

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

1. Präambel

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV“) wird geschlossen zwischen:

Auftraggeber (Verantwortlicher):

Die Schule bzw. Lehrkraft, die ClassCheck nutzt und Schülerdaten in die Plattform eingibt (nachfolgend „Auftraggeber“).

Auftragnehmer (Auftragsverarbeiter):

E.L. Lernkartei-Erfassungsdienste e.U.

Laudongasse 5/2

1080 Wien, Österreich

FN 670623 k, Handelsgericht Wien

E-Mail: hi@classcheck.net

(nachfolgend „Auftragnehmer“)

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Rahmen der Bereitstellung der Beurteilungsplattform ClassCheck. Dieser AVV konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien gemäß Art. 28 DSGVO.

2. Gegenstand und Dauer der Verarbeitung

Gegenstand: Der Auftragnehmer stellt die webbasierte Beurteilungsplattform ClassCheck bereit, über die Lehrkräfte Schülerbeurteilungen und -noten verwalten können. Im Rahmen dieser Dienstleistung werden personenbezogene Daten der Schüler*innen verarbeitet.

Dauer: Dieser AVV gilt für die gesamte Dauer der Nutzung von ClassCheck durch den Auftraggeber. Er endet automatisch mit der Beendigung des Nutzungsverhältnisses oder der Löschung des Kontos.

3. Art und Zweck der Verarbeitung

Die Verarbeitung dient folgenden Zwecken:

- Bereitstellung und Betrieb der Beurteilungsplattform ClassCheck
- Verwaltung von Benutzerkonten (Lehrkräfte)
- Speicherung und Verwaltung von Schülernamen, Beurteilungen, Noten und Notizen
- Erstellung von Beurteilungsübersichten und Berichten
- Verwaltung von Klassen und Fächern

Die Verarbeitung umfasst insbesondere das Erheben, Speichern, Verändern, Auslesen, Abfragen, Verwenden und Löschen personenbezogener Daten.

Besonderheit Ende-zu-Ende-Verschlüsselung: Sensible Schülerdaten (Schülernamen, Beurteilungen/Noten, Notizen) werden clientseitig im Browser der Lehrkraft verschlüsselt, bevor sie an den Server übertragen werden. Der Auftragnehmer hat keinen Zugang zu diesen Daten im Klartext. Dies stellt eine zusätzliche technische Schutzmaßnahme dar, die über die Anforderungen des Art. 32 DSGVO hinausgeht.

4. Art der personenbezogenen Daten

Im Rahmen der Auftragsverarbeitung werden folgende Kategorien personenbezogener Daten verarbeitet:

- **Kontodaten:** E-Mail-Adressen, Passwörter (verschlüsselt gespeichert), Namen
 - **Schülerdaten (E2E-verschlüsselt):** Schülernamen, Beurteilungen/Noten, Notizen der Lehrkraft
 - **Organisationsdaten:** Klassenzugehörigkeit, Fächer, Beurteilungsperioden
 - **Technische Daten:** IP-Adressen, Gerätetyp, Sitzungsdaten (zur Sicherheit und Missbrauchsverhinderung)
-

5. Kategorien betroffener Personen

- **Schüler*innen:** Minderjährige und ggf. volljährige Lernende, deren Beurteilungsdaten in der Plattform verwaltet werden
 - **Lehrkräfte:** Pädagogisches Personal, das die Plattform zur Verwaltung von Beurteilungen nutzt
-

6. Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich:

6.1 Weisungsgebundenheit

Personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers zu verarbeiten (Art. 28 Abs. 3 lit. a DSGVO), es sei denn, eine Verarbeitung ist nach Unionsrecht oder dem Recht eines Mitgliedstaates erforderlich. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

6.2 Vertraulichkeit

Sicherzustellen, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

6.3 Technisch-organisatorische Maßnahmen

Alle gemäß Art. 32 DSGVO erforderlichen technisch-organisatorischen Maßnahmen zu ergreifen (siehe Abschnitt 8 dieses Vertrages).

6.4 Unterauftragsverarbeiter

Keine weiteren Auftragsverarbeiter ohne vorherige schriftliche Genehmigung des Auftraggebers einzusetzen (siehe Abschnitt 7 dieses Vertrages).

6.5 Unterstützung des Auftraggebers

Den Auftraggeber bei der Erfüllung seiner Pflichten bezüglich Betroffenenrechten (Art. 15–22 DSGVO), Datensicherheit (Art. 32 DSGVO), Meldung von Datenschutzverletzungen (Art. 33–34 DSGVO) und Datenschutz-Folgenabschätzungen (Art. 35–36 DSGVO) zu unterstützen.

6.6 Meldung von Datenschutzverletzungen

Den Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden, über jede Verletzung des Schutzes personenbezogener Daten zu informieren (Art. 33 Abs. 2 DSGVO).

7. Unterauftragsverarbeiter

Der Auftraggeber erteilt dem Auftragnehmer hiermit eine allgemeine schriftliche Genehmigung zur Beauftragung weiterer Auftragsverarbeiter. Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern. Der Auftraggeber kann gegen solche Änderungen Einspruch erheben.

Derzeit werden folgende Unterauftragsverarbeiter eingesetzt:

Unterauftragnehmer	Zweck	Standort
Hetzner Online GmbH	Hosting und Infrastruktur (Server, Datenbank)	Deutschland (EU)
Stripe, Inc.	Zahlungsabwicklung (nur bei kostenpflichtigen Funktionen)	USA (EU-Standardvertragsklauseln)

Der Auftragnehmer stellt sicher, dass mit allen Unterauftragsverarbeitern Verträge geschlossen werden, die den gleichen Datenschutzstandards wie dieser AVV entsprechen.

