

## Vertrag zur Auftragsverarbeitung gem. Art. 28 Abs. 3 DS-GVO

zwischen

---

Name der Bildungseinrichtung

---

Adresse

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

und

**LivingLines UG**

c/o Campus Founders, Bildungscampus 11, 74076 Heilbronn,

vertreten durch den Geschäftsführer Jakob Seitz

als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“)

### 1. Vertragsgegenstand

- 1.1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers auf Grundlage der Nutzungsvereinbarung zwischen dem \_\_\_\_\_ als Auftraggeber und der LivingLines UG, als Auftragnehmer vom \_\_\_\_\_, nachfolgend gemeinsam Hauptvertrag. Zweck ist der Betrieb und die Bereitstellung der Lernplattform LivingLines für den schulischen Mathematikunterricht, einschließlich Nutzerverwaltung, Zuweisung und Bearbeitung von Aufgaben, Verarbeitung handschriftlicher Eingaben, automatische Auswertung und Feedback, Speicherung von Bearbeitungsständen sowie Klassen und Kursverwaltung.
- 1.2. Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrages vor.
- 1.3. Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.
- 1.4. Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

### 2. Umfang der Beauftragung und Weisungsrecht

- 2.1. Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrages und gemäß den Weisungen des Auftraggebers erheben oder verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung

personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, welchem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

2.2. Alle erteilten Weisungen sind vom Auftraggeber zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

2.3. Weisungsberechtigte Person des Auftraggebers ist \_\_\_\_\_.

### **3. Art der verarbeiteten Daten, Kreis der Betroffenen**

3.1. Personenbezogene Daten im Sinne des Art. 4 Nr.1 DS-GVO und dieses Vertrages sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Dies sind insbesondere:

- Stammdaten von Nutzerkonten, zum Beispiel frei wählbarer Benutzername, Bundesland, Schulart
- Kontaktdaten, ausschließlich E-Mail-Adresse bei registrierten Accounts
- Zugehörigkeiten, zum Beispiel Verknüpfung von Accounts mit Klassen und Kursen, bei anonymen Schülerzugängen nur selbst gewählter Anzeigename ohne E-Mail
- Zugangsdaten, zum Beispiel gehashte Passwörter, Authentifizierungs-Tokens, Rollen, Rechte
- Lern- und Inhaltsdaten, zum Beispiel handschriftliche Eingaben, erkannte Formeln, Aufgaben, Abgaben, Feedback, Ergebnisse
- Nutzungsdaten, zum Beispiel Logins, Zeitstempel, Interaktionen, Sitzungs-IDs
- Technische Metadaten, zum Beispiel IP-Adresse, Geräteinformationen, Browserinformationen, erforderliche Cookie-IDs
- Protokoll- und Betriebsdaten, zum Beispiel Systemlogs, Fehlerberichte, Monitoring-Ereignisse, temporäre Zwischenspeicher, Caches, Datensicherungen, Snapshots
- Supportdaten, zum Beispiel Anfragen schulischer Ansprechpartner, Name, E-Mail, Telefonnummer, Ticketinhalte, soweit Support genutzt wird

Nicht verarbeitet werden:

- Besondere Kategorien nach Artikel 9 DSGVO, zum Beispiel Gesundheitsdaten, biometrische Daten, religiöse oder politische Ansichten
- Zahlungs- und Abrechnungsdaten
- Ausweisdaten, zum Beispiel Personalausweisnummer, Steuer-ID, Sozialversicherungsnummer

3.2. Im Rahmen der Durchführung des Hauptvertrages erhält der Auftragnehmer Zugriff auf die unter Abs. 1 aufgeführten personenbezogenen Daten. Betroffene Personen sind Schülerinnen und Schüler,

Erziehungsberechtigte, Lehrkräfte, schulische Administratoren sowie LivingLines-Administratoren und Supportkontakte.

#### **4. Schutzmaßnahmen des Auftragnehmers**

- 4.1. Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen, um ein dem Risiko angemessenes Schutzniveau für die Daten zu gewährleisten.
- 4.2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO und behält diese bei. Dies sind insbesondere die in Anhang 1 aufgeführten wirksamen Maßnahmen der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle und Belastbarkeitskontrolle sowie das Verfahren zur Bewertung, Überprüfung und Evaluierung dieser Maßnahmen.
- 4.3. Eine Änderung der gem. Anhang 1 getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
- 4.4. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend Art. 28 Abs. 3 lit. b DS-GVO zur Vertraulichkeit verpflichten und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

#### **5. Informationspflichten des Auftragnehmers**

- 5.1. Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte (nachfolgend auch nur „Verletzung“) wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die

Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

- 5.1.1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
- 5.1.2. eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- 5.2. Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.
- 5.3. Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Abs. 1 betroffen sind.

