Vereinbarung über eine

Auftragsverarbeitung nach Art. 28 DSGVO

abgeschlossen zwischen

Daten der verantwortlichen und weisungsberechtigten Person (Pflichtfeld*)
(Unternehmensleitung, Schulleitung, Administrator, Lehrperson)

Name der Institution*:	
Vor- und Zuname*:	
Funktion der Person:	
Straße, Hausnummer*:	
PLZ, Ort*:	
Land/Staat:	
E-Mail-Adresse*:	

(im Folgenden als „Verantwortlicher“ bezeichnet)

und

GeoGraSim (geograsim.at)
Schroffenegger & Mößlang GesbR
Gerbergasse 24
6850 Dornbirn, Österreich
support@geograsim.at
(im Folgenden als „**Auftragsverarbeiter**“ bezeichnet)

gemeinsam kurz: die „**Parteien**“

Wichtiger Hinweis:

Bitte die Daten des Verantwortlichen vollständig ausfüllen und den Vertrag mit Ort, Datum und Unterschrift an support@geograsim.at senden. Eine elektronische Unterschrift (z. B. ID Austria / Handy-Signatur) oder eine eingescannte Unterschrift genügt (Art. 28 Abs. 9 DSGVO). Der Vertrag wird wirksam, sobald er vom Auftragsverarbeiter gegengezeichnet an den Verantwortlichen zurückgesendet wurde. Hinweis: Für Schulen, die GeoGraSim über den Marktplatz Lernapps beziehen, gilt bereits der Vertrag zur Auftragsverarbeitung zwischen dem Auftragsverarbeiter und dem Bundesministerium für Bildung; dieser Vertrag ist dann nicht erforderlich.

Verwendete E-Mail-Adressen (Benutzernamen) der Lehrpersonen können bei Bedarf als Liste im Anhang beigefügt werden.

1 Gegenstand dieser Vereinbarung

1.1 Der Verantwortliche beauftragt den Auftragsverarbeiter mit dem Betrieb der Lernplattform GeoGraSim und der Verarbeitung der Daten von Lehrpersonen und Schüler*innen laut der jeweils aktuellen Datenschutzerklärung (geograsim.at/datenschutz).

1.2 Die Daten folgender Kategorien von betroffenen Personen unterliegen der Verarbeitung: Lehrpersonen, Schüler*innen.

1.3 Im Rahmen der Datenanwendung verarbeitet der Auftragsverarbeiter folgende Datenkategorien für Lehrpersonen:
E-Mail-Adresse (zugleich Benutzername), Name, Schulname (optional), Passwort (nur als Hash), Klassen und Klassencodes, Lizenzzuordnungen, Zeitpunkte der Anmeldung.

1.4 Im Rahmen der Datenanwendung verarbeitet der Auftragsverarbeiter folgende Datenkategorien für Schüler*innen:
Benutzername (Pseudonym), PIN bzw. Passwort (nur als Hash), Vor- und Nachname (optional), E-Mail-Adresse (optional), Avatar, Klassenzugehörigkeit, Einstellungen zur Barrierefreiheit (z. B. Leichte Sprache, Nachteilsausgleich), Lern- und Aktivitätsdaten (Ergebnisse, Zeiten, Pausen, Zwischenstände während einer Sitzung, Reflexionstexte), Lizenzzuordnung.

2 Dauer der Vereinbarung

2.1 Die Verarbeitung auf Basis dieser Vereinbarung beginnt, wenn der vom Verantwortlichen vollständig ausgefüllte und unterschriebene Vertrag durch den Auftragsverarbeiter gegengezeichnet an den Verantwortlichen zurückgesendet wurde.

2.2 Die Vereinbarung gilt so lange, wie personenbezogene Daten verarbeitet werden. Die Verarbeitung beginnt mit der Eingabe der Daten und endet mit der Löschung der personenbezogenen Daten durch den Verantwortlichen (Lehrperson) oder bei eigenen Daten durch die einzelnen Benutzer*innen selbst.

2.3 Die Verarbeitung endet außerdem mit der Löschung nach den in der geltenden Datenschutzerklärung angegebenen Fristen: Konten von Lehrpersonen und Schüler*innen werden spätestens 28 Monate nach der letzten Anmeldung gelöscht; Lehrpersonen werden vorher per E-Mail informiert. Anonymisierte Auswertungen ohne Personenbezug bleiben davon unberührt.

