

Auftragsverarbeitungsvertrag

(AVV) gemäß Art. 28 DSGVO

zwischen

**Auftraggeber
(Schule):**

Schulname: _____
Schulleitung: _____
Adresse: _____
E-Mail: _____

Auftragnehmer:

Name: Nikola Iliev
Plattform: LehrerElternHub (lehrerelternhub.com)
Adresse: Borna, Sachsen, Deutschland
E-Mail: noreply@lehrerelternhub.com

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Gegenstand der Verarbeitung ist der Betrieb der Schulkommunikationsplattform LehrerElternHub.

(2) Die Dauer der Verarbeitung entspricht der Laufzeit des Nutzungsvertrags. Bei Beendigung werden alle Daten gemäß § 10 gelöscht.

(3) Die Verarbeitung erfolgt ausschließlich innerhalb der Europäischen Union (Server: Hetzner Cloud, Nürnberg, Deutschland).

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung umfasst folgende Tätigkeiten:

- Verwaltung von Benutzerkonten (Lehrkräfte und Eltern)
- Speicherung und Anzeige von Schülerdaten (Name, Avatar, Klassenzugehörigkeit)
- Verwaltung von Bewertungen, Krankmeldungen und Terminen
- Betrieb des FOREDU-Lernspiels (Spielcode, Teilnahme)
- Versand von transaktionalen E-Mails (Bestätigung, Passwort-Reset, Benachrichtigungen)

§ 3 Art der personenbezogenen Daten

Lehrkräfte: Vollständiger Name, E-Mail-Adresse, Schulname, Passwort (gehasht)

Eltern: Vollständiger Name, E-Mail-Adresse, Passwort (gehasht), DSGVO-Einwilligung

Schüler: Vorname, Nachname, Avatar (Emoji), LernSax-E-Mail (optional), Klassenzugehörigkeit, Bewertungen, Krankmeldungen, FOREDU-Spielfortschritt

§ 4 Kreis der betroffenen Personen

Betroffen sind: Lehrkräfte der Schule, Erziehungsberechtigte (Eltern) der Schüler, Schülerinnen und Schüler der teilnehmenden Klassen.

§ 5 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich:

- personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers zu verarbeiten (Art. 28 Abs. 3 lit. a DSGVO)
- alle mit der Verarbeitung betrauten Personen zur Vertraulichkeit zu verpflichten
- die gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zu treffen (siehe § 7)
- den Auftraggeber bei der Erfüllung seiner Pflichten nach Art. 32–36 DSGVO zu unterstützen
- nach Abschluss der Verarbeitung alle Daten zu löschen oder zurückzugeben (siehe § 10)
- dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten zur Verfügung zu stellen

§ 6 Besonderer Schutz von Kinderdaten (Art. 8 DSGVO)

- (1) Der Auftragnehmer ist sich bewusst, dass Daten von Kindern unter 16 Jahren verarbeitet werden und behandelt diese mit besonderer Sorgfalt.
- (2) Die Verarbeitung von Schülerdaten erfolgt nur mit Einwilligung der Erziehungsberechtigten. Diese Einwilligung wird bei der Registrierung elektronisch eingeholt.
- (3) Erziehungsberechtigte können ihre Einwilligung jederzeit widerrufen (Art. 7 Abs. 3 DSGVO). In diesem Fall werden alle Daten des betroffenen Kindes gelöscht.
- (4) Schülerdaten werden nicht an Dritte weitergegeben und nicht zu Werbezwecken oder Profiling verwendet.

§ 7 Technische und organisatorische Maßnahmen (TOMs)

Der Auftragnehmer setzt folgende Maßnahmen gemäß Art. 32 DSGVO um:

Maßnahme	Umsetzung
Verschlüsselung der Übertragung	SSL/TLS (Let's Encrypt) für alle Verbindungen
Passwort-Sicherheit	bcrypt-Hashing mit 12 Runden; Passwörter werden nie im Klartext gespeichert
Authentifizierung	JWT-Token mit 15-Minuten-Ablauf; Refresh-Token-Rotation
Serverstandort	Hetzner Cloud, Nürnberg, Deutschland (EU)
Datenbankzugriff	PostgreSQL nur über localhost erreichbar; kein externer Zugriff möglich
Zugriffskontrolle	Rollenbasiert: Lehrer sehen nur eigene Klasse; Eltern sehen nur Daten ihres eigenen Kindes
Tracking & Cookies	KEINE Cookies, KEIN Google Analytics, KEIN Tracking jeglicher Art
E-Mail-Versand	IONOS SMTP (smtp.ionos.de) — Server in Deutschland; kein Newsletter, keine Werbung
Protokollierung	Server-Logs werden für max. 30 Tage gespeichert und dann gelöscht
Löschkonzept	Nutzer können alle Daten selbst exportieren (Art. 15) und Löschung beantragen (Art. 17)
Subunternehmer	Hetzner Cloud (Hosting), IONOS (E-Mail/Domain) — beide mit Sitz in Deutschland

§ 8 Unterauftragsverhältnisse

Der Auftragnehmer setzt folgende Unterauftragnehmer ein:

- **Hetzner Online GmbH** (Industriestr. 25, 91710 Gunzenhausen) — Server-Hosting
- **IONOS SE** (Elgendorfer Str. 57, 56410 Montabaur) — Domain & E-Mail

Beide Unterauftragnehmer haben ihren Sitz in Deutschland und verarbeiten Daten ausschließlich innerhalb der EU.

§ 9 Rechte der betroffenen Personen

Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Betroffenenrechte:

- Auskunftsrecht (Art. 15 DSGVO) — Datenexport als JSON-Datei über die Plattform
- Recht auf Berichtigung (Art. 16 DSGVO) — Profilbearbeitung über die Plattform

- Recht auf Löschung (Art. 17 DSGVO) — Kontolöschung über die Plattform oder per E-Mail
- Recht auf Einschränkung (Art. 18 DSGVO) — auf Anfrage per E-Mail
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO) — JSON-Export aller Daten
- Widerspruchsrecht (Art. 21 DSGVO) — per E-Mail an noreply@lehrerelternhub.com

§ 10 Löschung und Rückgabe von Daten

- (1) Nach Beendigung des Vertragsverhältnisses löscht der Auftragnehmer alle im Auftrag verarbeiteten personenbezogenen Daten innerhalb von 30 Tagen.
- (2) Auf Wunsch des Auftraggebers können die Daten vor der Löschung in einem maschinenlesbaren Format (JSON) exportiert und übergeben werden.
- (3) Der Auftragnehmer bestätigt die vollständige Löschung schriftlich.

§ 11 Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, die Einhaltung dieses Vertrags zu überprüfen.
- (2) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zur Verfügung.

§ 12 Meldepflicht bei Datenschutzverletzungen

Der Auftragnehmer informiert den Auftraggeber unverzüglich (spätestens innerhalb von 24 Stunden) über Datenschutzverletzungen gemäß Art. 33 DSGVO per E-Mail.

Unterschriften

Ort, Datum:

Ort, Datum:

Auftraggeber (Schule)

Schulleitung / Stempel

Auftragnehmer

Nikola Iliev, LehrerElternHub