Muster-Datenschutz-Folgenabschätzung (DSFA) für den Einsatz von Korrigio

Gemäß Art. 35 DSGVO i. V. m. der Liste der Verarbeitungstätigkeiten, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (Bayerische Blacklist)

Version: 2.5 — 2026-06-19

> **Hinweis:** Diese Vorlage wurde von Korrigio (Felix Beck) erstellt, um Schulen bei der Durchführung ihrer DSFA gemäß Art. 35 DSGVO zu unterstützen. Die datenschutzrechtliche Verantwortung verbleibt bei der Schule als Verantwortlicher. Die Vorlage stellt keine Rechtsberatung dar. Abschnitte mit *[Schule]* sind von der Schule auszufüllen.

---

1. Administrative Angaben

Feld	Angabe
Bezeichnung der Verarbeitung	Einsatz des KI-gestützten Korrektur-Assistenzsystems „Korrigio”
Verantwortlicher (Art. 4 Nr. 7 DSGVO)	*[Schule: Name und Anschrift der Schule]*
Schulleitung	*[Schule: Name der Schulleiterin / des Schulleiters]*
Behördlicher Datenschutzbeauftragter	*[Schule: Name, Kontaktdaten des/der DSB]*
Auftragsverarbeiter (Art. 28 DSGVO)	Felix Beck, Kraillinger Weg 9, 82061 Neuried, info@korrigio.de
Datum der Erstellung	*[Schule: Datum]*
Datum der letzten Überprüfung	*[Schule: Datum — DSFA ist regelmäßig zu überprüfen, Art. 35 Abs. 11 DSGVO]*
Beteiligte Fachbereiche	*[Schule: z. B. Fachschaft Deutsch, Fachschaft Mathematik, Fachschaft Physik]*
AVV abgeschlossen am	*[Schule: Datum des unterschriebenen AVV mit Korrigio]*

---

2. Schwellwertanalyse — Warum ist eine DSFA erforderlich?

Unverändert gegenüber v1.0: Die Verarbeitung löst zwei Tatbestände der Bayerischen Blacklist aus (Nr. 9 KI, Nr. 16 schutzbedürftige Personen) und erfüllt mindestens vier der neun WP248-Kriterien der Art.-29-Datenschutzgruppe. Die DSFA ist zwingend erforderlich.

2.1 Hinweis zu EDPB Opinion 28/2024

Die Europäische Datenschutzbehörde hat am 17.12.2024 in Opinion 28/2024 klargestellt, dass die Schwelle für die Einstufung eines KI-Modells bzw. einer KI-Verarbeitung als „anonym" **hoch** ist: Sowohl die Wahrscheinlichkeit einer direkten Extraktion personenbezogener Daten aus dem Modell als auch die Wahrscheinlichkeit, solche Daten aus Modellabfragen zu gewinnen, muss „insignifikant" sein.

Folgerung für Korrigio: Auch der nach OCR digitalisierte Leistungsnachweis-Text bleibt personenbezogen, selbst wenn der Schülername abgedeckt war. Handschrift ist ein indirektes Identifizierungsmerkmal, der Textinhalt kann Rückschlüsse auf die schreibende Person erlauben (Stil, erwähnte Personen, Lebensumstände im Aufsatz). Die Verarbeitung stützt sich nicht auf eine Anonymisierungs-Fiktion, sondern auf die **Rechtsgrundlage** (Abschnitt 3.7) und die **technisch-organisatorischen Maßnahmen** (§6).

2.2 KM-Handlungsleitfaden „KI in der pädagogischen Praxis" (Stand 28.11.2025)

Das Bayerische Staatsministerium für Unterricht und Kultus hat am 28.11.2025 den Handlungsleitfaden „Künstliche Intelligenz in der pädagogischen Praxis" für Schulen veröffentlicht. Er adressiert sich ausdrücklich an „Schulleitungen, Datenschutzbeauftragte und weitere Personen, die in der Schule für die Einführung von Software zuständig sind" (S. 2) und ist die maßgebliche bayerische Auslegungsquelle für den Einsatz externer KI-Tools wie Korrigio.

Für Korrigio sind folgende Festlegungen des Handlungsleitfadens unmittelbar einschlägig:

- **Verfahren für kommerzielle KI-Anbieter (S. 4):** „Schulleitungen sind dafür verantwortlich zu prüfen, ob die rechtlichen Anforderungen erfüllt sind (siehe dazu 3.2) und nach erfolgreicher Prüfung einen AVV (Auftragsverarbeitungsvertrag) zu zeichnen." → Stützt die Verfahrensarchitektur Schulleitung-prüft-zeichnet-AVV.
- **Schulleitung als Freigeber (S. 5):** „Vor der Nutzung von KI-Systemen sind diese von der Schulleitung im Sinne eines Betriebsmittels freizugeben." → Stützt M15.
- **Informationspflicht, nicht Einwilligungspflicht (S. 5):** „Vor Nutzung der KI-Funktionalitäten sind die Lehrkräfte, Schülerinnen und Schüler sowie die Erziehungsberechtigten über den Einsatz der KI-Systeme […] zu informieren." → Stützt M18 und Abschnitt 3.7.
- **Erforderlichkeits-Ausnahme (S. 6):** „Sollen in einer KI-Anwendung personenbezogene Daten verarbeitet werden, weil es im konkreten

Einsatzszenario sinnvoll und notwendig ist, […] ist zu klären, ob die in Frage stehende Verarbeitung […] zur Erfüllung einer schulischen Aufgabe erforderlich ist. Ist das der Fall, dürfen die entsprechenden personenbezogenen Daten auch ohne Zustimmung der Betroffenen verarbeitet werden, sofern die Verarbeitung datenschutzkonform erfolgt." → Stützt die Rechtsgrundlage Art. 6 Abs. 1 lit. e DSGVO ohne zusätzliche Einwilligung (Abschnitt 3.7).

- **Handschrift als personenbezogenes Datum (S. 5):** „Zu personenbezogenen Daten zählen […] auch […] die Handschrift oder andere personenbeziehbare Inhalte." → Bestätigt die Risiken-Klassifizierung in §5 (R1, R2, R7).
- **AVV-Mindeststandards Schrems-II (S. 7):** „Es darf keine Datenübermittlung an Staaten erfolgen, in denen die DSGVO nicht gilt (Stichwort: Abuse Monitoring)." → Begründet das neue Risiko R10 und die TOM M26 (siehe §5 und §6).
- **Hochrisiko-KI-Abgrenzung (S. 8):** „Nicht als Hochrisiko-KI gelten dagegen nach aktuellem Stand KI-gestützte Rückmeldungen oder Feedbackvorschläge, die nur zur unterstützenden Lernbegleitung genutzt werden und nicht in Abschlussnoten oder andere formale Bewertungen einfließen." → Stützt die in `docs/datenschutz/eu-ki-verordnung-einstufung.md` dokumentierte Nicht-Hochrisiko-Einordnung.

