

Vereinbarung zur Auftragsverarbeitung (AVV)

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) für die Nutzung von SkooBase SEK
Fassung 2026-10-01 (1. Oktober 2026)

AUFTRAGGEBER (VERANTWORTLICHER)

Die Schule oder Lehrperson, die SkooBase nutzt und diese Vereinbarung in der Anwendung bestätigt oder unterzeichnet (siehe § 1 Abs. 2).

AUFTRAGNEHMER (AUFTRAGSVERARBEITER)

Cornelius Altrichter
Betreiber von SkooBase SEK
Silvrettastraße 13a
6780 Schruns, Österreich
info@skoobase.com

§ 1 Gegenstand, Parteien und Dauer

1. Der Auftragnehmer stellt dem Auftraggeber die Webanwendung SkooBase SEK (sek.skoobase.com, im Folgenden „SkooBase“) zur Verfügung (Hauptvertrag: die Allgemeinen Geschäftsbedingungen von SkooBase SEK in der jeweils gültigen Fassung). Dabei verarbeitet er personenbezogene Daten im Auftrag des Auftraggebers. Diese Vereinbarung regelt die Rechte und Pflichten beider Seiten bei dieser Verarbeitung.
2. Auftraggeber ist bei einer Schullizenz die Schule, vertreten durch die Person, die die Lizenz abschließt. Bei einer Einzellizenz ist Auftraggeber die Lehrperson. Verarbeitet sie die Daten im Rahmen ihrer dienstlichen Tätigkeit für eine Schule, die datenschutzrechtlich die Verantwortliche ist, schließt sie diese Vereinbarung zugleich für diese Schule ab und erklärt, dazu befugt zu sein. Die Schule erhält auf Wunsch jederzeit eine von beiden Seiten unterzeichnete Ausfertigung.
3. Diese Vereinbarung gilt nicht für Daten, die der Auftragnehmer als eigener Verantwortlicher verarbeitet: die Konto- und Anmeldedaten der Lehrpersonen, Nutzungs- und Serverprotokolle, Support-Anfragen sowie Vertrags- und Rechnungsdaten. Dafür gilt die Datenschutzerklärung von SkooBase.
4. Die Vereinbarung gilt, solange der Auftragnehmer Daten des Auftraggebers in SkooBase verarbeitet, also auch während der Testphase und nach Ablauf einer Lizenz bis zur Löschung der Daten.

§ 2 Art, Zweck und Umfang der Verarbeitung

1. Zweck der Verarbeitung ist ausschließlich die Bereitstellung von SkooBase als Werkzeug für die pädagogische und organisatorische Arbeit von Lehrpersonen und Schulen: Speichern, Anzeigen, Auswerten, Teilen innerhalb der Schule, Exportieren und Löschen der vom Auftraggeber eingegebenen Daten.
2. Die Arten der Daten und die Kategorien betroffener Personen sind in **Anlage 1** beschrieben.
3. Der Auftragnehmer verwendet die Daten für keine eigenen Zwecke. Er wertet sie nicht inhaltlich aus, gibt sie nicht weiter und nutzt sie nicht für Werbung oder zum Training von KI-Systemen. Für Betrieb und Support sieht er die Namen der Klassen und zählt Datensätze, etwa die Zahl der Klassen und der Schülerinnen und Schüler je Konto.

§ 3 Weisungen

1. Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers. Die Weisungen ergeben sich aus dieser Vereinbarung, dem Hauptvertrag und der Bedienung von SkooBase: Was der Auftraggeber in der Anwendung eingibt, ändert, freigibt, exportiert oder löscht, ist eine Weisung. Weitere Weisungen erteilt der Auftraggeber in Textform an info@skoobase.com.
2. Ist der Auftragnehmer durch Recht der Europäischen Union oder Österreichs zu einer anderen Verarbeitung verpflichtet, teilt er dies dem Auftraggeber vorher mit, sofern das betreffende Recht die Mitteilung nicht verbietet.
3. Hält der Auftragnehmer eine Weisung für rechtswidrig, weist er den Auftraggeber unverzüglich darauf hin. Er darf die Ausführung aussetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.
4. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere dafür, welche Daten er in SkooBase einträgt und auf welcher Rechtsgrundlage.