## **6. Kontrollrechte des Auftraggebers**

- 6.1. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

## **7. Einsatz weiterer Auftragsverarbeiter**

- 7.1. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von Unterauftragsverhältnissen mit Subunternehmern (nachfolgend „Unterauftragnehmerverhältnis“) befugt.
- 7.2. Ein Unterauftragnehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen oder Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt.
- 7.3. Gemäß 7.1 setzt der Auftragnehmer ggf. die in Anhang 2 aufgeführten Unterauftragnehmerverhältnisse ein.
- 7.4. Der Auftragnehmer wird jedem weiteren Unterauftragnehmer vertraglich dieselben Datenschutzpflichten auferlegen, die in diesem Vertrag in Bezug auf den Auftragnehmer festgelegt sind.

## **8. Anfragen und Rechte von Betroffenen und Zusammenarbeit mit den Aufsichtsbehörden**

- 8.1. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 – 22 DS-GVO sowie 32 - 36 DS-GVO.
- 8.2. Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Antwort ab.

## **9. Haftung**

- 9.1. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer allein der Auftraggeber gegenüber dem Betroffenen verantwortlich.
- 9.2. Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

## **10. Beendigung des Hauptvertrages**

Der Auftragnehmer wird auf die Weisung des Auftraggebers hin mit Beendigung des Hauptvertrages alle Daten entweder vollständig und unwiderruflich löschen oder an den Auftraggeber zurückgeben, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Verarbeitung der Daten besteht.

## **11. Schlussbestimmungen**

- 11.1. Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.
- 11.2. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.
- 11.3. Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.
- 11.4. Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Würzburg.

**Anlagen**

- Anhang 1 – Technische und organisatorische Maßnahmen
- Anhang 2 – aktuelle Unterauftragnehmer

---

Ort, Datum

---

Ort, Datum

---

LivingLines UG

---

Auftraggeber

## Anhang 1 – Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

### **1. Vertraulichkeit**

#### *Zutrittskontrolle*

Die physische Sicherheit der Server wird durch das Rechenzentrum des Hosters gewährleistet. Genutzte Arbeitsräume sind außerhalb der Arbeitszeiten nicht frei zugänglich. Während der Arbeitszeiten bewegen sich Besucher nicht unbeaufsichtigt in Bereichen mit möglichem Zugriff auf personenbezogene Daten. Der Zutritt erfolgt über ein elektronisches Zugangssystem des Betreibers der Räumlichkeiten. Zugangsberechtigungen werden nach dessen Verfahren erteilt und entzogen. Eine eigene Schlüsselverwaltung durch den Auftragnehmer ist derzeit nicht erforderlich.

#### *Zugangskontrolle*

Um Zugang zu IT-Systemen zu erhalten, müssen der Auftragnehmer und seine Beschäftigten über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden Benutzerberechtigungen von einem oder mehreren Administratoren vergeben.

Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, das Passwort besteht aus Groß und Kleinbuchstaben, Ziffern und Sonderzeichen.

Passwörter werden nach einem Turnus von 180 Tagen gewechselt. Ausgenommen hiervon sind Passwörter mit einer Mindestlänge von 32 Zeichen.

Remote-Zugriffe finden in der Regel nicht statt. Sofern sie erforderlich sind, erfolgen sie ausschließlich über verschlüsselte Verbindungen.

Alle für die Leistungserbringung genutzten Systeme werden mit aktuellen Sicherheitsupdates versorgt.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

Passwörter, die der Auftragnehmer vom Auftraggeber erhält oder für dessen IT-Systeme verwendet, werden verschlüsselt gespeichert und sind nur den Beschäftigten zugänglich zu machen, die konkret mit der Erbringung von Leistungen für den Auftraggeber betraut sind.

#### *Zugriffskontrolle*

Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers werden nach dem Need to know Prinzip vergeben. Zugriff erhalten nur Personen, die diese Daten, Datenbanken oder Anwendungen administrieren, warten oder entwickeln.

