitensystem; sie dient allein dem Nachtragen im führenden System des Verantwortlichen

- Protokollierung fehlgeschlagener Zugriffsversuche in Organisations-Apps zur Missbrauchsabwehr (je Anwendung: IP-Adresse und Zeitpunkt oder der eingegebene Name mit Klasse und Fehlermeldung); bei offenen Anmeldungen zu Veranstaltungen zusätzlich IP-Adresse und Zeitpunkt jedes Anmeldeversuchs zur Begrenzung der Anmeldungen je Anschluss
- 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 — in der Unterrichtsdokumentation der Lehrkraft (Modell D) ohne eigenen Zugang. **Altersspanne ca. 10–19 Jahre** — die Lern-Apps decken die Klassenstufen 5 bis 13 ab, die Betreuungsangebote der Organisations-Apps beginnen in Klasse 5
Erziehungsberechtigte	Nur in Organisations-Apps mit Anmeldeverfahren (Name, Kontaktdaten, Bestätigung der Betreuungsvereinbarung)
Betreuungs- und Projektleitungspersonen	Personen, die ein Betreuungsangebot, ein Projekt oder ein Angebot einer Veranstaltung des Verantwortlichen durchführen (auch Referentinnen und Referenten) — auch externe, nicht dem Kollegium angehörende Personen (Name, Kontaktdaten, Einsatzzeiten bzw. Verfügbarkeit)
Teilnehmende schulischer Veranstaltungen	Nur in Organisations-Apps zur Veranstaltungsplanung (Modell C): Schülerinnen und Schüler, Lehrkräfte und externe Gäste, die an einer vom Verantwortlichen geplanten Veranstaltung teilnehmen

4. Arten personenbezogener Daten

Lehrkräfte

Datenkategorie	Erhoben?	Anmerkung
E-Mail-Adresse	Ja	Für Authentifizierung (Clerk). Bei Anmeldung über den Identitätsdienst der Schule (Abschnitt 7) entfällt sie; das Konto trägt eine technische, nicht zustellbare Adresse und kein Passwort
Klar-Name (Vor- und Nachname)	**Nein**, Ausnahme Modell C	Wird für das Konto nicht erhoben — Datensparsamkeit nach Art. 5 Abs. 1 lit. c DSGVO. Nimmt eine Lehrkraft an einer Veranstaltung teil, die mit einer Organisations-App geplant wird, führt der Verantwortliche ihren Namen dort wie den aller Teilnehmenden (Modell C)
Benutzername / Kürzel	Ja, optional	Bei Bedarf zur Anzeige in der App (z. B. Lehrer-Kürzel in der Raumbuchung)
Pseudonyme Kennung und Pseudonym des Identitätsdienstes	Ja, nur bei Anmeldung über den Identitätsdienst	Die Kennung gilt nur gegenüber dem Auftragsverarbeiter; das Pseudonym dient als Anzeigename
Kurs-Zugehörigkeit	Ja	Erstellte Kurse und Einstellungen
Raum-/Geräte-Buchungsdaten	Ja (nur Raumbuchung)	Datum, Zeitslot, Raum bzw. Gerät, optionale Beschreibung; für Lehrkräfte derselben Schule einsehbar
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 vier Zugangsmodelle: zwei in den Lern-Apps (A anonym, B individuell), eines in den Organisations-Apps (C namentlich) und eines in der Unterrichtsdokumentation der Lehrkraft (D pseudonym, ohne eigenen Zugang der Schülerinnen und Schüler).

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
Selbst gewähltes Kürzel bzw. Anzeigename	Ja, nur Rückmelde-Apps und Quiz	Pseudonym, von der Schülerin oder dem Schüler selbst gewählt; ermöglicht der Lehrkraft die Zuordnung im Unterricht, ohne dass ein Konto entsteht
Antworten, handschriftliche Zeichnungen, automatische Rückmeldung	Ja, nur Rückmelde-Apps und Quiz	Antworten auf Fragen der Lehrkraft, mit Finger oder Stift angefertigte Zeichnungen sowie eine KI-gestützt erzeugte Rückmeldung dazu. Zeichnungen werden nach 48 Stunden gelöscht
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 beim ersten Login wird zu seiner Änderung aufgefordert. Meldet sich die Schülerin oder der Schüler über den Identitätsdienst der Schule an (Abschnitt 7), entsteht das Konto ohne E-Mail-Adresse und Passwort unter der pseudonymen Kennung des Dienstes; das dort vergebene Pseudonym dient als Anzeigename.

