Auftragsverarbeitungsvertrag

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

AUFTRAGGEBER (VERANTWORTLICHER)

Name der Schule / des Schulträgers:

Straße, Hausnummer:

PLZ, Ort:

Vertreten durch (Name, Funktion):

E-Mail: _____

— im Folgenden „Auftraggeber" —

und

AUFTRAGNEHMER (AUFTRAGSVERARBEITER)

Felix Beck
Kraillinger Weg 9
82061 Neuried, Deutschland
E-Mail: info@korrigio.de
(Betreiber des Dienstes **Korrigio** unter korrigio.de)

— im Folgenden „Auftragnehmer" —

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers zum Zweck der Bereitstellung des KI-gestützten Korrekturunterstützungsdienstes **Korrigio** (erreichbar unter korrigio.de).

(2) Der Gegenstand der Auftragsverarbeitung umfasst insbesondere: OCR-Verarbeitung von Fotos handschriftlicher Schülerarbeiten, KI-gestützte Fehlerkorrektur und Kommentarerstellung, Speicherung von Korrektur- und Kalibrierungsdaten.

(3) Die Verarbeitung erfolgt ab Vertragsschluss und endet mit der Kündigung des Nutzungsvertrags oder auf schriftliche Weisung des Auftraggebers.

§ 2 Art und Zweck der Verarbeitung, Datenkategorien, betroffene Personen

(1) **Art der Verarbeitung:** Erhebung, Speicherung, Übermittlung an KI-Dienste, Auswertung, Anzeige, Löschung personenbezogener Daten.

(2) **Zweck der Verarbeitung:** Unterstützung von Lehrkräften bei der Korrektur handschriftlicher Schülerarbeiten (Aufsätze, Klausuren) durch KI-gestützte Texterkennung, Fehlermarkierung und Kommentarerstellung.

(3) **Kategorien personenbezogener Daten:**

- Accountdaten der Lehrkräfte (E-Mail-Adresse, verschlüsseltes Passwort)
- Fotos/Scans handschriftlicher Schülerarbeiten (temporär, bis zur Löschung nach OCR)
- Digitalisierter Text der Schülerarbeiten (nach OCR, anonymisiert vor KI-Verarbeitung)
- KI-Korrekturdaten (Fehlermarkierungen, Kommentartexte, Notenorientierung)
- Kalibrierungsdaten der Lehrkraft (gespeicherte Korrekturentscheidungen)

(4) **Kategorien betroffener Personen:** Lehrkräfte (Accountdaten); Schülerinnen und Schüler (handschriftliche Arbeiten, ausschließlich anonymisiert vor KI-Verarbeitung).

§ 3 Pflichten des Auftragnehmers

3.1 Weisungsgebundenheit

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet ist (Art. 28 Abs. 3 lit. a DSGVO).

3.2 Vertraulichkeit

Der Auftragnehmer stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben (Art. 28 Abs. 3 lit. b DSGVO).

3.3 Technische und organisatorische Maßnahmen (TOM)

Der Auftragnehmer ergreift geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die konkreten Maßnahmen sind in **Anlage 2** beschrieben.

3.4 Unterauftragnehmer

Der Auftragnehmer setzt Unterauftragnehmer gemäß **Anlage 1** ein. Er ist berechtigt, weitere Unterauftragnehmer einzusetzen, wenn er den Auftraggeber mindestens 30 Tage vor dem beabsichtigten Einsatz informiert. Der Auftraggeber kann innerhalb dieser Frist Widerspruch einlegen. Wechselt der Auftragnehmer einen Unterauftragnehmer, informiert er den Auftraggeber unverzüglich.

3.5 Unterstützungspflichten

Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung von Betroffenenrechten (Art. 15–22 DSGVO), bei der Meldung von Datenschutzverletzungen (Art. 33–34 DSGVO) sowie bei der Durchführung von Datenschutz-Folgenabschätzungen (Art. 35 DSGVO).

3.6 Löschung und Rückgabe nach Auftragsende

Nach Beendigung des Auftrags löscht der Auftragnehmer alle verarbeiteten personenbezogenen Daten oder gibt sie an den Auftraggeber zurück, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.

3.7 Nachweis und Kontrolle

Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zur Verfügung, um die Einhaltung seiner Pflichten gemäß Art. 28 DSGVO nachzuweisen. Der Auftraggeber ist berechtigt, Überprüfungen durchzuführen oder durch Dritte durchführen zu lassen.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber ist alleiniger Verantwortlicher für die Rechtmäßigkeit der Datenverarbeitung im Rahmen des Nutzungsvertrags.