§ 4 Vertraulichkeit

1. Der Auftragnehmer betreibt SkooBase allein; außer ihm hat keine weitere Person Zugriff auf Server und Datenbank. Für Wartung und Weiterentwicklung setzt er Software-Werkzeuge ein, die unter seiner Aufsicht und nach seiner Freigabe arbeiten. Er ist zur Vertraulichkeit und zur Wahrung des Datengeheimnisses nach § 6 Datenschutzgesetz verpflichtet; diese Pflicht besteht nach Ende der Vereinbarung fort.
2. Zieht der Auftragnehmer künftig weitere Personen hinzu, verpflichtet er sie vor Beginn ihrer Tätigkeit schriftlich in gleicher Weise.

§ 5 Sicherheit der Verarbeitung

1. Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Sie sind in **Anlage 2** beschrieben.
2. Der Auftragnehmer darf die Maßnahmen an den Stand der Technik anpassen. Das vereinbarte Schutzniveau darf dabei nicht unterschritten werden.
3. Der Auftraggeber sorgt in seinem Bereich für Sicherheit: sichere Passwörter, sorgsamer Umgang mit dem Wiederherstellungs-Code, gesperrte Geräte, keine Weitergabe von Zugangsdaten.

§ 6 Weitere Auftragsverarbeiter

1. Der Auftraggeber genehmigt den Einsatz der in **Anlage 3** genannten weiteren Auftragsverarbeiter.
2. Will der Auftragnehmer einen weiteren Auftragsverarbeiter hinzuziehen oder ersetzen, informiert er den Auftraggeber mindestens 30 Tage vorher per E-Mail oder durch einen Hinweis in der Anwendung. Der Auftraggeber kann innerhalb dieser Frist widersprechen. Lässt sich der Widerspruch nicht ausräumen, kann der Auftraggeber den Hauptvertrag zum Zeitpunkt der Änderung kündigen; im Voraus bezahlte Entgelte für die Restlaufzeit werden anteilig erstattet.
3. Der Auftragnehmer verpflichtet jeden weiteren Auftragsverarbeiter vertraglich auf Datenschutzpflichten, die dieser Vereinbarung entsprechen. Kommt ein weiterer

Auftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragnehmer dem Auftraggeber dafür.

§ 7 Ort der Verarbeitung

Die Verarbeitung findet ausschließlich in Mitgliedstaaten der Europäischen Union statt. Eine Verlagerung in ein Drittland erfolgt nur mit vorheriger Zustimmung des Auftraggebers in Textform und nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 8 Rechte der betroffenen Personen

1. SkooBase ist so gebaut, dass der Auftraggeber Anträge betroffener Personen während der Laufzeit selbst erfüllen kann: Jede Lehrperson kann die Daten ihrer Klassen in der Anwendung einsehen, berichtigen, als Sicherung exportieren und löschen.
2. Darüber hinaus unterstützt der Auftragnehmer den Auftraggeber im Rahmen seiner Möglichkeiten bei der Beantwortung solcher Anträge. Er weist darauf hin, dass er verschlüsselt gespeicherte Inhalte (Anlage 2) nicht im Klartext einsieht und einzelne Schülerinnen und Schüler deshalb nicht selbst anhand ihres Namens herausuchen kann.
3. Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst.