Datenkategorie	Erhoben?	Anmerkung
E-Mail-Adresse	Ja	Für Authentifizierung (Clerk); entfällt bei Anmeldung über den Identitätsdienst (technische, nicht zustellbare Adresse)
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
Pseudonyme Kennung, Pseudonym und Gruppen des Identitätsdienstes	Ja, nur bei Anmeldung über den Identitätsdienst	Gruppen werden als Klassen übernommen (Abschnitt 7)
Kurs-/Klassenzugehörigkeit	Ja	Zuordnung zu Lehrkraft-Klassen
Lernfortschritt	Ja	Gelernte Fachbegriffe, Übungsergebnisse, Lernlevel
Selbst beigetragene Inhalte	Ja (nur kollaborative Apps)	Sachinformationen mit Quellenangabe. Für Mitschülerinnen und Mitschüler derselben Schule **ohne Urheberangabe** sichtbar; die Lehrkraft sieht die beitragende Person und kann Beiträge entfernen (Moderation)
KI-Chat-Verläufe	Ja, soweit aktiviert	Gespeichert während der Laufzeit der Lern-Session bzw. des Projekts
Antworten, handschriftliche Zeichnungen, automatische Rückmeldung	Ja, nur Rückmelde-Apps	Wie Modell A, jedoch dem Benutzerkonto zugeordnet, damit die Schülerin oder der Schüler eigene frühere Rückmeldungen wiederfindet. Zeichnungen werden auch hier nach 48 Stunden gelöscht
IP-Adresse	Ja	Server-Logs (automatisch)

Modell C — Namentliche Verwaltung in Organisations-Apps (z. B. Betreuungsanmeldung, Projektwahl, Veranstaltungsplanung, Bestelllisten): Hier ist die namentliche Zuordnung der Zweck der Anwendung. Der Verantwortliche führt diese Listen ohnehin; der Auftragsverarbeiter verarbeitet sie in seinem Auftrag. In der Veranstaltungsplanung gilt Modell C für alle Teilnehmenden, also auch für Lehrkräfte und externe Gäste.

Datenkategorie	Erhoben?	Anmerkung
Vor- und Nachname (Schüler bzw. Teilnehmende)	Ja	Zweck der Anwendung — z. B. Auswahl aus der Klassenliste, Anmeldung zur Betreuung, Projektzuteilung, Teilnehmerliste einer Veranstaltung
Klasse / Klassenstufe bzw. Gruppe	Ja	Zuordnung und Gruppenbildung
E-Mail-Adresse der Teilnehmenden	Ja, nur Veranstaltungsplanung, soweit angegeben	Versand des persönlichen Zugangslinks und — nach Freigabe durch den Verantwortlichen — des persönlichen Plans. **Schülerinnen und Schüler müssen keine Adresse angeben**; sie erhalten ihren Zugang dann als Link oder gedruckte QR-Karte. Bei der offenen Anmeldung legt der Verantwortliche je Veranstaltung fest, ob die Adresse Pflicht oder freiwillig ist; eine angegebene Adresse gilt erst als bestätigt, wenn der zugeschickte Link geöffnet wurde. Antworten auf diese E-Mails gehen an die Person, die die Veranstaltung angelegt hat
Wünsche und Zuteilung	Ja, Projektwahl und Veranstaltungsplanung	Gewählte Angebote in der Reihenfolge der Wünsche, daraus berechnete Zuteilung zu Angeboten und Zeitblöcken
Persönlicher Zugangslink	Ja, nur Veranstaltungsplanung	Zufällige, nicht erratbare Kennung (UUID) je Person; ersetzt ein Benutzerkonto
Geschlecht	Ja, nur Projektzuteilung	Ausschließlich für die Belegung geschlechtergetrennter Unterkünfte bei mehrtägigen Veranstaltungen
Persönliche Zugangs-PIN	Ja, nur Bestell-/Rückmeldelisten	Verhindert, dass Mitschüler in fremdem Namen antworten
Anwesenheit / Fehlzeiten	Ja, Betreuungsanmeldung und Veranstaltungsverwaltung	Tagesbezogene Erfassung; bei der Betreuung zusätzlich der Grund einer Abwesenheit und die Angabe, wer sie eingetragen hat (Sekretariat, Lehrkraft oder Betreuungskraft)
Freitext-Notizen zu Einzelnen	Ja, Betreuungsanmeldung und Veranstaltungsverwaltung	Veranstaltungsverwaltung: Sonderstatus und Begründung einer Gruppentrennung — Inhalt bestimmt allein der Verantwortliche (siehe § 3 Abs. 3). Betreuungsanmeldung: freiwillige Mitteilung der **Erziehungsbe-**