---

3. Systematische Beschreibung der Verarbeitung (Art. 35 Abs. 7 lit. a DSGVO)

3.1 Zweck der Verarbeitung

Korrigio unterstützt Lehrkräfte bei der Korrektur schriftlicher Schülerarbeiten (Aufsätze, Mathematik- und Physik-Leistungsnachweise) als **Assistenzsystem**. Das System erzeugt Fehlermarkierungen, Kommentarvorschläge und bei Mathematik Punktzuweisungen, die die Lehrkraft prüft, anpasst oder verwirft. Die endgültige Bewertung und Benotung obliegt ausschließlich der Lehrkraft. Korrigio trifft keine automatisierten Einzelentscheidungen im Sinne von Art. 22 DSGVO — jede KI-Ausgabe durchläuft eine dokumentierte menschliche Prüfung (siehe §6 M7 und §6 M20).

3.2 Kategorien betroffener Personen

Kategorie	Beschreibung
Schülerinnen und Schüler	Deren handschriftliche Arbeiten fotografiert, per OCR digitalisiert und durch KI analysiert werden
Lehrkräfte	Die ein Nutzerkonto bei Korrigio anlegen und den Dienst zur Korrekturunterstützung verwenden

3.3 Kategorien personenbezogener Daten

Datenkategorie	Personenbezug	Verarbeitung
Fotos/Scans handschriftlicher Arbeiten	Handschrift als indirektes Identifizierungsmerkmal; kein biometrisches Datum i. S. v. Art. 9 Abs. 1 DSGVO, da keine eindeutige Identifizierung bezweckt ist	OCR-Dienst wandelt Bild in Text um; Automatische Löschung 30 Tage nach Abschluss der Korrektur (Status Korrigiert), spätestens bei Löschung durch die Lehrkraft; während der Korrekturphase werden die Seitenbilder für die multimodale Mathematik-Bewertung und die Anzeige neben den KI-Markierungen benötigt.
Digitalisierter Fließtext (OCR-Ergebnis)	Inhalt der Schülerarbeit; ggf. im Text genannte Personen	Speicherung in Datenbank (Supabase, Frankfurt); Übermittlung an KI-Sprachmodell
KI-Korrekturvorschläge	Bezug zur Schülerarbeit, nicht unmittelbar zur Person	Speicherung in Datenbank bis Löschung durch Lehrkraft
Lehrkraft-Accountdaten	E-Mail-Adresse, Passwort-Hash (via Supabase Auth), Profilbild	Authentifizierung und Kontoverwaltung
Kalibrierungsdaten	Validierte Korrekturentscheidungen der Lehrkraft	Wenige-Beispiel-Lernen („Few-Shot Learning"); verbessert künftige Vorschläge für **diese Lehrkraft**; keine modellübergreifende Auswertung
Ereignisprotokolle (ab v11.0)	Pseudonymisierte Identifikatoren, Zeitstempel, Modell-Metadaten — kein Prompt-Klartext	Revisionsfeste Speicherung gemäß EU AI Act Art. 12 (siehe §6 M21)

3.4 Zwei-Stufen-Verarbeitungspipeline (Privacy by Design)

Vorbereitung (durch die Lehrkraft, vor dem Upload): Dienstliche Weisung — Namen auf der Arbeit abdecken (z. B. Aufkleber, Schwärzung) oder digital schwärzen (In-App-Schwärzung vor dem Upload). Alternativ können verbliebene Namen beim Korrekturschritt im Textvalidierungsdialog gelöscht werden. Die Lehrkraft bestätigt pro Upload via Pflicht-Checkbox, dass der Schülername entfernt oder abgedeckt wurde (siehe M19).

Stage 1 — Digitalisierung mit zwei Modus-Varianten

Modus A — OCR (Foto/Scan-Upload): Die Lehrkraft lädt fotografierte oder gescannte handschriftliche Schülerarbeiten hoch. Diese werden via AWS Bedrock (Claude Sonnet 4.6, EU-Region Frankfurt) per OCR in Plaintext umgewandelt. Der OCR-Output ist die Eingabe für Stage 2. Automatische Löschung 30 Tage nach Abschluss der Korrektur (Status Korrigiert), spätestens bei Löschung durch die Lehrkraft; während der Korrekturphase werden die Seitenbilder für die multimodale Mathematik-Bewertung und die Anzeige neben den KI-Markierungen benötigt. AWS Bedrock speichert weder das Bild noch den Text dauerhaft (gemäß AWS-DPA für Bedrock Services).

Modus B — Direct-Plaintext-Ingest (Lehrer-Upload): Die Lehrkraft fügt einen bereits digitalisierten Schüleraufsatz direkt als Plaintext ein — entweder per Copy-Paste in das Web-Formular oder durch Upload einer Datei (`.docx`, `.txt`, `.md`). Anwendungs-Szenario: Schülerinnen und Schüler haben ihre Arbeit selbst digitalisiert (z. B. über das mebis-Plugin „KI-gestütztes Feedback" oder per Apple-Notes-Live-Text auf dem iPad) und der Lehrkraft den Text übermittelt. Die OCR-Stage entfällt; der eingegebene Plaintext wird serverseitig (bei DOCX-Upload via `python-docx`, einer Pure-Python-Bibliothek, ohne externe Schnittstelle) zu Plaintext extrahiert und ist die Eingabe für Stage 2.

Beide Modus-Varianten produzieren denselben strukturierten Plaintext-Output. Stage 2 (Korrektur und Kommentartext via AWS Bedrock Claude Opus 4.6, EU-Region Frankfurt) ist von der gewählten Stage-1-Variante vollständig unabhängig.

Textvalidierung (Mensch-in-der-Schleife) — Pflicht für beide Modus-Varianten

Die Lehrkraft prüft den digitalisierten Text, korrigiert Erkennungsfehler und entfernt verbliebene Namen oder Identifikatoren, bevor Stage 2 startet. Die Validierungsansicht ist für beide Modi verpflichtend: Auch ein bereits digitalisierter Plaintext (Modus B) kann Tippfehler des Schülers oder OCR-Fehler des digitalisierenden Drittsystems (z. B. mebis-Plugin) enthalten — die Validierung verhindert, dass die KI-Korrektur Schülereingabefehler als „Rechtschreibfehler des Schülers" markiert.

Stage 2 — KI-Korrektur und Kommentarerstellung

Der geprüfte Fließtext wird an das KI-Sprachmodell (AWS Bedrock, EU-Region Frankfurt, Claude Opus 4.6) übermittelt; das Modell liefert Fehlermarkierungen und Kommentarvorschläge zurück. Stage 2 verarbeitet kein Bild und keine Handschrift mehr — ausschließlich anonymisierten Plaintext. Der KI-Anbieter erhält keine Information über Schule, Lehrkraft oder Schüler (Proxy-Architektur, siehe M5).