(2) Der Auftraggeber stellt sicher, dass Schülerinnen und Schüler sowie deren Erziehungsberechtigte in geeigneter Weise über die Nutzung von Korrigio informiert werden.

(3) Der Auftraggeber erteilt Weisungen zur Datenverarbeitung ausschließlich schriftlich oder in dokumentierter elektronischer Form.

§ 5 Haftung

Die Haftungsregelungen richten sich nach Art. 82 DSGVO sowie den Bestimmungen des zwischen den Parteien geschlossenen Nutzungsvertrags. Jede Partei haftet für die Verstöße, die in ihrem eigenen Verantwortungsbereich liegen.

§ 6 Schlussbestimmungen

(1) Dieser Vertrag unterliegt dem deutschen Recht.

(2) Änderungen dieses Vertrags bedürfen der Schriftform.

(3) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

Unterschriften

Ort, Datum — Auftraggeber (Schule / Schulträger)	Ort, Datum — Auftragnehmer (Felix Beck / Korrigio)
Unterschrift, Name in Druckbuchstaben, Funktion	Unterschrift, Name in Druckbuchstaben

Anlage 1: Unterauftragnehmer (Sub-Processors)

Der Auftragnehmer setzt folgende Unterauftragnehmer ein. Mit allen Unterauftragnehmern bestehen Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO.

Unternehmen	Serverstandort	Zweck	Verarbeitete Datenkategorien
Supabase Inc. / Supabase GmbH supabase.com	Frankfurt am Main, Deutschland (AWS eu-central-1)	Datenbank, Nutzerauthentifizierung, Dateispeicherung	Accountdaten (Lehrkraft), Korrektur- und Kalibrierungsdaten, temporäre Datei-Uploads
Amazon Web Services EMEA SARL aws.amazon.com/bedrock (Amazon Bedrock)	Frankfurt am Main, Deutschland (eu-central-1)	KI-gestützte Texterkennung (OCR), Fehlerkorrektur und Kommentarerstellung (Claude via Bedrock)	Fotos handschriftlicher Arbeiten (Stufe 1, OCR, temporär), anonymisierter Fließtext der Schülerarbeiten (Stufe 2), anonymisierte Kalibrierungsbeispiele. Keine Speicherung durch AWS gemäß DPA.
Netcup GmbH netcup.de	Nürnberg, Deutschland	Serverhosting (VPS), Reverse-Proxy (nginx), SSL/TLS	Server-Protokolldaten, HTTP-Anfragen (Transit-Daten)
Hetzner Online GmbH hetzner.com Industriestraße 25, 91710 Gunzenhausen	Falkenstein, Deutschland (EU)	Verschlüsselter Backup-Speicher (Storage Box) — Disaster-Recovery	Client-seitig AES-256-verschlüsseltes borgmatic-Backup der gesamten Produktionsdatenbank. Kein Klartextzugriff durch Hetzner; Ver- und Entschlüsselung

Unternehmen	Serverstandort	Zweck	Verarbeitete Datenkategorien
			ausschließlich auftraggeberseitig. AVV abgeschlossen 19.06.2026.
Stripe Payments Europe, Ltd. stripe.com	Irland (EU); ggf. USA via EU-Standardvertragsklauseln (SCCs) gem. Art. 46 Abs. 2 lit. c DSGVO	Zahlungsabwicklung für Premium-Abonnements und Schullizenzen	E-Mail-Adresse der zahlenden Stelle, Zahlungsdaten (Kreditkarte etc., ausschließlich bei Stripe gespeichert), Transaktionsdaten. Keine Schülerdaten.
Mistral AI SAS mistral.ai	Paris, Frankreich	Backup-LLM (Inferenz) — nur bei Ausfall der AWS-Region Frankfurt	Anonymisierter Fließtext der Schülerarbeiten (Stufe 2), nur im Ausfallfall. Keine Bilder, keine Schülernamen.
Sentry (Functional Software, Inc.) sentry.io	EU-Region (konfiguriert)	Fehler-Tracking (Stack Traces, Error-Kontexte)	Stack Traces und Error-Kontexte. Keine Nutzerinhalte, keine Schülerdaten.
Resend, Inc. resend.com 2261 Market Street #5039, San Francisco, CA 94114, USA (Rechtsträger: Plus Five Five, Inc.)	USA; Drittland-Übermittlung auf Grundlage von EU-Standardvertragsklauseln (SCCs) gem. Art. 46 Abs. 2 lit. c DSGVO	Transaktionaler E-Mail-Versand (Konto- und System-Mails)	E-Mail-Adresse der Lehrkraft und Inhalte transaktionaler System-E-Mails. Keine Schülerdaten.
Intuition Machines, Inc. (hCaptcha) hcaptcha.com 350 Alabama St, San Francisco, CA 94110, USA	USA; Drittland-Übermittlung auf Grundlage von EU-Standardvertragsklauseln (SCCs) gem. Art. 46 Abs. 2 lit. c DSGVO	Bot- und Missbrauchsabwehr auf den Authentifizierungsformularen	IP-Adresse und Interaktionsdaten der Lehrkraft (nur Auth-Seiten). Keine Schülerdaten.

