RECHTSSICHERER MUSTERVERTRAG FÜR SCHULEN & SCHULTRÄGER

Vereinbarung zur Auftragsverarbeitung (AVV)

gemäß Art. 28 der Datenschutz-Grundverordnung (DSGVO) über die Nutzung von Gradus21

AUFTRAGGEBER (SCHULE / SCHULTRÄGER):

Schule:

Straße & Hausnr.:

PLZ & Ort:

Vertreten durch:

AUFTRAGNEHMER:

Julian Kallidat (Gradus21)

Hardtstraße 6, 76467 Bietigheim, Deutschland
Telefon: +49 1520 3898458 • E-Mail: kontakt@gradus21.de • Web: https://gradus21.de
USt-IdNr.: Kleinunternehmer gem. § 19 UStG

§ 1 Gegenstand, Geltungsbereich und Dauer

(1) **Gegenstand des Auftrags:** Der Auftragnehmer stellt dem Auftraggeber die Software-Applikation (bereitgestellt als Web-Applikation sowie als native Desktop- und Mobil-Applikation für Windows, macOS, Linux, iOS/iPadOS und Android) und den Synchronisationsdienst „Gradus21“ zur pädagogischen Notenverwaltung, Leistungsdokumentation, Prüfungsberechnung und Datensicherung zur Verfügung.

(2) **Lokalbetrieb vs. Cloud-Sync:** Bei rein lokaler Speicherung verbleiben sämtliche Daten ausschließlich im lokalen Speicher des Dienstgeräts (z. B. IndexedDB im Web-Browser oder lokaler Sandbox-Datenspeicher der nativen Applikation; keine Auftragsverarbeitung). Die vorliegende Vereinbarung regelt die ergänzende Nutzung des verschlüsselten Cloud-Synchronisations- und Backup-Dienstes.

(3) **Laufzeit & Kündigung:** Diese Vereinbarung wird auf unbestimmte Zeit geschlossen. Sie kann von jeder Partei jederzeit mit einer Frist von einem Monat zum Monatsende in Textform gekündigt werden.

§ 2 Konkretisierung des Auftragsinhalts & Kategorien betroffener Daten

(1) **Art und Zweck der Verarbeitung:** Automatisierte Speicherung, verschlüsselte Synchronisation und Bereitstellung von Notenständen, Lerngruppen und Zeugnisnoten zur Erfüllung des pädagogischen Auftrags.

(2) **Kategorien betroffener Personen:** Lehrkräfte (Nutzer) sowie Schülerinnen und Schüler des Auftraggebers.

(3) **Arten der verarbeiteten Daten:**

- **Lehrkraft-Stammdaten:** E-Mail-Adresse, Kontokennung, Authentifizierungs-Token (Passkey / Master-Hash).
- **Schülerbezogene Daten:** Vor- und Nachname, Klasse/Lerngruppe, Fachbezeichnung, Prüfungsergebnisse, Zeugnisnoten, Fehlzeiten-/Attestvermerke (z. B. Status „K“).

Klarstellung zur Zero-Knowledge-Architektur (E2EE): Sämtliche schülerbezogenen Leistungs- und Stammdaten werden vor der Übertragung vollständig clientseitig auf dem Endgerät (im Browser bzw. in der nativen Applikation) mittels `AES-256-GCM` chiffriert. Der kryptografische Schlüssel (DEK) verlässt zu keinem Zeitpunkt das Dienstgerät der Lehrkraft. Der Auftragnehmer verarbeitet und speichert serverseitig ausschließlich unlesbaren Chiffretext.

§ 3 Weisungsgebundenheit des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist durch das Recht der Union oder der Mitgliedstaaten hierzu verpflichtet.

(2) Die Weisungen werden grundsätzlich durch die Konfiguration und Nutzung der Applikation (Web oder native App) durch die autorisierte Lehrkraft erteilt.

§ 4 Unterauftragsverhältnisse (Subunternehmer gem. Art. 28 Abs. 2 DSGVO)

(1) Der Auftraggeber genehmigt ausdrücklich die Beauftragung des folgenden Unterauftragsverarbeiters für das Server-Hosting:

Alfahosting GmbH, Ankerstraße 3b, 06108 Halle (Saale), Deutschland
Rechenzentrumsstandort: **Leipzig (Deutschland)** • ISO/IEC 27001 zertifiziert
Gegenstand: Bereitstellung von Server-Infrastruktur, Colocation, Strom- & Netzanbindung.

(2) Eine Datenübermittlung in Drittstaaten außerhalb der EU bzw. des EWR (insbesondere unter dem US CLOUD Act oder FISA 702) ist ausgeschlossen.

§ 5 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Sinne von Art. 4 Nr. 7 DSGVO verantwortliche Stelle für die Zulässigkeit der Datenverarbeitung im Rahmen der einschlägigen Landesschulgesetze.

(2) Dem Auftraggeber steht das Recht zu, die Einhaltung der technischen und organisatorischen Maßnahmen im erforderlichen Umfang zu überprüfen.

