Korrigio — Sub-Processor Register

Zuletzt aktualisiert: 2026-06-19 (Hetzner Online GmbH als verschlüsselter Backup-Sub-Auftragsverarbeiter ergänzt — L2-dsfa-01; AVV abgeschlossen 19.06.2026. Frühere Aktualisierung 2026-06-13: Resend + hCaptcha als US-Sub-Auftragsverarbeiter ergänzt — SEC-F-01/F-02; sie verarbeiten ausschließlich Lehrkraft-Account-/Sicherheitsdaten, keine Schülerdaten. Frühere Aktualisierung 2026-05-12: LLM-Architektur präzisiert — Opus primary, Sonnet intra-Bedrock-Fallback, Mistral second-tier fallback, siehe `backend/app/services/llm/client.py:_build_fallback_chain`.) **Verantwortlicher:** Felix Beck (siehe Impressum auf korrigio.de)

> Dieses Verzeichnis listet alle Sub-Auftragsverarbeiter im Sinne des Art. 28 Abs. 4 DSGVO. Lehrkräfte und Schulen werden über Änderungen informiert.

Sub-Auftragsverarbeiter	Zweck	Region	AVV-Status	Übermittelte Daten
AWS Bedrock	LLM-Inferenz (Anthropic Claude Opus primary für Korrektur + Sonnet als intra-Bedrock-Fallback / OCR multimodal)	Frankfurt (eu-central-1)	Signed (AWS GDPR DPA, auto-applied per AWS-Customer-Agreement, verifiziert 2026-05-08)	Anonymisierte Prompts, Bilddaten für OCR (anschließend gelöscht), Modell-Outputs
Mistral AI	LLM-Inferenz — zweite Fallback-Stufe für Bedrock-Regional-Ausfälle (true provider diversity; keine OCR weil kein Vision-Input)	Paris (Frankreich)	Signed (DPA via Terms-of-Service-Incorporation §11.2, verifiziert 2026-05-08)	Anonymisierte Prompts (nur im Ausfallfall)
Stripe	Zahlungsabwicklung	Irland (EU)	Signed (DPA via Stripe-Konsole)	E-Mail, Zahlungs-Metadaten
Sentry	Fehler-Tracking	EU (EU-Region konfiguriert)	Signed	Stack Traces, Error-Kontexte (KEINE Nutzerinhalte)
Netcup	VPS-Hosting + Mail	Nürnberg, Deutschland	Signed (Hosting-AGB + AVV)	Sämtliche App-Daten at rest
Supabase	Auth + Postgres			Sämtliche App-Daten

Sub-Auftragsverarbeiter	Zweck	Region	AVV-Status	Übermittelte Daten
		Frankfurt (eu-central-1)	Signed (DPA via Supabase-Dashboard)	
Hetzner Online GmbH	Verschlüsselter Backup-Speicher (Storage Box) — Disaster-Recovery	Falkenstein, Deutschland (EU)	Signed (AVV abgeschlossen 19.06.2026)	Client-seitig AES-256-verschlüsseltes borgmatic-Backup der gesamten Produktionsdatenbank — kein Klartextzugriff durch Hetzner
Resend	Transaktionaler E-Mail-Versand (Konto-/System-Mails)	USA (Drittland, SCCs)	Gilt automatisch via Resend-Terms (§12); EU-SCCs ausdrücklich inkorporiert (§6.2) — nur PDF archivieren	E-Mail-Adresse der Lehrkraft + E-Mail-Inhalte; KEINE Schülerdaten
hCaptcha (Intuition Machines, Inc.)	Bot-/ Missbrauchsabwehr auf den Auth-Formularen	USA (Drittland, SCCs)	Gilt automatisch via hCaptcha-Terms („incorporated by reference") — nur PDF archivieren	IP-Adresse + Interaktionsdaten der Lehrkraft (nur Auth-Seiten); KEINE Schülerdaten

Drittland-Übermittlung

Die KI-/Inhaltsverarbeitung (AWS Bedrock, Mistral) sowie Hosting und Datenbank (Netcup, Supabase) operieren ausschließlich auf EU-Servern. Eine Übermittlung in die USA findet bei **drei** Diensten statt — Stripe (Zahlung), Resend (E-Mail) und hCaptcha (Missbrauchsabwehr) — jeweils ausschließlich auf Grundlage von EU-Standardvertragsklauseln (SCCs, Art. 46 Abs. 2 lit. c DSGVO) und beschränkt auf **Account-, Kontakt- und Sicherheitsdaten der Lehrkraft**. **Schülerdaten (Handschriftbilder, Schülertexte) werden an keinen dieser drei Dienste und in kein Drittland übermittelt.**

Hinweis zu Stripe: Stripe Payments Europe, Ltd. hat seinen Sitz in Irland (EU). Im Rahmen konzerninterner Datenflüsse können Zahlungsmetadaten in die USA weitergeleitet werden; dies erfolgt ausschließlich auf Grundlage von EU-Standardvertragsklauseln (SCCs). Schülerdaten werden an Stripe nicht übermittelt.