Datenkategorie	Erhoben?	Anmerkung
		rechtigten zu ihrem Kind, ausschließlich für die betreuenden Lehrkräfte sichtbar (siehe § 3 Abs. 4)
Einverständniserklärungen (Datei)	Ja, nur Veranstaltungsverwaltung	Von Erziehungsberechtigten hochgeladene Dokumente
Name und Kontaktdaten der Erziehungsberechtigten	Ja, Betreuungsanmeldung und Veranstaltungsverwaltung	Betreuungsanmeldung: Name, E-Mail, Telefonnummer für Rückfragen während der Betreuungszeit. Veranstaltungsverwaltung: E-Mail-Adresse für die Einverständniserklärung zu einer mehrtägigen Veranstaltung. **Die Notfall-Telefonnummer ist auf Weisung des Verantwortlichen auch den eingesetzten Betreuungskräften sichtbar** — je Schule und Halbjahr schaltbar. Zweck: Ab dem Ende der Sekretariatszeit sind sie die einzigen Ansprechpartner vor Ort. Name, E-Mail-Adresse und Freitext-Mitteilung der Erziehungsberechtigten bleiben ihnen verborgen
Name und Kontaktdaten der Betreuungs-/Projektleitungsperson	Ja	Einsatzplanung und Nachweis geleisteter Betreuungsstunden. Veranstaltungsplanung: nur Name der Referentin oder des Referenten und Verfügbarkeit je Zeitblock; den Teilnehmenden wird der Name nur angezeigt, wenn der Verantwortliche das einstellt
Protokoll fehlgeschlagener Zugriffsversuche	Ja	Missbrauchsabwehr. Je Anwendung entweder IP-Adresse und Zeitpunkt (Betreuungsanmeldung) oder der eingegebene Name mit Klasse und Fehlermeldung (Projektwahl — dort tippen Schülerinnen und Schüler ihren Namen, und ohne dieses Protokoll bliebe unbemerkt, wenn jemand fremde Namen ausprobiert). Bei der offenen Anmeldung zu einer Veranstaltung IP-Adresse und Zeitpunkt jedes Anmeldeversuchs, um massenhafte Anmeldungen von einem Anschluss zu begrenzen
Persönlicher Zugangscode der Betreuungskraft	Ja, nur Betreuungsanmeldung	Sechsstelliger Code je Person, ausschließlich als bcrypt-Abdruck gespeichert und nach seiner Erzeugung nicht mehr anzeigbar; ersetzt

Datenkategorie	Erhoben?	Anmerkung
		einen Benutzerzugang für Personen, die nicht dem Kollegium angehören

Modell D — Unterrichtsdokumentation der Lehrkraft (z. B. Sitzplan mit Beteiligungsnotizen): Die Schülerinnen und Schüler haben hier **keinen eigenen Zugang**; die Lehrkraft dokumentiert ihre eigenen Unterrichtsbeobachtungen. Beim Auftragsverarbeiter liegen diese Beobachtungen ausschließlich unter einer Nummer; die Zuordnung der Nummer zum Namen wird auf dem Endgerät der Lehrkraft verschlüsselt und ist für den Auftragsverarbeiter nicht auflösbar. Damit die Anwendung im Unterricht auch ohne Netzverbindung nutzbar bleibt, hält sie die Daten zusätzlich auf dem Endgerät der Lehrkraft vor; dieses Gerät liegt im Verantwortungsbereich des Verantwortlichen. **Noten und Leistungsbewertungen werden in dieser Anwendung nicht gespeichert.**