3.4.1 Eingesetzte KI-Modelle (Stand 2026-05-21)

Die in der obenstehenden Pipeline genannten KI-Komponenten setzen sich konkret aus folgenden Modellen zusammen. Modellwechsel innerhalb dieser Liste sind via Konfiguration möglich und werden in Anhang C (Änderungshistorie) dokumentiert:

Aufgabe	Modell	Anbieter	Standort
Handschrifterkennung (OCR)	Claude Sonnet 4.6 (multimodal)	AWS Bedrock	Frankfurt am Main (eu-central-1)
Korrektur + Kommentar (primär)	Claude Opus 4.6	AWS Bedrock	Frankfurt am Main (eu-central-1)
Korrektur + Kommentar (1. Fallback)	Claude Sonnet 4.6	AWS Bedrock	Frankfurt am Main (eu-central-1)
Korrektur + Kommentar (2. Fallback)	Mistral Large	Mistral AI SAS	Paris, Frankreich

Die Fallback-Chain (Korrektur + Kommentar) realisiert Verfügbarkeits- und Anbieter-Diversität:

- **Intra-Bedrock-Fallback** (Opus 4.6 → Sonnet 4.6, beide Frankfurt) springt bei modellspezifischen transienten Fehlern (Quota-Limit, Rate-Limit, modell-temporäre Störungen) ein. Anbieter, Region und AVV bleiben identisch — die Auftragsverarbeiter-Bindung ändert sich nicht.
- **Cross-Provider-Fallback** (Bedrock-Region Frankfurt → Mistral AI Paris) greift nur, wenn die gesamte AWS-Bedrock-Region Frankfurt unerreichbar ist. Anbieter wechselt von AWS zu Mistral AI SAS, Region von Frankfurt nach Paris — beide EU-Standorte. Der AVV mit Mistral AI SAS besteht parallel zum AWS-DPA (siehe §3.5 + Anhang A).

Keine Modelle für deterministische Berechnungen: Fehlerzählungen, Notenpunkt-Berechnung, Wortzahl und andere deterministische Größen werden ausschließlich durch Programmcode auf Korrigios Server berechnet — niemals durch ein KI-Modell (Architekturprinzip „Code-vs-KI-Trennung").

Konfigurations-Variablen im Code (`backend/app/core/config.py`): `OCR_MODEL`, `LLM_CORRECTION_MODEL`, `LLM_MODEL`, `LLM_FALLBACK_MODEL`. Modellwechsel sind ohne Code-Änderung möglich; jeder Wechsel wird in Anhang C dieser DSFA erfasst.

Unterschied zur Vorfassung v1.0: Die automatische Named-Entity-Recognition wurde entfernt (sie erfasste auch literarische Figuren und Autoren als „Personen" und machte deren Analyse unmöglich). Die Schutzwirkung wird nun durch zwei gestufte menschliche Kontrollen erreicht: Abdecken vor der Aufnahme + Textprüfung nach OCR.

Korrigio implementiert Anonymisierung über das Vier-Augen-Prinzip „Akknowledgment-Click + audit-log": Lehrkräfte entfernen oder verdecken den Schülernamen vor dem Fotografieren oder Scannen und bestätigen dies pro Upload via Pflicht-Checkbox. Die Bestätigung wird in

`audit.anonymization_acknowledgment_log` revisionssicher (Append-only, Hash-Chain) protokolliert. Eine automatische algorithmische Erkennung und Ersetzung personenbezogener Daten findet nicht statt.

Proxy-Architektur: Alle Anfragen an externe Dienste (OCR, KI) laufen über den Korrigio-Server. Weder der OCR-Dienst noch das KI-Sprachmodell erhalten Informationen darüber, von welcher Lehrkraft, welchem Schüler oder welcher Schule eine Anfrage stammt. Korrigio tritt als einziger Endnutzer gegenüber den Anbietern auf.

3.5 Auftragsverarbeiter und Unterauftragnehmer

Aktualisiert 2026-06-19 (Resend + hCaptcha sowie Hetzner-Backup-Speicher ergänzt):

Dienstleister	Rolle	Serverstandort	Verarbeitete Daten
Felix Beck / Korrigio	Auftragsverarbeiter	Nürnberg, Deutschland (Netcup VPS)	Alle Daten
Supabase Inc. / GmbH	Unterauftragnehmer (Datenbank, Auth)	Frankfurt am Main, Deutschland	Accountdaten, Korrekturdaten, temporäre Uploads
Amazon Web Services EMEA SARL	Unterauftragnehmer (KI-Verarbeitung, primär)	Frankfurt am Main, Deutschland	OCR-Bilder (Stufe 1), Fließtext (Stufe 2)
Mistral AI SAS	Unterauftragnehmer (Backup-LLM, EU-natives Fallback)	Paris, Frankreich	Fließtext (Stufe 2), nur bei AWS-Ausfall aktiv
Netcup GmbH	Unterauftragnehmer (Hosting)	Nürnberg, Deutschland	Server-Protokolldaten, HTTP-Anfragen, ggf. Audit-Protokolle
Hetzner Online GmbH	Unterauftragnehmer (verschlüsselter Backup-Speicher)	Falkenstein, Deutschland (EU)	Client-seitig AES-256-verschlüsseltes borgmatic-Backup der gesamten Produktionsdatenbank — kein Klartextzugriff (Backup enthält alle Datenarten, jedoch ausschließlich verschlüsselt)
Stripe Payments Europe, Ltd.	Unterauftragnehmer (Zahlung)	Irland (EU); ggf. USA via SCCs	Zahlungsdaten der Lehrkraft (kein Schülerbezug)
Resend, Inc.	Unterauftragnehmer (transaktionaler E-Mail-Versand)	USA (Drittland, SCCs)	E-Mail-Adresse + System-Mail-Inhalte der Lehrkraft (kein Schülerbezug)

Dienstleister	Rolle	Serverstandort	Verarbeitete Daten
Intuition Machines, Inc. (hCaptcha)	Unterauftragnehmer (Bot-/ Missbrauchsabwehr)	USA (Drittland, SCCs)	IP-Adresse + Interaktionsdaten der Lehrkraft auf Auth-Seiten (kein Schülerbezug)

Drittlandübermittlung: Bei Stripe (Zahlung), Resend (E-Mail) und hCaptcha (Missbrauchsabwehr) auf Grundlage von EU-Standardvertragsklauseln (SCCs, Art. 46 Abs. 2 lit. c DSGVO) — ausschließlich Account-/Sicherheitsdaten der Lehrkraft. Alle übrigen Verarbeitungen finden ausschließlich auf Servern in der EU statt. Keine Schülerdaten werden in Drittländer übermittelt.