2.4 Der Vertrag endet ebenso nach Beendigung des Angebotes durch den Auftragsverarbeiter welcher in diesem Fall alle personenbezogenen Daten auf Anfrage durch den Verantwortlichen 30 Tage lang zur Verfügung stellt.

3 Rechte und Pflichten des Auftragsverarbeiters und des Verantwortlichen

Solange der Auftragsverarbeiter die Datenanwendung betreibt und personenbezogene Daten für den Verantwortlichen verarbeitet, gelten in Entsprechung des Art 28 DSGVO folgende Bedingungen:

3.1 Der Auftragsverarbeiter verpflichtet sich, sämtliche gesetzliche Vorgaben der Datenschutz-Grundverordnung (DSGVO) zu beachten und Datenanwendungen (logisch und physisch) ausschließlich innerhalb der EU oder des EWR zu betreiben. Jede Form der Verlagerung der Datenanwendung (dazu zählt auch die Verlegung des Sitzes des Auftragsverarbeiters) in ein Drittland (außerhalb der EU oder des EWR) bedarf der ausdrücklichen, vorherigen schriftlichen Zustimmung durch den Verantwortlichen.

3.2 Der Auftragsverarbeiter verarbeitet die Daten ausschließlich zur Bereitstellung der Lernplattform für den Verantwortlichen, seine Lehrpersonen und Schüler*innen (Anmeldung, Lernen, Auswertung für die Lehrperson). Zudem verarbeitet der Auftragsverarbeiter Lernergebnisse in anonymisierter Form ohne Personenbezug für statistische Auswertungen zur Verbesserung des Programms und zur Lernforschung.

3.3 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.

3.4 Jede weitere Verarbeitung der Daten durch den Auftragsverarbeiter zu jeglichem Zwecke kann nur nach schriftlichem Auftrag durch den Verantwortlichen durchgeführt werden.

3.5 Der Auftragsverarbeiter gewährleistet, dass sich Personen, die Zugang zu den im Auftrag verarbeiteten Daten erhalten, vor Zugriff auf diese Daten schriftlich zur Vertraulichkeit verpflichten. Zudem bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit beim Auftragsverarbeiter aufrecht.

3.6 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Auftragsverarbeiter und der Verantwortliche verpflichteten sich, die in Anlage 1 aufgeführten Maßnahmen umzusetzen.

3.7 Die Verarbeitung von Daten in Privatwohnungen ist gestattet.

3.8 Zwischen dem Auftragsverarbeiter und sämtlichen Sub-Auftragsverarbeitern bestehen aufrechte Verträge zur Auftragsverarbeitung. Der Auftragsverarbeiter ist befugt, folgende Unternehmen als Sub-Auftragsverarbeiter einzusetzen:

Hosting der Webanwendung und der Datenbank, Domain, Versand von System-E-Mails:

World4You Internet Services GmbH, Wolfgang-Pauli-Straße 2, BT3, 4020 Linz, Österreich (FN 232485s). World4You betreibt den Server über ihren genehmigten Subauftragsverarbeiter IONOS SE (ISO/IEC 27001), Elgendorfer Straße 57, 56410 Montabaur, Deutschland; Rechenzentrum in Deutschland (EU).

Support-Postfach (Anfragen an support@geograsim.at, interne Benachrichtigungen):

Microsoft Ireland Operations Ltd. (ISO/IEC 27001), One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland; Datenhaltung in Rechenzentren in der EU (EU Data Boundary).

3.9 Beabsichtigte Änderungen oder die Hinzuziehung weiterer Sub-Auftragsverarbeiter gibt der Auftragsverarbeiter dem Verantwortlichen so rechtzeitig schriftlich (per E-Mail) bekannt, dass dieser widersprechen kann. Widerspricht der Verantwortliche, kann er die Vereinbarung ohne Nachteile beenden; der Auftragsverarbeiter stellt die Daten in diesem Fall 30 Tage lang zur Rückgabe bereit und löscht sie anschließend. Die jeweils aktuelle Liste der Sub-Auftragsverarbeiter steht in der Datenschutzerklärung.

3.10 Der Auftragsverarbeiter schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit den Sub-Auftragsverarbeitern ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters. Der Subauftragnehmer darf die Datenanwendung ausschließlich innerhalb der EU oder des EWR betreiben.