Datenkategorie	Erhoben?	Anmerkung
Vor- und Nachname (Schüler)	Ja, ausschließlich verschlüsselt	Die Zuordnung Nummer → Name wird auf dem Endgerät der Lehrkraft verschlüsselt und nur in dieser Form übertragen; der Auftragsverarbeiter besitzt den Schlüssel nicht (siehe Anlage 2 Nr. 1)
Nummer und Sitzplatz	Ja	Lerngruppe, Raum und Platz; ohne die verschlüsselte Zuordnung nicht auf eine Person beziehbar
Notizen zur mündlichen Beteiligung	Ja	Zeitpunkt, Platz, Art des Beitrags (gemeldet · aufgerufen · Sorgfalt beim Arbeiten) und eine Wertung der Lehrkraft. **Eine Note wird nicht gespeichert** — die Notizen sind Unterrichtsbeobachtungen, aus denen die Lehrkraft später eigenständig bewertet
Noten / Leistungsbewertungen	**Nein**	Werden nicht gespeichert. Die Beteiligungsnotizen sind Unterrichtsbeobachtungen; die Bewertung nimmt die Lehrkraft außerhalb dieser Anwendung vor
Anwesenheitsnotizen	Ja	Anwesend, fehlt oder verspätet mit Ankunftszeit; Gedächtnisstütze zum Nachtragen, das Fehlzeitensystem des Verantwortlichen bleibt führend
Lerngruppe, Fach, Schulhalbjahr	Ja	Zuordnung zur Lehrkraft
Fotos der Schülerinnen und Schüler	**Nein**	Verbleiben auf dem Endgerät der Lehrkraft und werden nicht an den Auftragsverarbeiter übermittelt

Hinweise:

- **Datensparsamkeit bei Namen — Trennlinie zwischen Lern- und Organisations-Apps:** In den **Lern-Apps** (Modell A und B) erhebt und speichert der Auftragsverarbeiter **keine Klar-Namen (Vor- oder Nachnamen) von Schülern**. Lernstände, Übungsergebnisse und KI-Chats hängen an einem pseudonymen Konto; die Authentifizierung erfolgt anonym über Kurscode (Modell A) oder über E-Mail-Adresse plus Benutzernamen (Modell B). In **Organisations-Apps**, die der Verantwortliche zur Verwaltung einsetzt (Modell C), ist die namentliche Zuordnung dagegen der Zweck der Anwendung — dort werden Vor- und Nachnamen auf Weisung und im Auftrag des Verantwortlichen verarbeitet. **Diese Datenräume sind technisch getrennt: Namen aus Organisations-Apps werden weder mit den Lern-App-Konten zusammengeführt noch an den KI-Tutor übergeben.** 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. In der **Unterrichtsdokumentation der Lehrkraft** (Modell D) werden Namen zwar verarbeitet, liegen beim Auftragsverarbeiter aber ausschließlich verschlüsselt; auch dieser Datenraum ist von den Lern-App-Konten und vom KI-Tutor getrennt.
- **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.
- **Modell D:** Die Beobachtungen dienen allein der Lehrkraft, die sie erhoben hat. Ein Verlauf über die Zeit wird gebildet, damit ein Nachlassen der Beteiligung früh auffällt und die Lehrkraft nachfragen kann; **Noten werden nicht gespeichert** — die Anwendung dokumentiert Beobachtungen, nicht Bewertungen. Eine automatisierte Entscheidung oder ein Scoring findet nicht statt, und die drei Arten von Beiträgen werden nicht zu einem Punktwert verrechnet.
- **Betreuungskräfte, die nicht dem Kollegium angehören (Modell C, Betreuungsanmeldung):** Ein Betreuungsangebot wird häufig von älteren Schülerinnen und Schülern derselben Schule oder von externen Honorarkräften durchgeführt. Sie sehen ausschließlich die Kinder ihres Raums an ihrem Diensttag, deren Namen und Klassen sowie — soweit der Verantwortliche das aktiviert — die Notfall-Telefonnummer. **Der Auftragsverarbeiter weist ausdrücklich darauf hin, dass der Verantwortliche diese Personen vor dem ersten Einsatz schriftlich auf Vertraulichkeit zu verpflichten hat** (Art. 29, Art. 32 Abs. 4 DSGVO); bei nicht dem Kollegium angehörenden Personen folgt diese Pflicht nicht schon aus dem Dienstverhältnis. Der Auftragsverarbeiter kann das technisch nicht erzwingen und tut es nicht.