3.6 Speicherdauer

Datenkategorie	Speicherdauer
Fotos/Scans handschriftlicher Arbeiten	Automatische Löschung 30 Tage nach Abschluss der Korrektur (Status Korrigiert), spätestens bei Löschung durch die Lehrkraft; während der Korrekturphase werden die Seitenbilder für die multimodale Mathematik-Bewertung und die Anzeige neben den KI-Markierungen benötigt.
Digitalisierter Text und Korrekturvorschläge	Bis Löschung durch Lehrkraft oder Kontolöschung
Kalibrierungsdaten	Bis Löschung durch Lehrkraft oder Kontolöschung
Server-Log-Dateien	Automatische Löschung nach 30 Tagen
Lehrkraft-Accountdaten	Bis Kontolöschung
KI-Ereignisprotokolle (v11.0)	Mindestens 6 Monate (EU AI Act Art. 12 Abs. 3), maximal 183 Tage (Datenminimierung Art. 5 Abs. 1 lit. e DSGVO). Automatische Löschung via Retention-Sweep.
Anonymisierungs-Protokollereignisse (v11.0)	183 Tage
Protokolle menschlicher Aufsicht (v11.0)	366 Tage (ein volles Schuljahr; Betriebsnachweis Art. 14 AI Act)
Protokolle administrativer Aktionen (v11.0)	366 Tage

3.7 Rechtsgrundlage

Einschlägige Rechtsgrundlage: Art. 6 Abs. 1 lit. e DSGVO (Wahrnehmung einer Aufgabe im öffentlichen Interesse) i. V. m. dem Bildungs- und Erziehungsauftrag gemäß BayEUG (insbesondere Art. 2 Abs. 1) und BaySchO (§§ 19 ff. — Leistungsnachweise und Bewertung). Die Korrektur von Schülerarbeiten ist eine dienstliche Pflicht der Lehrkraft; Korrigio unterstützt diese Pflicht als Assistenzsystem.

Keine zusätzliche Einwilligung erforderlich: Der KM-Handlungsleitfaden „KI in der pädagogischen Praxis" (28.11.2025) stellt auf S. 6 ausdrücklich klar:

> „Sollen in einer KI-Anwendung personenbezogene Daten verarbeitet werden, weil es im konkreten Einsatzszenario sinnvoll und notwendig ist, […] ist zu klären, ob die in Frage stehende Verarbeitung der betroffenen personenbezogenen Daten zur Erfüllung einer schulischen Aufgabe erforderlich ist. Ist das der Fall, dürfen die entsprechenden personenbezogenen Daten auch ohne Zustimmung der Betroffenen verarbeitet werden, sofern die Verarbeitung datenschutzkonform erfolgt."

Die Korrektur von Leistungsnachweisen ist Kernaufgabe der Schule und damit eindeutig „zur Erfüllung einer schulischen Aufgabe erforderlich". Eine Einwilligung der Erziehungsberechtigten nach Art. 6 Abs. 1 lit. a DSGVO ist daher nicht erforderlich. Die Schule kann eine solche Einwilligung aus Gründen der Vorsicht zusätzlich einholen; dies bleibt jedoch der pflichtgemäßen Ermessensentscheidung der DSB überlassen.

Verfahrensschritte gemäß KM-Handlungsleitfaden (S. 4-5, S. 15):

1. **Schulleitungs-Freigabe** als Betriebsmittel (S. 5: „Vor der Nutzung von KI-Systemen sind diese von der Schulleitung im Sinne eines Betriebsmittels freizugeben.")
2. **Prüfung der rechtlichen Anforderungen** durch die Schulleitung (S. 4)
3. **Zeichnung des AVV** zwischen Schule und Korrigio (S. 4)
4. **Kontrolle des AVV** durch den örtlichen Datenschutzbeauftragten (S. 7: „Der örtliche Datenschutzbeauftragte kontrolliert den AVV.")
5. **Information** der Lehrkräfte, Schüler und Erziehungsberechtigten (S. 5: „informieren" — keine Einwilligung)
6. **Aufnahme ins Verfahrensverzeichnis** der Schule (S. 15 Checkliste)

[Schule: Die unter 1-6 genannten Schritte sind nachweisfähig zu dokumentieren.]

---

4. Bewertung der Notwendigkeit und Verhältnismäßigkeit (Art. 35 Abs. 7 lit. b DSGVO)

Weitgehend unverändert gegenüber v1.0. Ergänzende Klarstellung:

4.1 Notwendigkeit der Verarbeitung

Zusätzlich zur bisherigen Begründung (manuelle Korrektur 30–60 min pro Arbeit, 100–200 Arbeiten pro Halbjahr pro Deutschlehrkraft): Mathematik- und Physik-Korrekturen (seit v2.0 und v9.0 in Korrigio integriert) sind noch zeitaufwändiger wegen Folgefehler-Analyse und Rechenschritt-Validierung. Der Effizienzgewinn ist messbar und rechtfertigt die Verarbeitung.

4.2 Verhältnismäßigkeit

Grundsatz	Umsetzung
Datenminimierung	Nur die Handschrift und der daraus extrahierte Text werden verarbeitet. Keine Noten, keine Verhaltensdaten, keine Lernverlaufsdaten, keine Schülerprofile. **Ab v11.0:** Audit-Protokolle speichern nur kryptografische Hashes (SHA-256), niemals Klartext-Prompts oder -Antworten.
Zweckbindung	Daten werden ausschließlich zur Korrekturunterstützung verwendet. Keine Verwendung für KI-Training (vertraglich und technisch ausgeschlossen), keine Analyse, keine Weitergabe an Dritte.
Speicherbegrenzung	Handschrift-Bilder werden 30 Tage nach Korrekturabschluss (Status Korrigiert) automatisch gelöscht (scan_retention_sweep). Korrekturvorschläge werden nur so lange gespeichert, wie die Lehrkraft sie benötigt. Audit-Logs nach 183 bzw. 366 Tagen automatisch gelöscht.
Privacy by Design	Zwei-Stufen-Architektur trennt Bilddaten von KI-Verarbeitung. Menschliche Textprüfung zwischen beiden Stufen. Proxy-Architektur verhindert Zuordnung durch den KI-Anbieter.

4.3 Prüfung milderer Mittel

Der Begriff „erforderlich” in Art. 6 DSGVO bezieht sich nach gefestigter EuGH-Rechtsprechung auf die **konkrete Datenverarbeitung im Einsatzszenario**, nicht auf die Frage, ob das gesamte Werkzeug alternativlos ist. „Erforderlich” bedeutet verhältnismäßig zum verfolgten Zweck; geprüft werden mildere Mittel, die denselben Effekt erbringen. Würde der Begriff als „absolute Alternativlosigkeit”

verstanden, wäre kein digitales Schulwerkzeug (mebis, ByCS, WebUntis, Excel-Notenlisten) jemals zulässig. Die folgende Tabelle dokumentiert die Prüfung milderer Mittel für Korrigio:

Alternative	Bewertung
Keine digitale Unterstützung (Status quo)	Kein Datenschutzrisiko, aber keine Entlastung der Lehrkraft. Nicht verhältnismäßig im Vergleich zum nach den TOMs geringen Risiko.
Manuelle Texteingabe statt OCR	Möglich — Korrigio unterstützt diesen Weg als Alternative (Freitextfeld). Praktikabel bei kleineren Textmengen, unpraktikabel bei Klassensätzen.
Nur lokale Verarbeitung ohne Cloud-KI	Derzeit technisch nicht in vergleichbarer Qualität möglich. Open-Source-Modelle (Llama, Mistral) erreichen die nötige Deutsch-Korrektur-Qualität aktuell nicht. Fortschritte werden beobachtet — Architekturwechsel möglich, da Modell austauschbar (Modellabstraktions-Schicht).