§ 6 Betroffenenrechte, Löschung und Rückgabe von Daten

(1) **Unterstützung bei Betroffenenrechten:** Soweit eine betroffene Person Anträge auf Auskunft (Art. 15), Berichtigung (Art. 16) oder Löschung (Art. 17) an den Auftragnehmer richtet, wird dieser das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) **Automatisierte 1-Klick-Löschung:** Die Lehrkraft kann über die Benutzeroberfläche der Web- oder Desktop-/Mobil-Applikation jederzeit sämtliche synchronisierten Server-Backups unwiderruflich und rückstandsfrei löschen.

(3) **Beendigung:** Nach Vertragsende werden alle auf den Servern verbleibenden verschlüsselten Sicherungskopien innerhalb von 30 Tagen endgültig vernichtet.

§ 7 Haftung und Schlussbestimmungen

(1) Die Haftung richtet sich nach Art. 82 DSGVO. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, berührt dies die Gültigkeit der übrigen Bestimmungen nicht.

(3) Es gilt ausschließlich das Recht der Bundesrepublik Deutschland.

Ort, Datum und rechtsverbindliche Zeichnung der Vertragsparteien gem. Art. 28 Abs. 9 DSGVO:

FÜR DEN AUFTRAGGEBER (SCHULE / SCHULTRÄGER):

Ort, Datum: .....

Name / Funktion: .....

Rechtsverbindliche Unterschrift (ggf. Schulstempel)

FÜR DEN AUFTRAGNEHMER (GRADUS21):

Ort, Datum: **Bietigheim, 01.08.2026**

Name: **Julian Kallidat** (Inhaber)

gez. Julian Kallidat ✓ Elektronisch gezeichnet

VERBINDLICHER ANHANG ZUM AVV • GÜLTIG FÜR DAS SCHULJAHR 2026/2027

Anlage 1: Technische und organisatorische Maßnahmen (TOM)

Sicherheitskonzept und Schutzmaßnahmen gemäß Art. 32 DSGVO

Der Auftragnehmer trifft und dokumentiert folgende angemessene technische und organisatorische Maßnahmen (TOM), um ein dem Risiko für die Rechte und Freiheiten der betroffenen Schülerinnen, Schüler und Lehrkräfte angemessenes Schutzniveau zu gewährleisten:

KATEGORIE & SCHUTZZIEL	KONKRETE TECHNISCHE & ORGANISATORISCHE UMSETZUNG	BSI- / ISO-STANDARD
1. Vertraulichkeit Art. 32 Abs. 1 lit. a & b	**Clientseitige Ende-zu-Ende-Verschlüsselung:** Alle Schülerdaten, Namen und Noten werden vor dem Verlassen des Endgeräts (im Web-Browser oder in der nativen App) mit `AES-256-GCM` verschlüsselt. Der Schlüssel verbleibt lokal. **Sandboxing & Isolierung:** Native Clients nutzen restriktives OS-Sandboxing ohne Zugriff auf Drittanwendungsdaten. **KDF-Härtung:** Argon2id-Passwortableitung (19 MiB RAM) gegen Brute-Force. **Zutritts- & Zugangskontrolle:** ISO 27001 zertifiziertes Datencenter mit 24/7-Sicherheitsdienst, biometrischer Schleuse und Videoüberwachung.	**ISO/IEC 27001** BSI TR-02102-1
2. Integrität Art. 32 Abs. 1 lit. b	**Authenticated Encryption (AEAD):** Jeder verschlüsselte Datensatz besitzt ein Authentifizierungs-Tag. Manipulationen auf dem Übertragungsweg werden sofort erkannt und verworfen. **Transportverschlüsselung:** Durchgängiges TLS 1.3 mit Perfect Forward Secrecy (PFS) und HSTS Preloading.	**TLS 1.3** AEAD-GCM
3. Verfügbarkeit & Belastbarkeit Art. 32 Abs. 1 lit. b & c	**Redundante Infrastruktur:** Diesel-Notstromaggregate, unterbrechungsfreie Stromversorgung (USV), N+1 Klimatisierung und Brandschutz mit Sauerstoffreduktion am Standort Leipzig. **Datensicherung:** Tägliche automatisierte Backups auf getrennten Speicher-Arrays mit konfigurierbarer Aufbewahrungsfrist.	**Tier III / ISO 27001** DE-CIX Anbindung
4. Trennungsgebot & Löschung Art. 32 Abs. 1 lit. b	**Mandantentrennung:** Strikte logische und kryptografische Trennung jedes Benutzerkontos. Daten verschiedener Schulen/Lehrkräfte können nicht vermischt werden. **Recht auf Löschung:** Sofortige und vollständige Zerstörung gespeicherter Chiffre-Datensätze per 1-Klick-Funktion in der Web- oder nativen App.	**DSGVO Art. 17** Kryptografische Isolation
5. Regelmäßige Überprüfung Art. 32 Abs. 1 lit. d	**Sicherheitsaudits & Monitoring:** Regelmäßige Überprüfung der Open-Source-Codebasis, automatisierte Schwachstellenscans von Abhängigkeiten und kontinuierliches Log-Monitoring (ohne Erfassung personenbezogener Inhalte).	**OWASP ASVS** DSB-Prüfbericht

Bestätigung: Die vorstehenden technischen und organisatorischen Maßnahmen werden vom Auftragnehmer dauerhaft aufrechterhalten und dem jeweiligen Stand der Technik entsprechend fortentwickelt.