§ 9 Unterstützung und Meldung von Datenschutzverletzungen

1. Der Auftragnehmer unterstützt den Auftraggeber bei dessen Pflichten nach Art. 32 bis 36 DSGVO, insbesondere mit den Informationen, die der Auftraggeber für eine Datenschutz-Folgenabschätzung oder sein Verzeichnis von Verarbeitungstätigkeiten braucht.
2. Wird dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten des Auftraggebers bekannt, meldet er sie dem Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden, an die im Konto hinterlegte E-Mail-Adresse. Die Meldung enthält, soweit bekannt: Art der Verletzung, betroffene Daten und Personen, wahrscheinliche Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen.
3. Der Auftragnehmer führt ein Verzeichnis der im Auftrag durchgeführten Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

§ 10 Nachweise und Kontrollen

1. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieser Vereinbarung erforderlich sind.
2. Der Auftraggeber kann die Einhaltung selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer kontrollieren. Kontrollen werden mindestens 14 Tage vorher angekündigt und finden in der Regel anhand von Unterlagen und Auskünften statt. Eine Kontrolle im Rechenzentrum richtet sich nach den Bedingungen des Hosting-Anbieters.
3. Der Auftragnehmer wirkt an Kontrollen der Datenschutzbehörde mit und informiert den Auftraggeber, wenn eine solche Kontrolle dessen Daten betrifft.

§ 11 Löschung und Rückgabe

1. Während der Laufzeit kann jede Lehrperson die Daten ihrer Klassen selbst als Sicherung exportieren und löschen.
2. Nach Ende des Hauptvertrags löscht der Auftragnehmer nach Wahl des Auftraggebers alle im Auftrag verarbeiteten Daten oder gibt sie zurück, sofern keine gesetzliche Pflicht zur weiteren Speicherung besteht. Für die Rückgabe schaltet er den Zugang auf Anfrage für den Export frei oder stellt die Daten bereit. Ein Konto löscht der Auftragnehmer auf Verlangen an info@skoobase.com.
3. Trifft der Auftraggeber keine Wahl, bleiben die Daten nach Ablauf einer Lizenz gespeichert, damit sie nach einer Verlängerung wieder zur Verfügung stehen; der Zugang über die Anwendung ist in dieser Zeit gesperrt. Der Auftragnehmer löscht sie, sobald der Auftraggeber es verlangt.
4. Zwei Löschungen laufen automatisch und gelten als vereinbart: Archivierte Klassen werden am 15. Juni des zweiten Kalenderjahres nach der Archivierung gelöscht, je nach Zeitpunkt also nach rund eineinhalb bis zweieinhalb Jahren, mit vorheriger Warnung an die Lehrperson. Beiträge im Lehrerzimmer samt Antworten und Anhängen werden 30 Tage nach ihrer Erstellung gelöscht, ausgenommen angeheftete Beiträge.
5. In Datensicherungen lassen sich einzelne Einträge nicht gezielt entfernen. Gelöschte Daten verschwinden dort mit dem Ablauf der Sicherungen, in der Regel nach rund 30 Tagen.

§ 12 Haftung

Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO. Im Verhältnis der Parteien zueinander gelten die Haftungsregeln des Hauptvertrags, soweit dem zwingendes Recht nicht entgegensteht.

§ 13 Zustandekommen, Änderungen, Schlussbestimmungen

1. Diese Vereinbarung ist Bestandteil der Allgemeinen Geschäftsbedingungen und gilt damit ab der Registrierung. Beim Abschluss einer Lizenz bestätigt der Auftraggeber sie ausdrücklich im Bestellvorgang (elektronisches Format nach Art. 28 Abs. 9 DSGVO); der Auftragnehmer speichert dabei als Nachweis Zeitpunkt und Fassung der Bestätigung sowie IP-Adresse und Browserkennung. Wer vor dem 1. Oktober 2026 eine Lizenz abgeschlossen hat, bestätigt sie auf dieselbe Weise nach der Anmeldung; bei einer Schullizenz bestätigt die Schuladministration für die Schule. Auf Wunsch unterzeichnen beide Seiten sie zusätzlich.
2. Änderungen dieser Vereinbarung teilt der Auftragnehmer mindestens 30 Tage vor ihrem Inkrafttreten in Textform mit. Sie werden wirksam, wenn der Auftraggeber ihnen zustimmt. Änderungen, die das Schutzniveau senken, sind ohne ausdrückliche Zustimmung nicht möglich.
3. Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag geht diese Vereinbarung in Fragen des Datenschutzes vor.
4. Es gilt österreichisches Recht. Ist eine Bestimmung unwirksam, bleiben die übrigen wirksam.