8. Technisch-organisatorische Maßnahmen (TOM)

Der Auftragnehmer hat folgende technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO implementiert:

8.1 Vertraulichkeit

- SSL/TLS-Verschlüsselung aller Datenübertragungen (HTTPS)
- Ende-zu-Ende-Verschlüsselung (AES-256) aller sensiblen Schülerdaten
- Passwörter werden mit bcrypt gehasht und niemals im Klartext gespeichert
- Zugriffskontrolle durch rollenbasierte Berechtigungen
- Sitzungsverwaltung mit httpOnly-Cookies

8.2 Integrität

- Parametrisierte Datenbankabfragen zum Schutz vor SQL-Injection
- CSRF-Schutz (Cross-Site Request Forgery) bei allen Formularen
- Input-Validierung und -Sanitisierung aller Nutzereingaben
- Security-Header (CSP, X-Frame-Options, etc.)

8.3 Verfügbarkeit und Belastbarkeit

- Hosting auf dedizierten Servern bei Hetzner in Deutschland
- Regelmäßige Datensicherungen (Backups) der Datenbank
- Prozessmanagement mit automatischem Neustart bei Ausfällen

8.4 Wiederherstellbarkeit

- Datenbank-Backups ermöglichen die Wiederherstellung im Fehlerfall
- Versionskontrolle der Anwendung zur schnellen Wiederherstellung

8.5 Überprüfung und Bewertung

- Rate-Limiting zum Schutz vor Brute-Force-Angriffen auf Login und API-Endpunkte
- Kontosperrung nach wiederholten fehlgeschlagenen Anmeldeversuchen
- Regelmäßige Sicherheits-Updates der eingesetzten Software

9. Rechte und Pflichten des Auftraggebers

Der Auftraggeber ist im Rahmen dieses Vertrags verantwortlich für:

- Die Rechtmäßigkeit der Datenverarbeitung gemäß Art. 6 und Art. 9 DSGVO
- Die Information der betroffenen Personen gemäß Art. 13 und Art. 14 DSGVO
- Die Einholung erforderlicher Einwilligungen (insbesondere bei Minderjährigen unter 16 Jahren gemäß Art. 8 DSGVO)
- Die Erteilung von Weisungen an den Auftragnehmer bezüglich der Datenverarbeitung
- Die sichere Aufbewahrung des Wiederherstellungsschlüssels (bei Verlust können E2E-verschlüsselte Daten nicht wiederhergestellt werden)

Der Auftraggeber hat das Recht, dem Auftragnehmer jederzeit Weisungen bezüglich Art, Umfang und Verfahren der Datenverarbeitung zu erteilen.

10. Löschung und Rückgabe von Daten

Nach Beendigung des Nutzungsverhältnisses oder auf Weisung des Auftraggebers wird der Auftragnehmer alle personenbezogenen Daten löschen, sofern keine gesetzliche Aufbewahrungspflicht besteht.

Die Löschung erfolgt wie folgt:

- **Kontolöschung durch Lehrkraft:** Alle personenbezogenen Daten einschließlich aller Klassen, Schüler*innen und Beurteilungen werden unwiderruflich gelöscht.
- **Datenexport:** Vor der Löschung kann der Auftraggeber über die Kontoeinstellungen einen Export aller Daten im JSON-Format anfordern.

Auf Verlangen bestätigt der Auftragnehmer dem Auftraggeber die vollständige Löschung der Daten schriftlich.

Hinweis zur E2E-Verschlüsselung: Da sensible Schülerdaten Ende-zu-Ende verschlüsselt sind, hat der Auftragnehmer ohnehin keinen Zugang zu den Daten im Klartext. Die Löschung entfernt auch die verschlüsselten Daten vollständig vom Server.

11. Kontroll- und Prüfungsrechte

Der Auftraggeber hat das Recht, die Einhaltung der in diesem AVV festgelegten Pflichten durch den Auftragnehmer zu überprüfen (Art. 28 Abs. 3 lit. h DSGVO). Dazu gehören:

- Das Recht, Auskünfte und Nachweise über die getroffenen technisch-organisatorischen Maßnahmen einzuholen
- Das Recht, Inspektionen durchzuführen oder durch einen beauftragten Prüfer durchführen zu lassen, nach angemessener Vorankündigung und unter Wahrung der Geschäftsgeheimnisse des Auftragnehmers
- Das Recht, relevante Dokumentationen einzusehen

Der Auftragnehmer unterstützt den Auftraggeber bei der Durchführung von Überprüfungen und stellt die erforderlichen Informationen zur Verfügung.

12. Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Jede Partei haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wird.

Der Auftragnehmer haftet für den durch die Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen ist oder wenn er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

13. Schlussbestimmungen

- Dieser AVV unterliegt österreichischem Recht.
- Gerichtsstand ist Wien, Österreich.
- Änderungen und Ergänzungen dieses AVV bedürfen der Schriftform.
- Sollte eine Bestimmung dieses AVV unwirksam oder undurchführbar sein, so wird die Wirksamkeit der übrigen Bestimmungen hiervon nicht berührt.
- Dieser AVV ist Bestandteil der Nutzungsbedingungen von ClassCheck und tritt mit Beginn der Nutzung der Plattform in Kraft.

Kontakt und unterzeichnete Fassung

Für Rückfragen zum AVV oder um eine individuell unterzeichnete Fassung dieses Vertrages anzufordern, wenden Sie sich bitte an:

E.L. Lernkartei-Erfassungsdienste e.U.

E-Mail: hi@classcheck.net