Hinweis: Supabase, AWS, Netcup und Hetzner verarbeiten Daten ausschließlich auf Servern in Deutschland, Sentry in der EU-Region. Stripe (Irland), Resend (USA) und hCaptcha (USA) können Lehrkraft-Account- bzw. Sicherheitsdaten auf Grundlage von EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) in die USA übermitteln. Schülerdaten werden nicht in Drittstaaten übermittelt.

Anlage 2: Technische und Organisatorische Maßnahmen (TOM)

gemäß Art. 32 DSGVO

1. Verschlüsselung der Übertragung

Alle Datenübertragungen zwischen Nutzer und Server sowie zwischen Server und Unterauftragnehmern erfolgen ausschließlich über verschlüsselte Verbindungen (HTTPS/TLS 1.2 oder höher). Zertifikate werden über Let's Encrypt verwaltet.

2. Verschlüsselung gespeicherter Daten (At Rest)

Datenbankdaten werden von Supabase und AWS at rest verschlüsselt (AES-256). Passwörter werden ausschließlich als Bcrypt-Hash gespeichert; Klartext-Passwörter werden zu keinem Zeitpunkt gespeichert.

3. Pseudonymisierung und Anonymisierung

Die Anonymisierung erfolgt organisatorisch durch die Lehrkraft: Schülernamen und direkte Identifikatoren werden vor dem Upload entfernt oder abgedeckt (Acknowledgment-Modell, bestätigt pro Einreichung). Eine automatische algorithmische Erkennung und Ersetzung personenbezogener Daten findet nicht statt. Die KI-Modelle erhalten ausschließlich den von der Lehrkraft anonymisierten Text. Die Unterauftragnehmer erhalten keine Information über Lehrkraft, Schüler oder Schule.

4. Zugriffskontrolle

Der Zugriff auf Daten ist durch Supabase Auth abgesichert. Jede Lehrkraft kann nur auf ihre eigenen Daten zugreifen (API-Layer-Isolierung). Administrativer Zugriff auf die Produktionsumgebung ist auf den Auftragnehmer beschränkt und erfordert SSH- Schlüsselauthentifizierung.

5. Löschkonzept

- **Fotos/Scans handschriftlicher Arbeiten:** Seitenbilder werden 30 Tage nach Abschluss der Korrektur (Status „Korrigiert") automatisch gelöscht (scan_retention_sweep). Während der Korrektur werden sie für die Anzeige und die Mathematik-Bewertung benötigt; eine darüber hinausgehende dauerhafte Speicherung von Originalbildern findet nicht statt.
- **Server-Log-Dateien:** Automatische Löschung nach spätestens 30 Tagen.
- **Nutzerdaten bei Kontolöschung:** Vollständige Löschung aller verknüpften Daten auf Anfrage oder bei Kontolöschung.

6. Keine Speicherung beim KI-Anbieter

Die Nutzung von Amazon Bedrock erfolgt über eine API, die gemäß den AWS-Datenschutzbestimmungen und dem bestehenden Data Processing Agreement keine Speicherung der Eingabedaten bei AWS oder Anthropic vorsieht. Anfragen werden nicht für das Training von KI-Modellen verwendet.

7. EU-Serverstandorte

Die Verarbeitung von Schülerdaten (Handschriftbilder, Schülertexte) findet ausschließlich auf Servern innerhalb der Europäischen Union statt (Deutschland: Supabase Frankfurt, AWS Bedrock Frankfurt, Netcup Nürnberg, Hetzner Falkenstein; Frankreich: Mistral Paris als Backup-LLM). Lehrkraft-Account- bzw. Sicherheitsdaten können bei Stripe (Irland), Resend (USA) und hCaptcha (USA) auf Grundlage von EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) in die USA übermittelt werden. Schülerdaten werden nicht in Drittstaaten übermittelt.

8. Incident Response

Im Falle einer Datenschutzverletzung informiert der Auftragnehmer den Auftraggeber unverzüglich, spätestens innerhalb von 72 Stunden, um die Meldepflicht nach Art. 33 DSGVO zu ermöglichen.