Anlage 1 - Beschreibung der Verarbeitung

Betroffene Personen

- Schülerinnen und Schüler der Klassen, die der Auftraggeber in SkooBase führt
- ihre Erziehungsberechtigten
- Lehrpersonen der Schule, soweit Kolleginnen und Kollegen oder die Schulleitung Angaben über sie eintragen (zum Beispiel in Vertretungsplänen oder Mitteilungen)

Art der Verarbeitung

Speichern, Bereitstellen zum Abruf, Sichern, Löschen. Eine inhaltliche Auswertung durch den Auftragnehmer findet nicht statt.

Arten der Daten

Bereich	Daten	Speicherung
Stammdaten der Schülerinnen und Schüler	Vor- und Nachname, Adresse, Notizen	im Browser verschlüsselt
Kontaktdaten	Name und E-Mail-Adresse der Erziehungsberechtigten, Telefonnummern, Notfallnummer	im Browser verschlüsselt
Weitere Angaben	Geburtsdatum, Geschlecht, Schulstufe, Zugehörigkeit zu Klasse und Gruppen	unverschlüsselt, ohne Namen
Klasse	Klassenname, Schuljahr, Schulstufe, Fächer	unverschlüsselt
Leistung	Noten, Bewertungen und Kompetenzstufen je Schülerin oder Schüler; Titel und Datum der Leistungsfeststellungen; Bezeichnungen von Kategorien und Kompetenzen	unverschlüsselt, ohne Namen
Leistungsniveau	Niveau je Fach samt Datum	unverschlüsselt, ohne Namen
Leistung, Freitext	Notiz zum Leistungsniveau, Kommentar zum Kompetenzbericht	im Browser verschlüsselt
Verhalten	Bewertungsstufe und Datum	unverschlüsselt, ohne Namen
Verhalten, Freitext	Verhaltensbeobachtung	im Browser verschlüsselt
Unterrichtsplanung	Freitext je Unterrichtsstunde	unverschlüsselt
Checklisten	Titel der Liste; je Schülerin oder Schüler: erledigt oder nicht, Zähler für Erinnerungen	unverschlüsselt, ohne Namen
Checklisten, Freitext	Notiz je Schülerin oder Schüler	im Browser verschlüsselt

Werkzeuge	Gestoppte Zeiten, Ergebnis der Zufallsauswahl	unverschlüsselt, ohne Namen
Notizen, Aufgaben, Termine	Einträge der Lehrperson; Namen von Gruppen. Das Datum von Aufgaben und Terminen ist unverschlüsselt	im Browser verschlüsselt
Klassenkasse	Ein- und Auszahlungen (Beträge und Texte). Im Sondertopf sind Datum und Art der Buchung (Ein- oder Auszahlung) unverschlüsselt	im Browser verschlüsselt
Gemeinsame Bereiche der Schule	Mitteilungen und Aushänge der Direktion, Vertretungspläne, Anliegen an die Direktion samt Antworten, Beiträge im Lehrerzimmer, Terminabstimmungen, geteilte Notizen	mit dem Schulschlüssel verschlüsselt
Gemeinsame Bereiche, Begleitdaten	Wer welchen Aushang wann bestätigt hat, Stimmen bei Terminabstimmungen, Kategorie und Status von Anliegen	unverschlüsselt
Datei-Anhänge im Lehrerzimmer	Hochgeladene Dateien samt Dateiname	unverschlüsselt

„Ohne Namen“ bedeutet: Die Angabe hängt in der Datenbank an einer internen Nummer; der zugehörige Name ist verschlüsselt (Pseudonymisierung). Personenbezogene Daten bleiben diese Angaben trotzdem: Zusammen mit Geburtsdatum, Geschlecht, Klasse, Schule und Lehrperson kann eine Schülerin oder ein Schüler auch ohne Namen bestimmbar sein.