5. Dauer der Verarbeitung

(0) **Organisations-Apps mit namentlichen Listen (Modell C):** Die Daten werden für die Dauer des jeweiligen Vorgangs verarbeitet und danach gelöscht — Projekt- und Veranstaltungsdaten zum Ende der Veranstaltung, Bestell- und Rückmeldelisten nach Abschluss der Bestellung, jeweils vom

Verantwortlichen bzw. auf seine Weisung hin. **Bei der Betreuungsanmeldung löscht der Auftragsverarbeiter automatisiert: 90 Tage nach Ende des Schuljahres, in dem das Betreuungshalbjahr lag** (Gleichlauf mit der Frist aus Absatz 1). Gelöscht werden dabei die Anmeldung des Kindes, die Angaben der Erziehungsberechtigten samt Freitext-Mitteilung, die Raumzuteilung und die Anwesenheiten. Der Nachweis der gehaltenen Betreuungsnachmittage und die Datensätze der Betreuungskräfte bleiben als Abrechnungsgrundlage des Verantwortlichen erhalten; sie enthalten keine Daten der Kinder. Unabhängig davon endet die Verarbeitung spätestens mit den Fristen aus Absatz 1.

(0a) **Rückmeldungen aus dem Unterricht:** Sitzungen ohne Konto und **alle** handschriftlichen Zeichnungen werden 48 Stunden nach ihrem Beginn gelöscht, auch wenn die Sitzung an einem Konto hängt. Die übrige Konto-Historie (Antworten und Rückmeldung) folgt dem Lebenszyklus der übrigen Schülerdaten nach Absatz 1.

(0b) **Protokolle fehlgeschlagener Zugriffsversuche:** sieben Tage; die IP-Adressen aus offenen Anmeldungen zu Veranstaltungen 24 Stunden.

(0c) **Unterrichtsdokumentation der Lehrkraft (Modell D):** Sitzordnung, Beteiligungs- und Anwesenheitsnotizen sowie die verschlüsselte Namenszuordnung werden 90 Tage nach dem Ende des Schuljahres gelöscht, in dem sie entstanden sind (Gleichlauf mit Absatz 0 und Absatz 1).

(0d) **Anmeldung über einen Identitätsdienst der Schule (Abschnitt 7):** Sitzungen ohne Abmeldesignal werden nach 24 Stunden geschlossen, geschlossene Einträge des Sitzungsregisters nach 30 Tagen gelöscht; Anmeldevorgänge sind nach zehn Minuten ungültig und werden binnen eines Tages gelöscht. Konten, die über den Identitätsdienst entstanden sind, ohne dass für die Schule oder die Person ein Lizenzvertrag besteht, werden samt Identitätszuordnung, Sitzungen, daraus entstandenen Klassen und Lerndaten zwölf Monate nach der letzten Anmeldung gelöscht (zweistufig: Vormerkung, Löschung frühestens 14 Tage danach). Besteht ein Lizenzvertrag, gelten stattdessen die Absätze 1 und 2.

(0e) **Veranstaltungsplanung:** Der Auftragsverarbeiter löscht automatisiert **30 Tage nach dem letzten eingetragenen Veranstaltungstag** die Namen, Gruppen, E-Mail-Adressen, Zugangslinks, Wünsche und Zuteilungen aller Teilnehmenden sowie die Pläne und Anmeldeprotokolle der Veranstaltung. Erhalten bleiben die Einstellungen der Veranstaltung (einschließlich der Namen der Referentinnen und Referenten), damit sie als Vorlage dienen kann, und eine Statistik je Angebot ohne Personenbezug (wie oft gewählt, wie oft besucht). Ist kein Veranstaltungstag eingetragen, entfällt die automatische Löschung; dann gilt Absatz 0 Satz 1. Löscht der Verantwortliche die Veranstaltung selbst, werden alle zugehörigen Daten sofort entfernt.

(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 in der jeweils geltenden Fassung): 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. Schulinterne gemeinsame Datenräume (interner Datenfluss)

A — Datenraum der Lehrkräfte (Lehrmaterialien)

(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.

B — Datenraum der Schülerbeiträge (kollaborative Lern-Apps)

(1) In kollaborativen Lern-Apps führt der Auftragsverarbeiter pro Schule eine **gemeinsame Materialsammlung**, zu der angemeldete Schülerinnen und Schüler eigene Sachinformationen mit Pflicht-Quellenangabe beitragen (Mandantentrennung über `school_id`, technisch durchgesetzt via Row Level Security).

