Vereinbarung zur Auftragsverarbeitung

gem. Art. 28 EU-DSGVO

Auftragsverarbeiter:
Schoolhouse Software e.K.
Inhaber: Mark Lemke
An der Veerse 2a
29640 Schneverdingen
E-Mail: kontakt@schoolhouse.de

Verantwortlicher:
Die Schule bzw. Institution, die eine Lizenz für *TLH-Team* erworben hat, vertreten durch deren Leitung oder einen bevollmächtigten Angestellten (nachfolgend *Verantwortlicher*).

1. Grundlegendes

Die europäische Datenschutzgrundverordnung (EU-DSGVO) definiert in Art. 4 (1) den Begriff *personenbezogene Daten*. Sobald personenbezogene Daten verarbeitet werden - darunter fällt nach Art. 4 (2) auch die Speicherung - müssen die Rechtsgrundsätze der EU-DSGVO eingehalten werden.

Verschlüsselte Daten fallen nach Art. 4 (5) EU-DSGVO unter den Begriff *pseudonymisierte Daten*, deren Verarbeitung weniger strenge Auflagen hat. Dennoch unterliegt auch die Verarbeitung pseudonymisierter Daten der EU-DSGVO. Im Folgenden wird der Einfachheit halber nur von personenbezogenen Daten gesprochen, auch wenn pseudonymisierte Daten gemeint sind.

Sobald personenbezogene Daten vom Verantwortlichen an einen Auftragsverarbeiter übermittelt werden, liegt eine Auftragsverarbeitung vor, die nach Art. 28 (3) EU-DSGVO nur auf Grundlage einer Vereinbarung erfolgen darf. Die Begriffe *Verantwortlicher* und *Auftragsverarbeiter* sind in Art. 4 (7) und (8) EU-DSGVO definiert.

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragsverarbeiter nicht bestellt, da die gesetzliche Notwendigkeit hierfür nicht vorliegt.

2. Gegenstand und Dauer der Verarbeitung

Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Nutzung der Software *TLH-Team* sowie der damit verbundenen Supportleistungen.

TLH-Team ist eine webbasierte Software zur Schülerverwaltung und zum Zeugnisdruck. Die personenbezogenen Daten werden verschlüsselt auf Servern des Unterauftragsverarbeiters Microsoft (Microsoft Azure, Rechenzentrumsregion Germany West Central) gespeichert.

Im Rahmen des Supports können folgende Verarbeitungen stattfinden:

- Fernwartung über die Software *TeamViewer* zur Hilfestellung bei Problemen. Die Verbindung wird grundsätzlich vom Anwender initiiert, indem die Software gestartet und dem Auftragsverarbeiter per Telefon das temporäre Passwort mitgeteilt wird.

- Erstellung eines Benutzerkontos für den Auftragsverarbeiter durch einen Administrator der Schule, um direkten Zugriff auf die Datenbank zur Problemlösung zu ermöglichen. Dieser Zugriff erfolgt ausschließlich auf ausdrückliche Veranlassung des Verantwortlichen.
- Upload verschlüsselter Daten durch den Anwender auf das OneDrive Business des Auftragsverarbeiters zur Analyse. Die Verschlüsselung der Daten vor dem Upload obliegt dem Anwender.

Die Dauer der Verarbeitung ist an die Laufzeit des Lizenzvertrages gebunden und endet mit Kündigung des Vertrages bzw. Einstellung der Zahlung des jährlichen Beitrags, vorbehaltlich der in Abschnitt 10 genannten Aufbewahrungsfristen.

3. Art und Zweck der Verarbeitung

TLH-Team dient der Schülerverwaltung und dem Zeugnisdruck. Die Software ermöglicht es den Anwendern, Schülerdaten zu erfassen, zu verwalten und Zeugnisse zu erstellen. Um die Sicherheit zu gewährleisten, werden sämtliche Daten über eine sichere Verbindung (HTTPS) übertragen und vor der Übertragung clientseitig verschlüsselt. Personenbezogene Daten werden zusätzlich Ende-zu-Ende verschlüsselt.