In unverschlüsselten Freitextfeldern (Unterrichtsplanung, Klassenname, Titel von Checklisten und Leistungsfeststellungen, eigene Kategorien und Kompetenzen) sowie in Datei-Anhängen und ihren Dateinamen sollte der Auftraggeber keine Namen von Schülerinnen und Schülern und keine sensiblen Angaben ablegen.

Besondere Kategorien personenbezogener Daten

SkooBase hat keine eigenen Felder für Gesundheitsdaten, Religionsbekenntnis oder andere besondere Kategorien nach Art. 9 DSGVO. In Freitextfeldern kann der Auftraggeber solche Angaben aber eintragen. Die dafür vorgesehenen Felder (Notizen, Verhaltensbeobachtung, Notiz zum Leistungsniveau) werden im Browser verschlüsselt; für die oben genannten unverschlüsselten Freitextfelder gilt das nicht. Ob und auf welcher Rechtsgrundlage er solche Angaben einträgt, entscheidet der Auftraggeber.

Anlage 2 - Technische und organisatorische Maßnahmen

1. Verschlüsselung und Pseudonymisierung

- Die in Anlage 1 als „im Browser verschlüsselt“ bezeichneten Daten werden im Browser der Lehrperson mit AES-GCM (256 Bit) verschlüsselt, bevor sie an den Server gehen, und dort nur verschlüsselt gespeichert. Jeder Eintrag erhält einen eigenen Zufallswert (IV).
- Der persönliche Schlüssel einer Lehrperson ist mit ihrem Passwort gesichert (PBKDF2, SHA-256, 100 000 Runden). Das Passwort wird bei der Anmeldung über die verschlüsselte Verbindung an den Server übertragen und dort geprüft, aber nicht gespeichert; gespeichert wird nur ein Prüfwert.
- Jede neu angelegte Klasse hat einen eigenen Klassenschlüssel; ältere Klassen und die Klassenkasse hängen am persönlichen Schlüssel der Lehrperson. Damit Klassen innerhalb der Schule geteilt und übergeben werden können, ist der Klassenschlüssel zusätzlich mit dem Schulschlüssel hinterlegt. Der Schulschlüssel liegt verschlüsselt auf dem Server.
- Ein technischer Zugriff des Auftragnehmers auf verschlüsselte Inhalte ist damit nicht ausgeschlossen: über den Schulschlüssel, und weil der Server die Anwendung ausliefert und das Passwort bei der Anmeldung prüft. Der Auftragnehmer nimmt einen solchen Zugriff nicht vor, außer der Auftraggeber weist ihn dazu an oder eine gesetzliche Pflicht verlangt es. In Datenbank und Sicherungen sind Inhalte, die nur am persönlichen Schlüssel hängen, ohne das Passwort der Lehrperson nicht lesbar.
- Unverschlüsselt gespeicherte Angaben zu Schülerinnen und Schülern hängen an einer internen Nummer statt am Namen.
- Die Übertragung erfolgt ausschließlich über HTTPS (TLS 1.2 oder 1.3).

2. Zugang zur Anwendung

- Persönliches Konto je Lehrperson, Anmeldung mit Benutzername und Passwort, optional mit zweitem Faktor (TOTP).
- Sperre der IP-Adresse für 15 Minuten nach fünf fehlgeschlagenen Anmeldungen.
- Die Anwendung meldet nach einer Stunde ohne Verbindung ab; das Sitzungs-Cookie gilt höchstens acht Stunden, ist für Skripte nicht lesbar und wird nur über HTTPS und nur an SkooBase gesendet.
- Persönliches Sicherheitswort bei der Anmeldung als Schutz vor gefälschten Anmeldeseiten.