Ergebnis: Die KI-Verarbeitung in Korrigio steht in vernünftigem Verhältnis zum durch die TOMs (siehe §6) auf „gering" reduzierten Restrisiko — die Erforderlichkeit nach Art. 35 Abs. 7 lit. b DSGVO ist damit positiv festgestellt.

---

5. Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen (Art. 35 Abs. 7 lit. c DSGVO)

5.1 Identifizierte Risiken

Nr.	Risiko	Betroffene	Beschreibung
R1	Unbefugter Zugriff auf Handschrift-Scans	Schüler	Dritte könnten auf die temporär gespeicherten Fotos zugreifen
R2	Re-Identifizierung durch KI-Anbieter	Schüler	KI-Anbieter könnte Textinhalte einer Person zuordnen
R3	Fehlerhafte KI-Korrektur mit Bewertungsfolge	Schüler	Fehlerhafte KI-Vorschläge werden ungeprüft übernommen und beeinflussen die Note
R4	Zweckentfremdung der Daten	Schüler, Lehrkraft	Daten werden für andere Zwecke als die

Nr.	Risiko	Betroffene	Beschreibung
			Korrekturunterstützung verwendet
R5	Datenverlust durch Systemausfall	Schüler, Lehrkraft	Korrekturdaten gehen durch technischen Defekt verloren
R6	Profilbildung über Schüler	Schüler	Aus den Korrekturergebnissen werden Leistungsprofile erstellt
R7 (neu v2.0)	**Verbleib personenbezogener Inhalte im OCR-Text**	Schüler	Namensnennungen im Aufsatz-Inhalt oder versehentlich mitfotografierte Namensfelder erreichen die KI
R8 (neu v2.0)	**Manipulation oder Löschung von Protokolldaten**	Schüler, Lehrkraft	Ereignisprotokolle werden nachträglich verändert, verhindert Nachvollziehbarkeit nach Art. 12 AI Act
R9 (neu v2.0)	**Ausfall der KI-Anbieter-Bindung an No-Training-Zusagen**	Schüler	Vertragsbruch durch Unterauftragnehmer — Daten fließen in Modelltraining
R10 (neu v2.1)	**Drittlands-Zugriff auf AWS-Bedrock-Daten via US CLOUD Act / FISA Section 702**	Schüler	AWS Bedrock wird in Frankfurt betrieben, AWS ist jedoch US-Konzern; US-Behörden könnten theoretisch via CLOUD Act oder FISA Section 702 Datenherausgabe verlangen. KM-Handlungsleitfaden S. 7 verlangt explizit: „Es darf keine Datenübermittlung an Staaten erfolgen, in denen die DSGVO nicht gilt.”

5.2 Risikobewertung

Nr.	Eintrittswahrscheinlichkeit	Schwere	Maßnahmen	Restrisiko
R1	Gering	Mittel	M1, M2, M3, M6	Gering
R2	Sehr gering	Mittel	M4, M5, M6	Sehr gering
R3	Mittel	Mittel	M7, M8, M20	Gering
R4	Sehr gering	Hoch		Sehr gering

Nr.	Eintrittswahrscheinlichkeit	Schwere	Maßnahmen	Restrisiko
			M9, M10, M11	
R5	Gering	Gering	M12, M13	Gering
R6	Sehr gering	Hoch	M4, M5, M14	Sehr gering
R7	Mittel	Mittel	**M19, M20**	Gering
R8	Sehr gering	Hoch	**M21, M22**	Sehr gering
R9	Sehr gering	Hoch	M10, M11	Sehr gering
R10 (v2.1)	Sehr gering	Mittel	**M26**, M5, M9, M10	Sehr gering

6. Maßnahmen zur Bewältigung der Risiken (Art. 35 Abs. 7 lit. d DSGVO)

6.1 Technische Maßnahmen (von Korrigio umgesetzt)

Nr.	Maßnahme	Adressierte Risiken	Status
M1	**Verschlüsselung:** TLS 1.3 für alle Datenübertragungen; Datenbankverschlüsselung at rest	R1	aktiv
M2	**Zugriffskontrolle:** Authentifizierung über Supabase Auth (JWT/JWKS); jede Lehrkraft sieht nur eigene Daten	R1	aktiv
M3	**Automatische Löschung von Source-Files:** Hochgeladene Foto- und Scan-Dateien (Seitenbilder) werden 30 Tage nach Abschluss der Korrektur (Status Korrigiert) automatisch gelöscht (scan_retention_sweep). Im Plaintext-Modus (Phase 90 — Pfad A) werden hochgeladene Source-Files (`.docx`, `.txt`, `.md`) ebenfalls sofort nach der serverseitigen Plaintext-Extraktion gelöscht — die Extraktion erfolgt vollständig im Hauptspeicher (UploadFile-Bytes sind request-scoped und werden nach Beendigung des HTTP-Requests vom Garbage-Collector freigegeben); ein dauerhafter Source-File-Speicher entsteht in beiden Modus-Varianten nicht. Nur der extrahierte Plaintext landet in der Submission-Datensatz-Spalte `confirmed_text`.	R1	aktiv
M4	**Zweistufige Personenbezugs-Trennung:** Bild-Pipeline und Text-Pipeline sind getrennt; Textprüfungsschritt zwischen OCR und KI-Korrektur gibt der Lehrkraft Gelegenheit zur finalen Entfernung von Namen	R2, R6, R7	aktiv (ersetzt die automatische NER-