Die Fernwartung über *TeamViewer* dient dazu, bei Problemen schnelle und präzise Hilfestellung zu ermöglichen. Ein Supportmitarbeiter kann dabei den Bildschirminhalt des Anwenders sehen und optional dessen Maus und Tastatur übernehmen. Der Anwender kann die Steuerungsübernahme jederzeit deaktivieren.

Der direkte Datenbankzugriff über ein vom Verantwortlichen bereitgestelltes Benutzerkonto dient ausschließlich der Fehlerdiagnose und Problemlösung.

Der Upload verschlüsselter Daten auf OneDrive Business dient der Analyse und Behebung von Problemen, die sich nicht anderweitig lösen lassen.

4. Art der personenbezogenen Daten

Folgende Kategorien personenbezogener Daten können verarbeitet werden:

- Kontaktdaten der Schüler
- Identifikationsmerkmale der Schüler
- Religionszugehörigkeiten
- Schülerbilder
- Noten und Beurteilungen
- Ankreuzzeugnisse
- Dokumentationen und Beratungsprotokolle
- Kontaktdaten der Erziehungsberechtigten
- Kontaktdaten der Notfallkontakte
- Namen und Kürzel der Klassenlehrer

Es ist nicht möglich, exakt anzugeben, welche personenbezogenen Daten bei der Nutzung von *TeamViewer* oder bei einem direkten Datenbankzugriff sichtbar werden. Es können sich darunter die oben genannten Daten befinden.

Gleiches gilt für Daten, die vom Anwender verschlüsselt auf OneDrive Business hochgeladen werden.

5. Kategorien betroffener Personen

Die verarbeiteten personenbezogenen Daten beziehen sich auf:

- Schülerinnen und Schüler
- Erziehungsberechtigte
- Notfallkontakte
- Klassenlehrerinnen und Klassenlehrer

6. Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter hat folgende technische und organisatorische Maßnahmen gemäß Art. 32 EU-DSGVO getroffen:

6.1 Verschlüsselung

- Sämtliche Daten werden vor der Übertragung clientseitig mittels **AES-256** (CBC-Modus, PKCS7-Padding, zufälliger Initialisierungsvektor) verschlüsselt.
- Personenbezogene Daten werden zusätzlich Ende-zu-Ende verschlüsselt unter Verwendung von **Elliptic Curve Cryptography (ECC)** mit der Kurve **brainpoolP512r1**, wie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen.
- Die Ableitung des Passworts erfolgt mittels **PBKDF2**.
- Die Übertragung jeglicher Daten erfolgt ausschließlich über **HTTPS**.
- Ruhende Daten in Azure Storage sind zusätzlich durch **AES-Verschlüsselung** auf Speicherebene geschützt.

6.2 Authentifizierung und Schlüsselverwaltung

- Das Passwort des Anwenders erreicht zu keinem Zeitpunkt den Server. Stattdessen wird lediglich eine kryptografische Ableitung des Passworts übermittelt.
- Bei der Kontoerstellung wird ein ECC-Schlüsselpaar erzeugt. Der öffentliche Schlüssel, die ECC-Parameter sowie die PBKDF2-Parameter werden zusammen mit der Passwort-Ableitung auf dem Server gespeichert.
- Der private Schlüssel wird vor der serverseitigen Speicherung mit einer weiteren Ableitung des Passworts verschlüsselt, die nicht an den Server übermittelt wird.
- Sämtliche personenbezogenen Daten werden mit einem zufällig generierten Schlüssel verschlüsselt. Dieser Schlüssel wird mit dem privaten ECC-Schlüssel verschlüsselt und ist für alle Anwender einer Schule (eines Kunden) identisch.
- Das Login erfolgt mit Kundennummer, Benutzername und der Passwort-Ableitung. Nach erfolgreicher Authentifizierung wird ein Bearer-Token ausgestellt, das mittels **HMAC-SHA-256** auf Basis der Passwort-Ableitung verifiziert wird.

