

Auftragsverarbeitungsvertrag – Teacher's Desk

Muster für einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO zwischen einer Schule und der Mindoo GmbH für die Nutzung von Teacher's Desk über MindooDB Cloud. Felder in [eckigen Klammern] füllt die Schule aus. Stand: Oktober 2026.

Vertragsparteien

Verantwortlicher (Auftraggeber): [Name der Schule], [Anschrift], vertreten durch [Schulleitung]

Auftragsverarbeiter (Auftragnehmer): Mindoo GmbH, Karpfenweg 12, 76189 Karlsruhe, Deutschland, vertreten durch die Geschäftsführer Karsten Lehmann und Tammo Riedinger.
Ansprechpartner für Datenschutz: Karsten Lehmann, info@mindoo.de

Präambel

Lehrkräfte der Schule nutzen Teacher's Desk, um ihren Unterricht zu planen und Daten von Lernenden zu führen. Die Daten werden auf den Endgeräten Ende-zu-Ende-verschlüsselt und über MindooDB Cloud zwischen den Geräten synchronisiert. Der Auftragnehmer speichert dabei ausschließlich verschlüsselte Daten und besitzt keine Schlüssel, um sie zu entschlüsseln. Dieser Vertrag regelt die Pflichten beider Parteien nach Art. 28 DSGVO.

§ 1 Gegenstand, Dauer, Art und Zweck

- Gegenstand:** Bereitstellung der Synchronisation und Speicherung verschlüsselter Daten für Teacher's Desk über MindooDB Cloud sowie der zugehörigen Benutzerverwaltung.
- Dauer:** Der Vertrag gilt, solange Lehrkräfte der Schule MindooDB Cloud nutzen. Er endet mit dem letzten Nutzungsvertrag, ohne dass es einer Kündigung bedarf.
- Art der Verarbeitung:** Speichern, Übertragen und Löschen verschlüsselter Datensätze. Eine inhaltliche Auswertung findet nicht statt und ist technisch nicht möglich.
- Zweck:** Abgleich der Daten zwischen den Geräten einer Lehrkraft und, falls genutzt, mit berechtigten Kolleginnen und Kollegen.

Kategorie	Betroffene	Datenarten
Inhaltsdaten (verschlüsselt)	Lernende, Erziehungsberechtigte	Namen, Kontaktdaten, Noten, Beobachtungen, Anwesenheit, Sitzpläne, Gesprächsprotokolle, Anhänge
Inhaltsdaten (verschlüsselt)	Lehrkräfte, Kollegium	Namen, Fächer, Stundenplan, Termine, Notizen
Konto- und Verbindungsdaten	Lehrkräfte	Benutzername, öffentliche Schlüssel, IP-Adressen, Zeitpunkte der Synchronisation, Abrechnungsdaten

Die Inhaltsdaten können besondere Kategorien nach Art. 9 DSGVO enthalten, etwa Hinweise auf Förderbedarf oder Gesundheit. Sie liegen beim Auftragnehmer nur verschlüsselt vor.

§ 2 Weisungsgebundenheit

Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung der Schule. Die Weisungen ergeben sich aus diesem Vertrag und der Bedienung der App durch die Lehrkräfte. Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er die Schule unverzüglich.

§ 3 Vertraulichkeit

Alle Personen, die beim Auftragnehmer Zugang zu den Systemen haben, sind schriftlich auf Vertraulichkeit verpflichtet. Diese Pflicht besteht nach Ende ihrer Tätigkeit fort.

§ 4 Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt.

§ 5 Unterauftragsverarbeiter

Die Schule genehmigt die in Anlage 2 genannten Unterauftragsverarbeiter. Über neue oder ersetzte Unterauftragsverarbeiter informiert der Auftragnehmer mindestens 30 Tage vorher; die Schule kann aus wichtigem Grund widersprechen. Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dasselbe Schutzniveau. Inhalte werden ausschließlich in Deutschland gespeichert. Der vorgeschaltete Netzwerk-Proxy von Cloudflare kann Verbindungsdaten auch außerhalb der EU verarbeiten; dies ist durch das EU-US Data Privacy Framework und EU-Standardvertragsklauseln abgesichert.

§ 6 Unterstützung bei Betroffenenrechten

Die Lehrkräfte können Auskünfte, Berichtigungen, Löschungen und Exporte (Daten-Checkout) direkt in der App vornehmen. Wendet sich eine betroffene Person an den Auftragnehmer, leitet er die Anfrage unverzüglich an die Schule weiter. Da der Auftragnehmer die Inhalte nicht entschlüsseln kann, beschränkt sich seine Unterstützung auf Konto- und Verbindungsdaten.