Nr.	Maßnahme	Adressierte Risiken	Status
			Komponente aus v1.0)
M5	**Proxy-Architektur:** KI-Anbieter erhält keine Information über Schule, Lehrkraft oder Schüler	R2, R6	aktiv
M6	**EU-Hosting:** Alle Server in Deutschland (Nürnberg, Frankfurt). Keine Schülerdaten in Drittländern.	R1, R2	aktiv
M7	**Human-in-the-Loop:** Jede KI-Korrektur muss von der Lehrkraft geprüft und bestätigt werden	R3	aktiv
M8	**KI-Transparenz:** Nutzungsbedingungen weisen explizit auf Fehlerhaftigkeit der KI-Ergebnisse hin	R3	aktiv
M9	**Kein KI-Training:** Vertragliche und technische Garantie, dass Daten nicht zum Training von KI-Modellen verwendet werden	R4	aktiv (AWS Bedrock DPA)
M10	**AVV mit Unterauftragnehmern:** Auftragsverarbeitungsverträge mit allen Dienstleistern gemäß Art. 28 DSGVO	R4, R9	aktiv
M11	**Keine Speicherung beim KI-Anbieter:** AWS Bedrock speichert keine Eingabedaten (gemäß DPA)	R4, R9	aktiv
M12	**Regelmäßige Backups:** Tägliche client-seitig AES-256-verschlüsselte Backups (borgmatic → Hetzner Storage Box, Falkenstein — Unterauftragnehmer, AVV 19.06.2026, kein Klartextzugriff durch Hetzner)	R5	aktiv
M13	**Redundante Infrastruktur:** Datenbank bei Supabase (Frankfurt) mit eigener Backup-Strategie	R5	aktiv
M14	**Keine Profilbildung:** Korrigio erstellt keine schülerbezogenen Leistungsprofile. Fehlerstatistiken beziehen sich auf einzelne Arbeiten, nicht auf Personen über Zeitverläufe.	R6	aktiv
M19	**Bestätigungs-Pflicht beim Upload mit Audit-Log (AKLOG-03..06):** Vor dem ersten Upload muss die Lehrkraft im Dialog aktiv bestätigen, den Schülernamen vor dem Fotografieren oder Scannen entfernt, abgedeckt oder digital geschwärzt (In-App-Schwärzung vor dem Upload) zu haben. Jeder Upload erzeugt einen revisionsfesten Eintrag im `audit.anonymization_acknowledgment_log` (pseudonymisierter Nutzer, Submission-Hash, Zeitpunkt, `acknowledgment_given`-Boolean). Auf Wunsch wird die Bestätigung pro Lehrkraft als Voreinstellung gespeichert (`anonymization_acknowledgment_default=true`); der Audit-Log-Eintrag wird trotzdem für jeden	R7	aktiv (v11.0)

Nr.	Maßnahme	Adressierte Risiken	Status
	Upload erzeugt. Diese Maßnahme realisiert das Vier-Augen-Prinzip „Akknowledgment-Click + audit-log" auf technischer Ebene.		
M20	**Textprüfungsschritt zwischen OCR und KI-Korrektur:** Nach der Texterkennung zeigt die UI den erkannten Text und fordert die Lehrkraft auf, verbleibende personenbezogene Inhalte zu entfernen, bevor die KI-Korrektur startet	R3, R7	aktiv
M21	**Revisionsfeste KI-Ereignisprotokollierung (EU AI Act Art. 12):** Jeder KI-Inferenzaufruf wird automatisch protokolliert (Modell, Zeitpunkt, Dauer, Ausgang, pseudonymisierter Nutzer). Protokolle enthalten keine Klartext-Prompts oder -Antworten, nur kryptografische Hashes. Append-only-Tabelle mit DB-Trigger-Immutabilität und Hash-Chain für Tamper-Evidenz.	R8	aktiv (v11.0)
M22	**Automatisierte Aufbewahrungsfrist-Durchsetzung:** Täglicher Retention-Sweep (`app.scripts.retention_sweep`) wechselt in die eingeschränkte PostgreSQL-Rolle `korrigio_audit_retention`, verifiziert die Hash-Ketten aller fünf Tabellen und löscht danach Protokolleinträge, die die Aufbewahrungsfrist überschritten haben. Sentry-P1-Alarm bei Kettenbruch oder Sweep-Ausfall.	R8	aktiv (v11.0)
M23	**Protokoll menschlicher Aufsicht (AI Act Art. 14):** Jede Korrektur-Prüfung, -Bestätigung und -Ablehnung durch die Lehrkraft wird revisionsfest in `audit.human_oversight_log` protokolliert. Nachweis: KI-Ausgaben werden niemals automatisch wirksam — der Mensch entscheidet stets.	R3, R8	aktiv (v11.0)
M24	**Protokoll privilegierter Aktionen:** Administrative Vorgänge (Datenexport, Kontolöschung, Retention-Sweep) werden revisionsfest in `audit.admin_action_log` protokolliert.	R8	aktiv (v11.0)
M25	**Wiederherstellungsfähigkeit & Notfallplan (Art. 32 Abs. 1 lit. c DSGVO):** Wöchentlicher automatisierter Restore-Drill verifiziert die Wiederherstellbarkeit der Backups (Hash-Ketten + Tabellen-Counts gegen Live-Stand). Dokumentiertes Notfall-Wiederherstellungsverfahren liegt unter `docs/ops/disaster-recovery.md` vor; deckt VPS-Total-Verlust, Postgres-Korruption und Storage-Box-Verlust. Zielwerte für die Wiederherstellung (RTO ≈ 8h, RPO ≈ 24h) sind als interne Messgrößen, nicht als kontraktuelle SLA-Zusagen, dokumentiert; tatsächliche Werte	R5, R7	aktiv (v12.0)

Nr.	Maßnahme	Adressierte Risiken	Status
	werden nach erstem realem Recovery-Vorfall gemessen und im Runbook fortgeschrieben.		
M26	**Schrems-II-Defense für AWS Bedrock (Frankfurt) und EU-nativer Fallback:** AWS ist US-Konzern; US-Behörden könnten theoretisch via CLOUD Act / FISA Section 702 Zugriff auf in der EU verarbeitete Daten verlangen. Korrigio mindert dieses Risiko durch: (a) ausschließliche Nutzung der AWS-EU-Region Frankfurt (eu-central-1) für Bedrock ohne grenzüberschreitendes Routing; (b) AWS-DPA inklusive Standardvertragsklauseln + ergänzende EU-Annex-Klauseln + Transparency-Report-Verpflichtung; (c) keine personenbezogenen Anmelde-/Identifikationsdaten in den API-Aufrufen (Proxy-Architektur, vgl. M5); (d) Mistral AI SAS Paris als jederzeit aktivierbarer EU-nativer Fallback-LLM ohne US-Konzern-Bindung (siehe §3.5). Ein theoretischer behördlicher Zugriffsversuch wäre durch die Proxy-Architektur ohnehin auf inhaltsbezogene, nicht personenidentifizierende Daten beschränkt. Erfüllt KM-Handlungsleitfaden S. 7 („Es darf keine Datenübermittlung an Staaten erfolgen, in denen die DSGVO nicht gilt").	R10	aktiv (v2.1)

