

Vereinbarung zur Auftragsverarbeitung (AVV)

gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

■ Anleitung für Schulen

Um Kando rechtssicher an Ihrer Schule einzusetzen, drucken Sie bitte dieses Dokument aus, füllen Sie die Kontaktdaten der Schule aus, unterschreiben Sie den Vertrag und senden Sie eine Kopie per E-Mail an **info@kandoapp.de**. Wir senden Ihnen das gegengezeichnete Dokument umgehend zurück.

Vertragsparteien

1. Auftraggeber (Verantwortlicher im Sinne der DSGVO):

NAME DER SCHULE

SCHULLEITUNG / VERTRETEN DURCH

STRASSE, HAUSNUMMER, PLZ, ORT

2. Auftragnehmer (Auftragsverarbeiter):

David Herder (Kando App)

E-Mail: info@kandoapp.de

§ 1 Gegenstand, Dauer und Zweck des Auftrags

Der Auftragnehmer stellt dem Auftraggeber die Software-as-a-Service-Anwendung "Kando" zur Verfügung. Gegenstand und Zweck der Verarbeitung ist die verschlüsselte Bereitstellung und Synchronisation von Lernstandsdaten und Lerngruppen zur Vorbereitung und Auswertung von Tests im Unterricht. Die Laufzeit dieses Vertrags richtet sich nach der Dauer der Nutzung des Kando-Dienstes durch den Auftraggeber.

§ 2 Kategorien betroffener Personen und Datenarten

Im Rahmen der Durchführung des Auftrags werden folgende Daten verarbeitet:

Kategorien betroffener Personen:

- Schülerinnen und Schüler (Nutzer der Tests)
- Lehrkräfte (Nutzer des Erstellungssystems)

Datenkategorien:

- **Stammdaten:** Schülernummer (pseudonym), Name und Lerngruppenzugehörigkeit. Das Namensfeld ist ein freies Textfeld; die Schule legt fest, ob nur Vornamen eingetragen werden.
- **Leistungsdaten:** Antworten in Tests, Ergebnisse, erreichte Punkte/Prozente, Noten, fachliche Rückmeldungen.
- **Besondere Kategorien (Art. 9 DSGVO):** Gegebenenfalls technische Ausgleichs- oder Förderoptionen, soweit sie Rückschlüsse auf Gesundheit, Behinderung oder Förderbedarf erlauben.
- **Metadaten:** IP-Adressen, Verbindungszeitpunkte, Gerätekennungen, Prüfungsereignisse (Soft Exam Mode).
- **Live-Runde:** Spielnamen (vorgegeben oder frei gewählt), verschlüsselte Fragen und Antworten mit Eingangszeit. Nur im Arbeitsspeicher des Servers, Löschung beim Schließen, spätestens drei Stunden nach dem Start; keine Leistungsdaten.
- **Daten der Lehrkraft:** Konto-E-Mail, Anzeigenname, Anmelde- und Sitzungsdaten sowie Rückmeldungen aus dem Feedback-Formular.

§ 3 Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet die Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach den dokumentierten Weisungen des Auftraggebers. Der Auftragnehmer setzt die vereinbarten technischen und organisatorischen Maßnahmen (TOMs) um und stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben.

§ 4 Pflichten des Auftraggebers

Der Auftraggeber ist für die Einhaltung der gesetzlichen Vorschriften zum Datenschutz verantwortlich. Dazu gehört insbesondere die Prüfung, ob für Ausgleichs- oder Förderoptionen mit Rückschluss auf Gesundheit, Behinderung oder Förderbedarf eine Rechtsgrundlage nach Schulrecht, Landesdatenschutzrecht oder Art. 9 DSGVO erforderlich ist. Der Auftraggeber hat das Recht, die Einhaltung der technischen und organisatorischen Maßnahmen des Auftragnehmers vor Beginn der Verarbeitung und danach regelmäßig zu kontrollieren.

§ 5 Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber mit angemessenen Maßnahmen bei der Erfüllung der Rechte betroffener Personen nach Art. 12 bis 23 DSGVO sowie bei den Pflichten nach Art. 32 bis 36 DSGVO. Anfragen betroffener Personen, die den Auftragnehmer unmittelbar erreichen, leitet er unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst.

§ 6 Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer meldet dem Auftraggeber jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnisnahme, in Textform an die vom Auftraggeber benannte Kontaktstelle. Die Meldung beschreibt Art und Umfang des Vorfalls, die betroffenen Datenkategorien, die getroffenen Sofortmaßnahmen und die Ansprechstelle. Die Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO obliegt dem Auftraggeber.

§ 7 Löschung und Rückgabe nach Beendigung

Nach Beendigung des Auftrags löscht der Auftragnehmer die im Auftrag verarbeiteten Daten oder gibt sie nach Wahl des Auftraggebers zurück. Der Auftraggeber teilt seine Wahl in Textform mit; ohne Mitteilung wird nach 30 Tagen gelöscht. Verschlüsselte Sicherungskopien werden im Rahmen des regulären Backupzyklus

überschrieben, spätestens nach 90 Tagen. Gesetzliche Aufbewahrungspflichten bleiben unberührt; der Auftragnehmer benennt sie auf Anfrage.

§ 8 Unterauftragsverhältnisse

Der Auftragnehmer setzt als Unterauftragsverarbeiter für das Hosting und den E-Mail-Versand die **Strato AG** (Sitz in Deutschland, Rechenzentren in Deutschland) ein. Die Einbindung weiterer Unterauftragsverarbeiter bedarf der Zustimmung des Auftraggebers (Textform ausreichend).

§ 9 Technische und organisatorische Maßnahmen (TOM)

Der Auftragnehmer sichert die Integrität, Vertraulichkeit und Verfügbarkeit der Daten durch angemessene TOMs zu. Hierzu zählen insbesondere:

- **Vertraulichkeit (Ende-zu-Ende-Verschlüsselung):** Lokale Verschlüsselung aller Schüler- und Ergebnisdaten auf dem Endgerät mit AES-256-GCM vor Serverübertragung; auf dem Server liegen ausschließlich verschlüsselte Pakete.
- **Kontowiederherstellung:** Für den Fall einer vergessenen Anmeldung hinterlegt die Anwendung beim Auftragnehmer einen mit einem serverseitigen Hauptschlüssel gesicherten Umschlag des Kontoschlüssels. Der Auftragnehmer kann die Daten damit technisch entschlüsseln; er tut dies ausschließlich zur Wiederherstellung eines Kontos oder auf dokumentierte Weisung des Auftraggebers.
- **Integrität:** Authentifizierte Verschlüsselung, Datenbank-Zugriffsbeschränkungen auf Zeilenebene (Row Level Security).
- **Verfügbarkeit & Belastbarkeit:** Regelmäßige Überwachung der Systeme, AirDrop- und Offline-Fallbacks zur Vermeidung von Datenverlust.
- **Löschkonzept:** Automatische Löschung temporärer Testdaten nach maximal 24 Stunden, manuelle Löschfunktionen.

Unterschriften

Mit der Unterschrift wird dieser Vertrag und die Einhaltung der darin genannten technischen und organisatorischen Maßnahmen rechtsverbindlich vereinbart.

Für den Auftraggeber (Schule):

ORT, DATUM, UNTERSCHRIFT

Für den Auftragnehmer (Kando):

David Herder

ORT, DATUM, UNTERSCHRIFT