§ 7 Meldung von Datenschutzverletzungen

Der Auftragnehmer meldet der Schule Verletzungen des Schutzes der Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis. Die Meldung enthält die Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie vorliegen. So kann die Schule ihre eigene Meldefrist von 72 Stunden einhalten.

§ 8 Löschung nach Vertragsende

Nach Vertragsende löscht der Auftragnehmer die gespeicherten Daten innerhalb von 30 Tagen, sofern keine gesetzliche Aufbewahrungspflicht besteht. Vorher können die Lehrkräfte alle Inhalte über den Daten-Checkout exportieren. Datensicherungen werden nach spätestens 30 Tagen überschrieben.

§ 9 Nachweise und Kontrollen

Der Auftragnehmer stellt der Schule auf Anfrage die Informationen zur Verfügung, die zum Nachweis dieser Pflichten nötig sind. Kontrollen vor Ort sind nach Absprache mit angemessener Vorlaufzeit möglich.

§ 10 Haftung und Schlussbestimmungen

Die Haftung richtet sich nach Art. 82 DSGVO. Änderungen bedürfen der Textform. Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam. Gerichtsstand ist Karlsruhe.

Für die Schule	Für die Mindoo GmbH
Ort, Datum:	Ort, Datum:
Unterschrift:	Unterschrift:

Anlage 1: Technische und organisatorische Maßnahmen

Die wichtigste Maßnahme ist die Ende-zu-Ende-Verschlüsselung: Inhalte verlassen das Gerät der Lehrkraft nur verschlüsselt, und der Auftragnehmer besitzt keine Schlüssel.

Schutzziel	Maßnahme
Vertraulichkeit der Inhalte	Verschlüsselung auf dem Endgerät mit AES-256-GCM; Schlüssel nur auf den berechtigten Geräten; Server speichern ausschließlich verschlüsselte Daten
Zugang zur App	Entsperren der Identität per Passkey (Face ID, Touch ID, Hardware-Key) oder Passwort, geprüft auf dem Gerät
Transport	Verschlüsselte Übertragung per TLS 1.2 oder höher über den Cloudflare-Proxy zusätzlich zur Inhaltsverschlüsselung; Cloudflare sieht dabei nur verschlüsselte Inhalte und Verbindungsdaten
Zutritt zu Rechenzentren	Rechenzentren der Hetzner Online GmbH in Falkenstein und Nürnberg mit Zutrittskontrolle, Videoüberwachung und Zertifizierung nach ISO/IEC 27001:2022
Zugriff auf Server	Administration der Server durch die Cygnus Networks GmbH im Auftrag des Auftragnehmers; Zugang nur für 2 benannte Personen, per SSH-Schlüssel, mit Protokollierung. Auch Administratoren sehen nur verschlüsselte Inhalte
Trennung	Getrennte Datenbanken je Tenant und Fachbereich; Rechte pro Datenbank in der App einsehbar
Integrität und Versionen	Fortschreibende Speicherung (append-only): frühere Versionen bleiben erhalten, Änderungen sind mit Ed25519 signiert
Verfügbarkeit	Lokale Kopie auf jedem Gerät, Offline-Betrieb; regelmäßige verschlüsselte Backups der Server in Deutschland, Aufbewahrung rollierend 30 Tage
Wiederherstellung	Backup und Restore in MindooDB Haven; Wiederherstellung früherer Versionen
Organisation	Verpflichtung auf Vertraulichkeit; Ansprechpartner für Datenschutz: Karsten Lehmann; Überprüfung der Maßnahmen jährlich

Anlage 2: Unterauftragsverarbeiter

Unternehmen	Anschrift	Leistung	Standort der Verarbeitung
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen	Server-Hosting für MindooDB Cloud in den Rechenzentren Falkenstein und Nürnberg	Deutschland
Cygnus Networks GmbH	Roonstraße 23a, 76137 Karlsruhe	Administration der Server	Deutschland
Cloudflare, Inc.	101 Townsend St, San Francisco, CA 94107, USA	DNS und Proxy vor den Servern (TLS- Terminierung, Schutz vor Angriffen)	Weltweites Netz, auch USA; Absicherung durch EU-US Data Privacy Framework und Standardvertragsklauseln

Cloudflare leitet den Datenverkehr zu den Servern weiter. Weil die Inhalte bereits auf dem Gerät verschlüsselt werden, sieht Cloudflare nur verschlüsselte Daten sowie Verbindungsdaten wie IP-Adressen.

Mit allen drei Unternehmen besteht ein Auftragsverarbeitungsvertrag; bei Cloudflare ist er Teil der Nutzungsbedingungen. Hetzner ist für seine Rechenzentren nach ISO/IEC 27001:2022 zertifiziert (<https://www.hetzner.com/unternehmen/zertifizierung/>).