3. Zugriff und Trennung

- Der Server liefert jeder Lehrperson nur ihre eigenen Klassen und die Klassen, die ihr ausdrücklich freigegeben wurden. Freigaben lassen sich auf einzelne Module beschränken und jederzeit zurücknehmen.
- Die Daten verschiedener Schulen sind logisch getrennt; gemeinsame Bereiche sind nur für Angehörige der jeweiligen Schule abrufbar. Was Lehrpersonen eintragen, ist über Schulgrenzen hinweg nicht sichtbar.
- Einer Schule ordnet sich zu, wer deren Schulkennzahl angibt und eine E-Mail-Adresse bestätigt. Hat die Schule in SkooBase eine Schulleitung oder Schuladministration hinterlegt, erfährt diese per E-Mail, wenn sich jemand neu der Schule zuordnet; die Schuladministration kann das Konto sperren.

4. Server und Betrieb

- Eigener virtueller Server in einem Rechenzentrum in Deutschland (siehe Anlage 3), keine geteilte Datenbank mit anderen Kunden des Hosting-Anbieters.
- Firewall, Verwaltungszugang nur mit kryptografischem Schlüssel, automatische Sperre bei wiederholten Angriffen, automatische Sicherheitsupdates.
- Administrativen Zugang hat ausschließlich der Auftragnehmer.
- Die Anwendung lädt Skripte, Schriften und Stile nur vom eigenen Server; es sind keine Analyse-, Werbe- oder Tracking-Dienste eingebunden.
- Fehlermeldungen an Lehrpersonen enthalten keine Datenbankinhalte.

5. Verfügbarkeit und Wiederherstellung

- Tägliche Datensicherung auf dem Server, Aufbewahrung rund 14 Tage.
- Tägliche zusätzlich verschlüsselte Kopie (AES-256) außerhalb des Servers, gespeichert innerhalb der EU; den Schlüssel dazu hat nur der Auftragnehmer. Aufbewahrung rund 30 Tage.
- Sicherungen, die vor einer Programmänderung entstehen, werden nach rund einer Woche gelöscht.
- Dokumentierter Ablauf für die Wiederherstellung auf einem neuen Server.
- Jede Lehrperson kann die Daten ihrer Klassen während der Laufzeit zusätzlich selbst als Sicherung exportieren.

6. Nachvollziehbarkeit und Überprüfung

- Protokolliert wird, wann eine Lehrperson eine Klasse exportiert, eine Sicherung heruntergeladen oder eingespielt hat (Aufbewahrung 13 Monate), sowie die Zeitpunkte der Anmeldungen (13 Monate).
- Die Datensicherung prüft sich bei jedem Lauf selbst und protokolliert Abweichungen. Die Verwahrung der Schulschlüssel wird täglich geprüft; bei Auffälligkeiten erhält der Auftragnehmer eine E-Mail.
- Regelmäßige Durchsicht des Programmcodes nach einer festen Liste bekannter Fehlerarten vor jeder Veröffentlichung.

Anlage 3 - Weitere Auftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
World4You Internet Services GmbH Wolfgang-Pauli-Straße 2, BT3 4020 Linz, Österreich	Hosting: virtueller Server, auf dem Anwendung und Datenbank laufen; Versand der System-E-Mails von SkooBase	Österreich, Deutschland
IONOS SE Elgendorfer Straße 57 56410 Montabaur, Deutschland	Betrieb des Rechenzentrums und der Server-Infrastruktur im Auftrag von World4You	Deutschland

Mit World4You besteht ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO; IONOS SE ist darin als weiterer Auftragsverarbeiter genannt.

Kein Auftragsverarbeiter im Sinne dieser Vereinbarung ist der Zahlungsdienstleister (Lemon Squeezy). Er erhält keine Daten von Schülerinnen, Schülern oder Erziehungsberechtigten und verarbeitet die Zahlungsdaten der Käuferin oder des Käufers in eigener Verantwortung (siehe Datenschutzerklärung).