6.2 Organisatorische Maßnahmen (von der Schule umzusetzen)

Nr.	Maßnahme	Umsetzung
M15	**Freigabe als Betriebsmittel durch die Schulleitung** (KM-Handlungsleitfaden S. 5: „Vor der Nutzung von KI-Systemen sind diese von der Schulleitung im Sinne eines Betriebsmittels freizugeben.")	*[Schule: Schulleitungs-Beschluss schriftlich dokumentieren und im Verfahrensverzeichnis vermerken]*
M16	**Schulung der Lehrkräfte**	*[Schule: Lehrkräfte über die Pflicht zum Abdecken der Namen vor der Aufnahme und zur Prüfung der KI-Ergebnisse informieren]*
M17	**Zugangsbeschränkung**	*[Schule: Festlegen, welche Lehrkräfte Korrigio nutzen dürfen]*
M18	**Information (nicht Einwilligung) der Lehrkräfte, Schüler und Erziehungsberechtigten**	*[Schule: Muster-Informationsblatt verteilen; Empfang nachweisbar dokumentieren. Eine*

Nr.	Maßnahme	Umsetzung
	nach Art. 13 DSGVO (KM-Handlungsleitfaden S. 5: „[…] sind die Lehrkräfte, Schülerinnen und Schüler sowie die Erziehungsberechtigten über den Einsatz der KI-Systeme […] zu informieren.")	*ausdrückliche Einwilligung ist nicht erforderlich (siehe Abschnitt 3.7), kann von der Schule aber zusätzlich eingeholt werden.]*
M19-Schule	**Dienstliche Weisung Namensabdeckung**	*[Schule: Schriftliche Weisung an die Lehrkräfte, dass Schülernamen auf Arbeiten vor dem Fotografieren durch Aufkleber, Schwärzung oder Umschlagblatt abgedeckt werden müssen. Realisiert die AKLOG-03..06-Bestätigungspflicht auf organisatorischer Ebene.]*

§6 Auditprotokollierung (EU AI Act Art. 12)

Korrigio führt fünf zweckgetrennte Audit-Tabellen im dedizierten `audit.*`-Schema:

Tabelle	Zweck	Speicherfrist
`audit.ai_event_log`	Eine Zeile pro bewertungsrelevantem LLM-Aufruf (Korrektur, Kommentar, Kalibrierung)	183 Tage
`audit.anonymization_acknowledgment_log`	Eine Zeile pro Upload-Bestätigung	183 Tage
`audit.human_oversight_log`	Eine Zeile pro Lehrkraft-Eingriff (accept/override/edit)	366 Tage
`audit.admin_action_log`	Eine Zeile pro privilegierter Admin-Aktion (Datenexport, Kontolöschung, Retention-Sweep)	366 Tage
`audit.eh_suggestion_log`	Eine Zeile pro KI-EH-Lücken-Vorschlag-Lebenszyklus (generated / confirmed / rejected; Art. 14 menschliche Aufsicht)	366 Tage

Manipulationsschutz: PostgreSQL-Trigger blockieren UPDATE/DELETE für die Anwendungsrolle. Zusätzlich verkettet jede Tabelle ihre Zeilen über SHA-256-Hashes (`prev_row_hash` ⇒ `row_hash`); nachträgliche Änderungen sind kryptographisch erkennbar via `chain_verifier.verify_chain()`.

Löschung: Eine täglich um 03:00 Uhr (Europe/Berlin) ausgeführte Bereinigung (`app.scripts.retention_sweep`) wechselt vor jeglicher Löschung in eine eingeschränkte PostgreSQL-Rolle (`korrigio_audit_retention`), prüft die Hash-Ketten aller fünf Tabellen und bricht bei Integritätsverletzung mit P1-Sentry-Alarm ab. Ergebnis und gelöschte Zeilenanzahl werden selbst wieder als Audit-Zeile verewigt.

Pseudonymisierung: Nutzer-IDs werden ausschließlich als HMAC-SHA256(user_id, audit_user_pepper) gespeichert. Pepper-Rotation = Krypto-Erlöschen aller historischen `user_hash`-Werte (siehe Runbook `docs/runbooks/audit-pepper.md`).

---

7. Stellungnahme des behördlichen Datenschutzbeauftragten (Art. 35 Abs. 2 DSGVO)

[Vom DSB der Schule auszufüllen. Struktur unverändert gegenüber v1.0.]

---

8. Ergebnis und Freigabe

8.1 Gesamtbewertung des Restrisikos

Nach Umsetzung der in Abschnitt 6 beschriebenen technischen und organisatorischen Maßnahmen ist das Restrisiko für die Rechte und Freiheiten der betroffenen Schülerinnen und Schüler als **gering** einzustufen:

- Handschrift-Bilder werden 30 Tage nach Abschluss der Korrektur (Status Korrigiert) automatisch gelöscht (scan_retention_sweep)
- Zweistufige Personenbezugs-Trennung (Namensabdeckung vor Aufnahme + Textprüfung nach OCR)
- Proxy-Architektur verhindert Zuordnung durch KI-Anbieter
- Lehrkraft behält volle Entscheidungshoheit (kein Automatismus)
- Alle Schülerdaten verbleiben in der EU (Deutschland: Frankfurt, Nürnberg; Backup-LLM: Paris)
- Vertragliche Absicherung durch AVV mit allen Unterauftragnehmern
- **Ab v11.0:** Revisionsfeste Ereignisprotokollierung gemäß EU AI Act Art. 12 mit hash-basierter Tamper-Evidenz und automatisierter Aufbewahrungsfrist-Durchsetzung via `korrigio_audit_retention`-Rolle
- **Ab v2.1:** Schrems-II-Defense für AWS Bedrock (M26) explizit dokumentiert; Mistral Paris als jederzeit aktivierbarer EU-nativer Fallback
- **Konformität mit dem KM-Handlungsleitfaden „KI in der pädagogischen Praxis" (28.11.2025)** in allen relevanten Verfahrensschritten (Abschnitte 2.2, 3.7, 6.1 M26, 6.2 M15 + M18)

- **Nicht-Hochrisiko-Einstufung nach EU AI Act Art. 6 Abs. 3** ist in `docs/datenschutz/eu-ki-verordnung-einstufung.md` (Anbieter-Bewertung gemäß Art. 6 Abs. 4) detailliert begründet und steht in Einklang mit KM-Handlungsleitfaden S. 8

8.2 Entscheidung der Schulleitung

[Struktur unverändert gegenüber v1.0]