Die Vernichtung von Datenträgern und Papier erfolgt bei entsprechender Notwendigkeit durch einen Dienstleister mit Vernichtung nach DIN 66399. Anderenfalls sorgt der Auftragnehmer selbst für eine geeignete Vernichtung.

#### *Trennung*

Personenbezogene Daten des Auftraggebers werden logisch von Daten anderer Kunden getrennt verarbeitet. Die Trennung erfolgt durch mandantenbezogene Kennzeichnungen in Datenbanktabellen sowie durch rollenbasierte Zugriffsrechte. Export und Supportzugriffe erfolgen ausschließlich mandantenbezogen.

#### *Pseudonymisierung & Verschlüsselung*

Sämtliche Datenübertragungen erfolgen über verschlüsselte Verbindungen. Ein administrativer Zugriff auf Systeme des Auftragnehmers erfolgt ausschließlich über verschlüsselte Verbindungen. Produktive

Datenbanken und Datensicherungen sind im Ruhezustand verschlüsselt. Soweit möglich werden personenbezogene Daten pseudonymisiert verarbeitet.

## **2. Integrität**

### *Eingabekontrolle*

Der Auftragnehmer wird Eingaben, Änderungen oder Löschungen von personenbezogenen Daten, die er im Auftrag des Auftraggebers durchführt, in geeigneter Weise dokumentieren, sofern nicht sichergestellt ist, dass das jeweilige IT-System selbst eine Protokollierung entsprechender Aktivitäten durchführt.

### *Weitergabekontrolle*

Eine Weitergabe erfolgt nur im abgestimmten Umfang. Die Nutzung lokaler Arbeitsumgebungen des Auftragnehmers ist zulässig, sofern diese geschützt sind und keine Synchronisation mit privaten Cloudspeichern erfolgt. Produktive Daten werden für Entwicklungszwecke möglichst pseudonymisiert. Private Wechseldatenträger sind ausgeschlossen.

## **3. Verfügbarkeit und Belastbarkeit**

Produktive Daten werden im Rechenzentrum des Hosters betrieben. Datensicherungen und Wiederherstellungstests erfolgen nach dessen Verfahren. Der Auftragnehmer stellt sicher, dass der Hoster geeignete Sicherungen und Wiederherstellungsmöglichkeiten vorhält und dokumentiert.

## **4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

Der Auftragnehmer trägt durch Richtlinien und/oder Anweisungen an die Beschäftigten dazu bei, dass eine Verarbeitung personenbezogener Daten in einer Weise gewährleistet ist, die den Anforderungen der DSGVO entspricht.

Dies beinhaltet insbesondere eine regelmäßige Überprüfung der Wirksamkeit der getroffenen Maßnahmen zum Schutz personenbezogener Daten und ggf. der Anpassung.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Beschäftigten erkannt und unverzüglich dem Auftraggeber gemeldet werden, wenn dies Daten betrifft, die im Rahmen der Auftragsverarbeitung für den Auftraggeber verarbeitet werden.

### *Auftragskontrolle*

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag abgeschlossen. Unterauftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

### *Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen*

Etwaige nach Art. 25 DSGVO erforderliche Maßnahmen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten durch den Auftraggeber sind vom Auftraggeber zu treffen bzw. durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer festzulegen.

## Anhang 2 – aktuelle Unterauftragnehmer

Der Auftragnehmer setzt folgende Unterauftragsverarbeiter ein. Verarbeitung nur im Rahmen des Hauptvertrags. Drittlandübermittlungen finden nicht statt.

Firma	Wodanio GmbH
Leistung	Hosting von Compute, Speicher, Netzwerk, Container Orchestrierung, Datenbankbetrieb, Monitoring, Backups
Datenkategorien	Die in Ziffer 3.1 genannten Daten einschließlich Logdaten und Datensicherungen
Zweck	Betrieb der LivingLines Plattform gemäß Hauptvertrag
Sitz	97268 Kirchheim, Deutschland
Verarbeitungsort	Rechenzentrum in Kirchheim, Deutschland
Vertragsgrundlage	AVV vom 13.10.2025
TOMs Referenz	gemäß AVV Wodanio, Anhang 1
Löschfristen	Backups nach Zyklus, Logs gemäß Vereinbarung
Datenschutzkontakt	Philip Reichert, philip.reichert@wodanio.com