(2) **Anders als im Datenraum A werden hier personenbezogene Schülerdaten verarbeitet:** Jeder Beitrag ist intern der beitragenden Person zugeordnet. Die Sichtbarkeit ist gestuft — Mitschülerinnen und Mitschüler derselben Schule sehen den Beitrag **ohne** Urheberangabe, die Lehrkräfte der Schule sehen die beitragende Person und können Beiträge entfernen. Die Trennung ist technisch umgesetzt: Die Schüler-Ansicht wird über eine Datenbankfunktion mit festgelegtem Spaltensatz ausgeliefert, der die Urheber-Kennung nicht enthält.

(3) Zweck der Zuordnung ist ausschließlich die **Moderation**: Die Lehrkraft muss einen unzulässigen oder falschen Beitrag der beitragenden Person zuordnen können, um ihrer pädagogischen Begleitung und Aufsichtspflicht nachzukommen. Eine Bewertung der Beiträge findet nicht statt; es werden keine Noten gespeichert.

(4) Löscht eine Schülerin oder ein Schüler das Benutzerkonto, bleibt der Sachbeitrag der Sammlung der Schule erhalten, die Zuordnung zur Person wird jedoch entfernt (Anonymisierung).

7. Anmeldung über einen Identitätsdienst der Schule

(1) Setzt der Verantwortliche einen Identitäts- und Anmeldedienst ein (z. B. Eduplaces, künftig VIDIS/Schulconnex), so erfolgt die Anmeldung von Lehrkräften und Schülern über diesen Dienst.

(2) Der Auftragsverarbeiter empfängt und speichert dabei eine **pseudonyme Kennung** der Person, die Sitzungskennung, die Rolle (Lehrkraft oder Schüler), die Schulzuordnung sowie die Gruppen- bzw. Klassenzugehörigkeit. **Klarnamen werden weder angefordert noch übermittelt** (der entsprechende Berechtigungsumfang wird bewusst nicht abgerufen).

(3) Der Identitätsdienst ist **kein Unterauftragsverarbeiter** des Auftragsverarbeiters im Sinne von § 7 dieses Vertrags. Er wird vom Verantwortlichen eingesetzt und ist seinerseits dessen Auftragsverarbeiter; zwischen ihm und dem Auftragsverarbeiter besteht kein Auftragsverarbeitungsverhältnis nach Art. 28 DSGVO.

(4) Meldet sich eine Person beim Identitätsdienst ab, beendet der Auftragsverarbeiter die zugehörige Sitzung, soweit der Dienst ihn darüber unterrichtet (Backchannel-Logout).

(5) Nach jeder Anmeldung meldet der Auftragsverarbeiter dem Identitätsdienst unter der pseudonymen Kennung zurück, ob für die Person ein Zugang über eine Schul-Lizenz, ein Klassen-Abo oder ein Eltern-Abo besteht oder kein Zugang, und ob es sich um eine Probephase handelt. Weitere Daten werden nicht übermittelt. Die Rückmeldung dient der Abrechnung der Plattformnutzung zwischen dem Verantwortlichen und dem Identitätsdienst; der Verantwortliche erteilt die Weisung dazu mit dem Einsatz des Identitätsdienstes.

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 (Passwort-Login); Administrationszugang zu Clerk mit Mehr-Faktor-Authentifizierung; 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)
Verschlüsselung der Namenszuordnung (Unterrichtsdokumentation)	In der Unterrichtsdokumentation der Lehrkraft (Anlage 1, Abschnitt 4, Modell D) wird die Zuordnung von Nummer zu Name bereits auf dem Endgerät der Lehrkraft verschlüsselt (AES-GCM; der Schlüssel wird aus einem nur ihr bekannten Passwort abgeleitet) und ausschließlich in verschlüsselter Form übertragen und gespeichert. Der Auftragsverarbeiter besitzt den Schlüssel nicht und kann die Zuordnung nicht herstellen
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; beim ersten Login wird zu ihrer Änderung aufgefordert

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, Schülerinnen und Schüler mit individuellem Konto, Eltern im Eltern-Abo)	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: 25.10.2026