Anhang A: Unterauftragnehmer-Liste

Unterauftragnehmer	Anschrift	Serverstandort	Leistung	AVV vorhanden
Supabase Inc. / GmbH	970 Toa Payoh North, Singapore (Firma) / Frankfurt (Server)	Frankfurt am Main, DE	Datenbank, Authentifizierung, Dateispeicher	Ja (DPA)
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, Luxembourg	Frankfurt am Main, DE	KI-Sprachmodell (Claude via Bedrock), OCR	Ja (DPA)
Netcup GmbH	Daimlerstraße 25, 76185 Karlsruhe	Nürnberg, DE	VPS-Hosting, Reverse Proxy	Ja (AVV)
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen	Falkenstein, DE	Verschlüsselter Backup-Speicher (Storage Box)	Ja (AVV 19.06.2026)
Stripe Payments Europe, Ltd.	1 Grand Canal Street Lower, Dublin 2, Irland	Irland (EU); USA via SCCs	Zahlungsabwicklung	Ja (DPA + SCCs)
Mistral AI SAS	15 Rue des Halles, 75001 Paris, Frankreich	Paris, Frankreich	Backup-LLM (Inferenz)	Ja (DPA)
Sentry (Functional Software, Inc.)	132 Hawthorne Street, San Francisco, CA	EU-Region (konfiguriert)	Fehler-Tracking	Ja (DPA)
Resend, Inc.	2261 Market Street #5039, San Francisco, CA 94114 (Rechtsträger: Plus Five Five, Inc.)	USA (Drittland, SCCs)	Transaktionaler E-Mail-Versand	Ja (Terms + SCCs)

Unterauftragnehmer	Anschrift	Serverstandort	Leistung	AVV vorhanden
Intuition Machines, Inc. (hCaptcha)	350 Alabama St, San Francisco, CA 94110	USA (Drittland, SCCs)	Bot-/ Missbrauchsabwehr	Ja (Terms + SCCs)

Anhang B: Verweis auf weitere Dokumente

- **AVV:** Separat abzuschließen zwischen Schule und Korrigio.
- **Eltern-Informationsblatt:** Muster-Informationsschreiben für Erziehungsberechtigte.
- **Datenschutzerklärung:** korrigio.de/datenschutz
- **Nutzungsbedingungen:** korrigio.de/nutzungsbedingungen
- **Sub-Processor-Register:** `docs/datenschutz/sub-processors.md` / korrigio.de/sub-processors
- **EU AI Act Ereignisprotokoll-Auszug für Ihre Schule:** Auf Anfrage via info@korrigio.de; Self-Service-Export über Admin-Oberfläche ab v12.0
- **Audit-Pepper-Runbook:** `docs/runbooks/audit-pepper.md`
- **Audit-Retention-Runbook:** `docs/runbooks/audit-retention.md`

Anhang C: Änderungshistorie

Version	Datum	Änderung
v1.0	März 2026	Erstveröffentlichung auf Basis automatischer NER-Anonymisierung
v2.0-draft	April 2026 (Entwurf)	Entfernung NER-Komponente (Migration 028, 24.03.2026) dokumentiert; neue TOMs M19–M24 für v11.0-Protokollierungsinfrastruktur; Risiken R7–R9 ergänzt; Hinweis zu EDPB Opinion 28/2024 in §2.1
v2.0	2026-04-25	Finale Version: §3.4 Anonymisierungskontrolle auf Akknowledgment-Click + audit-log umgestellt; §6 Auditprotokollierung (EU AI Act Art. 12) als neuer Top-Level-Abschnitt eingefügt; M19 auf AKLOG-03..06-Bestätigungspflicht aktualisiert; M22 auf host-cron Retention-Sweep aktualisiert (statt Celery); alle

Version	Datum	Änderung
		-Markierungen auf aktiv gesetzt
v2.1	**2026-05-21**	**Einarbeitung des KM-Handlungsleitfadens „KI in der pädagogischen Praxis" (Stand 28.11.2025) als maßgebliche bayerische Auslegungsquelle: neuer §2.2 mit Belegstellen-Zitaten zu S. 4-8 + S. 15; §3.5 Mistral als zweiter EU-LLM-Anbieter explizit in Haupt-Tabelle aufgenommen; §3.7 Rechtsgrundlage präzisiert (Erforderlichkeits-Ausnahme nach KM-Leitfaden S. 6 stützt Art. 6 Abs. 1 lit. e ohne zusätzliche Einwilligung); neues Risiko R10 (CLOUD-Act-Zugriff AWS Bedrock); neue TOM M26 (Schrems-II-Defense AWS + EU-nativer Mistral-Fallback); M15 + M18 mit KM-Zitaten geschärft (Betriebsmittel-Freigabe, Informationspflicht statt Einwilligungspflicht); §8.1 Restrisiko-Bewertung um KM-Konformitäts-Bullet und Nicht-Hochrisiko-Verweis ergänzt; neue §3.4.1 mit konkreter Modell-Tabelle (OCR = Claude Sonnet 4.6 multimodal; Korrektur primär = Claude Opus 4.7; Fallbacks = Sonnet 4.6 + Mistral Large 2 Paris); Modellbezeichnungen im §3.4-ASCII-Pipeline-Diagramm an aktuellen Stand angepasst (Claude-Multimodal → Claude Sonnet 4.6 OCR; Stufe-2-Primärmodell Sonnet 4.6 → Opus 4.7)**
v2.2	**2026-05-22**	**Phase-90-Plaintext-Pfad: §3.4 Pipeline-Beschreibung auf „Stage 1 mit zwei Modus-Varianten" (Modus A OCR via AWS Bedrock; Modus B Direct-Plaintext-Ingest via Lehrer-Upload)**

Version	Datum	Änderung
		erweitert; §6.1 M3 ergänzt um „extrahierte Source-Files (.docx/.txt/.md) werden nach Plaintext-Extraktion sofort gelöscht — kein dauerhafter Source-File-Speicher in beiden Modi". Sub-Processor-Liste unverändert (python-docx ist Pure-Python).
v2.3	**2026-06-11**	**Korrektur des Lösch-Versprechens §3.3/§3.4/§3.6 (30 Tage nach Korrigiert statt nach OCR-Bestätigung); M3 angepasst (scan_retention_sweep); M19/§3.4-Vorbereitung um „digital geschwärzt (In-App-Schwärzung)" erweitert (Phase 112)**
v2.4	**2026-06-19**	**Sub-Prozessor-Register auf 8 angeglichen (Resend + hCaptcha in §3.5/Anhang A ergänzt; Drittland-Satz korrigiert — drei US-Empfänger statt „ausschließlich Stripe"); Modellname auf deployed Opus 4.6 korrigiert; „Mistral Large 2" → „Mistral Large" (Cross-Surface-Drift-Fix §5 A); eingetragene Anschriften der US-Sub-Prozessoren in Anhang A nachgetragen (Resend-Rechtsträger: Plus Five Five, Inc.)**
v2.5	**2026-06-19**	**Hetzner Online GmbH als Sub-Auftragsverarbeiter (verschlüsselter Backup-Speicher, Storage Box Falkenstein) in §3.5 + Anhang A ergänzt und M12 entsprechend präzisiert (L2-dsfa-01); AVV mit Hetzner abgeschlossen 19.06.2026 (elektronisch). Das Backup ist client-seitig AES-256-verschlüsselt — kein Klartextzugriff durch Hetzner; EU-Standort,**

Version	Datum	Änderung
		keine Drittland-Übermittlung.