Hinweis zu Resend: Resend, Inc. (USA) versendet ausschließlich transaktionale System-E-Mails (Registrierungs-/Passwort-Bestätigung, E-Mail-Änderung, Widerrufsbestätigung, Feedback-/Missbrauchsmeldungen, Betriebs-Alerts). Verarbeitet werden die E-Mail-Adresse der Lehrkraft und der Mail-Inhalt — keine Schülerdaten. Drittland-Übermittlung in die USA auf SCC-Grundlage.

Hinweis zu hCaptcha: Intuition Machines, Inc. (USA) schützt die Anmelde-/Registrierungsformulare vor automatisiertem Missbrauch (Art. 6 Abs. 1 lit. f DSGVO). Verarbeitet werden IP-Adresse und Interaktionsdaten der Lehrkraft, ausschließlich auf den Authentifizierungsseiten — keine Schülerdaten. Drittland-Übermittlung in die USA auf SCC-Grundlage. *Optionaler Privacy-Hardening-Pfad (v24): Wechsel auf einen EU-gehosteten Captcha-Dienst; setzt voraus, dass die Supabase-Auth-Captcha-Integration (unterstützt nur hCaptcha/Turnstile) durch serverseitige Verifikation ersetzt wird.*

Hinweis zu Sentry: Sentry (Functional Software, Inc.) verarbeitet Fehler-Tracking-Daten ausschließlich in der EU-Region. Stack Traces und Error-Kontexte enthalten keine personenbezogenen Nutzerinhalte (Schülertexte, Korrekturdaten). Konfiguriert per `SENTRY_DSN` mit EU-Endpoint.

Hinweis zu Hetzner: Hetzner Online GmbH (Industriestr. 25, 91710 Gunzenhausen) stellt eine Storage Box in Falkenstein (Deutschland) als Backup-Ziel bereit. Dort liegt ein **client-seitig AES-256-verschlüsseltes** borgmatic-Backup der gesamten Produktionsdatenbank. Der Backup-Inhalt umfasst zwar alle Datenarten (auch Schüler-Inhaltsdaten), ist für Hetzner jedoch zu keinem Zeitpunkt im Klartext zugänglich — die Ver- und Entschlüsselung erfolgt ausschließlich auftraggeberseitig (borgmatic). EU-Standort, **keine Drittland-Übermittlung.** AVV mit Hetzner abgeschlossen 19.06.2026.

Änderungshinweis

Neuaufnahmen oder Wechsel von Sub-Auftragsverarbeitern werden vor Inkrafttreten in der Korrigio-App (Anmeldung) und per E-Mail an alle Bestandskunden bekanntgegeben. Lehrkräfte / Schulen können im Einzelfall der Änderung widersprechen.

Prüfpfad

Änderungen an dieser Datei sind via Git-History nachvollziehbar. Bei Anfragen zur AVV-Dokumentation: info@korrigio.de.

DPA-Belege (lokale Beweissicherung)

Wortlaute der DPAs zum Zeitpunkt der Geltung sind als PDF beim Verantwortlichen archiviert (BayLDA-Beweisanforderung):

- AWS GDPR DPA — Quelle: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf (Stand: 2026-05-08)
- Mistral DPA — Quelle: https://legal.mistral.ai/terms/data-processing-addendum (Stand: 2026-05-08)

- Resend DPA — Quelle: https://resend.com/legal/dpa (gilt automatisch via Terms-Acceptance §12; EU-SCCs ausdrücklich inkorporiert §6.2 — geprüft 2026-06-13). PDF archiviert 2026-06-13 (`Data Processing Addendum · Resend.pdf`).
- hCaptcha DPA — Quelle: https://newassets.hcaptcha.com/dpa/IMI_Data_Processing_Addendum_4.20.2023.pdf (von den hCaptcha-Terms „incorporated by reference" — geprüft 2026-06-13). PDF archiviert 2026-06-13 (`IMI_Data_Processing_Addendum_4.20.2023.pdf`).

Alle vier DPAs (AWS, Mistral, Resend, hCaptcha) werden automatisch durch das jeweilige Customer-Agreement bzw. die Terms-of-Service-Incorporation bindend; eine separate Counter-Signature ist nicht erforderlich. Alle vier PDF-Belege liegen gemeinsam im AVV-Archiv des Verantwortlichen (Ordner „AVV der eingebundenen Services"). Die SEC-F-01/F-02-Dokumentationslücke ist damit geschlossen.

Der Hetzner-Storage-Box-AVV (ChessRiddle ↔ Hetzner Online GmbH) wurde am 19.06.2026 elektronisch via Checkbox abgeschlossen (die Auftraggeber-Signaturzeile bleibt vereinbarungsgemäß leer). Anlage 1 dieses AVV erfasst Schüler-Inhaltsdaten sowie „Schülerinnen und Schüler" als betroffene Personengruppe. Das AVV-PDF liegt beim Verantwortlichen im AVV-Archiv (nicht im Repository). Die L2-dsfa-01-Register-Lücke ist damit geschlossen.

Stand: 2026-06-19 — siehe `docs/datenschutz/korrigio-dsfa-vorlage.md` §6 für die technische Implementierung der Datenflüsse.