3.11 Der Auftragsverarbeiter wird den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person (Auskunft, Berichtigung und Löschung, Information, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) fristgerecht nachzukommen. Sollte sich ein Betroffener an den Auftragsverarbeiter oder einen Subauftragnehmer anstelle des Verantwortlichen wenden, verpflichten sich diese, den Antrag dem Verantwortlichen so zukommen zu lassen, dass der Verantwortlichen den Antrag fristgerecht bearbeiten kann.

3.12 Der Auftragsverarbeiter wird den Verantwortlichen bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Ergreifung technischer und organisatorischer Maßnahmen, Security Breach Notification, Erstellung einer Datenschutz Folgenabschätzung) bei Bedarf beratend unterstützen.

3.13 Der Auftragsverarbeiter wird nach Abschluss der Datenanwendung alle personenbezogenen Daten entweder laut der geltenden Datenschutzbestimmung löschen oder auf schriftliche Anfrage durch den Verantwortlichen zurückgeben.

3.14 Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der dem Auftragsverarbeiter in diesem Vertrag auferlegten Pflichten zur Verfügung zu stellen.

3.15 Sollte der Auftragsverarbeiter der Auffassung sein, dass eine vom Verantwortlichen gestellt Anfrage gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder deren Mitgliedstaaten verstößt, so hat er dies dem Verantwortlichen unverzüglich und begründet mitzuteilen.

3.16 Der Verantwortlichen ist berechtigt, die Einhaltung sämtlicher maßgeblichen datenschutzrechtlichen Vorschriften sowie die Einhaltung der vertraglichen Bestimmungen selbst oder durch Dritte beim Auftragsverarbeiter sowie allfälligen Subauftragnehmern zu kontrollieren. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

_____, den _____

Für den Verantwortlichen

_____

Name und Unterschrift

_____

Dornbirn, den _____

Für den Auftragsverarbeiter

_____

Name und Unterschrift
Thomas Schroffenegger, für die GesbR

Anlage 1 zum Vertrag zur Auftragsdatenverarbeitung

Technisch-Organisatorische-Maßnahmen

1 VERTRAULICHKEIT im Einflussbereich des Auftragsverarbeiters

- **Zutrittskontrolle**: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch Schlüssel, ISO 27001 Standard beim Hoster.
- **Zugangskontrolle**: Schutz vor unbefugter Systemnutzung, Kennwörter (einschließlich entsprechender Policy), Verschlüsselung der Datenübertragungen (SSL, HTTPS).
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch: Standardprozess für Berechtigungsvergabe, Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger, Datenschutzgerechte Wiederverwendung von Datenträgern, Clear-Desk/Clear-Screen Policy.
- **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt (Username ohne Personenbezug, Pseudonymisierung von Forschungsdaten)
- **Klassifikationsschema für Daten**: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

2 VERTRAULICHKEIT im Einflussbereich des Verantwortlichen

- **Zugangskontrolle**: Schutz vor unbefugter Systemnutzung durch die Verwendung eines entsprechenden Kennwortes für den Zugang als Administrator (einschließlich entsprechender Policy).
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems und außerhalb des Standardprozesses für Berechtigungsvergabe durch den Verantwortlichen.
- **Pseudonymisierung**: Je nach lokaler Gesetzeslage des Verantwortlichen und dem Alter der eingegebenen Personen entscheidet der Verantwortliche rechtskonform und in eigenen Verantwortung, ob er zur Nutzung des Systems mit personenbezogenen Daten oder ausschließliche mit pseudonymisierten Benutzerdaten berechtigt ist (anonymisierte primäre Identifikationsmerkmale der personenbezogenen Daten: nur intern bekannter Nickname/ID ohne Personenbezug, keine User-Mailadressen, keine echten Vor-/Nachnamen mit Personenbezug).

3 DATENINTEGRITÄT[1]

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport: Verschlüsselung von Daten, elektronische Signatur;
- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch Protokollierung.

4 VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Auftragsverarbeiter und Hostingpartner: Backup-Strategie (online, on-site/off-site, 24-stündig), unterbrechungsfreie Stromversorgung, Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene;
- **Logging, Metriken, Alerts;**
- Rasche **Wiederherstellbarkeit**;
- **Löschungsfristen:** Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

[1] Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

5 VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen/Besprechungen;
- Datenschutzfreundliche Voreinstellungen;
- Passwort Policy;
- Statistische Verfahren zur Beobachtung von Hackingversuchen;
- Regelmäßige Updates von Softwarekomponenten;
- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-27001 Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.