6.3 Infrastruktur und Verfügbarkeit

- Die Datenspeicherung erfolgt in **Microsoft Azure**, Rechenzentrumsregion **Germany West Central** (Frankfurt), mit geo-redundanter Replikation (**RA-GRS**).
- Es werden **Azure Tables** und **Azure Blobs** als Speicherdienste verwendet.
- Das Backend läuft als **Azure Function** in derselben Region.

- Das Frontend ist als **WebAssembly-Anwendung (WASM)** realisiert und wird vollständig im Browser des Anwenders ausgeführt; eine serverseitige Verarbeitung personenbezogener Daten durch das Frontend findet nicht statt.
- Zusätzlich zur Redundanz durch Azure wird alle **12 Stunden** ein vollständiges Backup aller Daten angelegt.

6.4 Protokollierung

- **Application Insights** ist aktiv. Der Standort des Anwenders wird dabei erfasst, IP-Adressen werden jedoch anonymisiert (als 0.0.0.0) gespeichert.

6.5 Organisatorische Maßnahmen

- Der Auftragsverarbeiter ist ein Einzelunternehmen. Der Zugang zu Verwaltungskonten und Systemen ist ausschließlich dem Inhaber vorbehalten.
- Die Arbeitsumgebung befindet sich in einem nicht öffentlich zugänglichen Büro.

7. Unterauftragsverhältnisse

Der Auftragsverarbeiter setzt folgende Unterauftragsverarbeiter ein:

- **Microsoft Corporation** - Bereitstellung der Cloud-Infrastruktur (Azure: Datenspeicherung, Compute, Application Insights) sowie OneDrive Business (Office 365/SharePoint) für den verschlüsselten Datenaustausch im Rahmen des Supports. Ein entsprechender Auftragsverarbeitungsvertrag (Microsoft Data Protection Addendum) liegt vor.

Sollten sich die Unterauftragsverhältnisse ändern, wird der Verantwortliche vorab informiert. Die Änderung bedarf der Zustimmung des Verantwortlichen.

8. Kontrollrechte des Verantwortlichen

Der Verantwortliche hat das Recht, die Einhaltung dieser Vereinbarung und der datenschutzrechtlichen Vorgaben zu überprüfen. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 EU-DSGVO niedergelegten Pflichten zur Verfügung zu stellen.

Die Kontrolle erfolgt in der Regel durch:

- Schriftliche Auskunft des Auftragsverarbeiters zu den getroffenen technischen und organisatorischen Maßnahmen.
- Beantwortung von Fragebögen und Checklisten des Verantwortlichen.
- Vorlage relevanter Zertifizierungen oder Nachweise der eingesetzten Unterauftragsverarbeiter (insbesondere Microsoft Azure).

Da die personenbezogenen Daten ausschließlich verschlüsselt in der Cloud-Infrastruktur des Unterauftragsverarbeiters gespeichert werden und der Auftragsverarbeiter in nicht öffentlichen Räumen tätig ist, ist eine Vor-Ort-Kontrolle weder vorgesehen noch erforderlich. Sollte der Verantwortliche dennoch eine weitergehende Prüfung für notwendig erachten, ist diese nach angemessener Vorankündigung und in gegenseitigem Einvernehmen zu vereinbaren.

9. Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen dieser Vereinbarung und auf Weisung des Verantwortlichen zu verarbeiten. Eine Verarbeitung für eigene Zwecke findet nicht statt.
2. Erhält der Auftragsverarbeiter einen behördlichen Auftrag, Daten des Verantwortlichen herauszugeben, so hat er - sofern gesetzlich zulässig - den Verantwortlichen unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.
3. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass alle mit der Datenverarbeitung beauftragten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Diese Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.
4. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 EU-DSGVO ergriffen hat.
5. Der Auftragsverarbeiter ergreift die technischen und organisatorischen Maßnahmen, damit der Verantwortliche die Rechte der betroffenen Personen innerhalb der gesetzlichen Fristen jederzeit erfüllen kann, und stellt dem Verantwortlichen alle dafür notwendigen Informationen zur Verfügung.
6. Wird ein Antrag einer betroffenen Person an den Auftragsverarbeiter gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Verantwortlichen hält, leitet der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiter und informiert den Antragsteller entsprechend.
7. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 EU-DSGVO genannten Pflichten.
8. Der Auftragsverarbeiter führt ein Verarbeitungsverzeichnis nach Art. 30 EU-DSGVO.
9. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Ansicht ist, dass eine Weisung des Verantwortlichen gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.
10. Im Falle einer Datenschutzverletzung informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Bekanntwerden, und unterstützt ihn bei der Erfüllung der Meldepflichten nach Art. 33 und 34 EU-DSGVO.
11. Im Falle einer Inanspruchnahme des Verantwortlichen durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 EU-DSGVO verpflichtet sich der Auftragsverarbeiter, den Verantwortlichen im Rahmen seiner Möglichkeiten zu unterstützen.

10. Datenherausgabe, Löschung und Recht auf Vergessenwerden

Der Verantwortliche kann personenbezogene Daten jederzeit über die Software *TLH-Team* einsehen, berichtigen und löschen, soweit die Software diese Funktionalität bereitstellt.

Benutzerkonten können jederzeit durch einen Administrator der Schule gelöscht werden.

Nach Beendigung des Vertragsverhältnisses besteht die Möglichkeit, alle Daten in Form eines verschlüsselten ZIP-Archivs im CSV-Format zu erhalten. Dies muss explizit beim Auftragsverarbeiter angefordert werden.

Nach Vertragsende werden sämtliche Daten des Verantwortlichen - sofern nicht ausdrücklich anders gewünscht - noch 365 Tage aufbewahrt, um eine versehentliche Datenlöschung oder einen erneuten Bedarf zu ermöglichen. Nach Ablauf dieser Frist werden die Daten unwiderruflich gelöscht.

Durch die Nutzung von *TeamViewer* werden auf Seiten des Auftragsverarbeiters keine personenbezogenen Daten dauerhaft gespeichert.

Auf OneDrive Business hochgeladene Daten werden nach Abschluss der Analyse unverzüglich gelöscht.

11. Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich.
2. Der Verantwortliche hat ein Verarbeitungsverzeichnis nach Art. 30 EU-DSGVO zu führen.
3. Der Verantwortliche hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.
4. Der Verantwortliche stellt sicher, dass Daten, die zum Zwecke des Supports auf OneDrive Business hochgeladen werden, vor dem Upload ordnungsgemäß verschlüsselt sind.
5. Die Erstellung eines Benutzerkontos für den Auftragsverarbeiter zur Problemlösung erfolgt ausschließlich auf Veranlassung und in Verantwortung des Verantwortlichen. Der Verantwortliche kann dieses Benutzerkonto jederzeit wieder löschen.
6. Im Falle einer Inanspruchnahme des Verantwortlichen durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 EU-DSGVO gilt Abschnitt 9, Punkt 11 dieser Vereinbarung entsprechend.

12. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragsverarbeiter, wird dieser die betroffene Person an den Verantwortlichen verweisen, sofern eine Zuordnung nach Angaben der betroffenen Person möglich ist. Der Auftragsverarbeiter leitet den Antrag unverzüglich an den Verantwortlichen weiter und unterstützt diesen im Rahmen seiner Möglichkeiten. Der Auftragsverarbeiter haftet nicht, wenn das Ersuchen der betroffenen Person vom Verantwortlichen nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

13. Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

Es gilt das Recht der Bundesrepublik Deutschland.

Schoolhouse Software e.K.
15.04.2026