

MUSTER 2 DER ICT-FACHGRUPPE OSKIN

Datenschutz- Folgenabschätzung (Risikoanalyse)

Einsatz einer KI-Plattform - § 7b DSG ZG / § 5a VIP (BGS 157.12)



Muster der ICT-Fachgruppe OSKIN. Anonymisiertes Anschauungsbeispiel, kein rechtlicher Rat. Die Plattform «beispielKI» und die beispielKI GmbH sind frei erfundene Muster. Angaben in eckigen Klammern sind Platzhalter, alle Personenzahlen und Daten sind Musterwerte. Sie sind durch die effektiven Werte des jeweiligen Schulträgers zu ersetzen; die Risikobeurteilung ist im Einzelfall vorzunehmen.

FELD	ANGABE
Verantwortlich	[Vorname Name], Leitung ICT [Schulträger]
Auftraggeber	[Vorname Name], Rektorat [Schulträger]
Rechtsgrundlage	§ 7a/7b DSG ZG (BGS 157.1); § 5a VIP (BGS 157.12)
Gegenstand	beispielKI Schulträgerlizenz (beispielKI GmbH, Musterstadt)
Status	Muster
Freigabe durch	[Rektorat / Gemeinderat - ausstehend]

01 Zweck und Einordnung

§ 5a VIP

Teil des Gesamtprozesses nach § 7a bis 7b DSG ZG

Diese Datenschutz-Folgenabschätzung (DSFA) dokumentiert die systematische Risikoanalyse für den geplanten Einsatz der KI-Plattform beispielKI beim Schulträger ab Schuljahr 20XX/XX. Sie erfüllt die Anforderungen von § 5a der Verordnung über die Informationssicherheit von Personendaten (VIP, BGS 157.12) des Kantons Zug.

Die vorgelagerte Schwellenwertanalyse (siehe separates Dokument) ergab, dass die Schwelle für eine DSFA nach § 7b Abs. 1 DSG ZG erreicht ist. Die DSFA ist Teil des in § 7a-7b DSG ZG vorgesehenen Gesamtprozesses. Die Risikoanalyse, die getroffenen technischen und organisatorischen Massnahmen sowie der mit beispielKI abgeschlossene Vertragsanhang Schweizer Datenschutzrecht bilden zusammen die Grundlage für die Beurteilung, ob eine Vorabkonsultation mit der Datenschutzstelle des Kantons Zug nach § 7b Abs. 3 DSG ZG erforderlich ist (siehe Kapitel 6). Ergänzend zur DSFA sind eine Rechtsgrundlagenanalyse und ein ISDS-Konzept zu erstellen.

02 Beschreibung der Datenbearbeitung

Fünf Teile

Zweck, Personen, Daten, Datenfluss, Bekanntgabe ins Ausland

2.1 Zweck der Datenbearbeitung

beispielKI wird als zentrale KI-Plattform für das Weiterbildungsprogramm 20XX/XX und den laufenden Unterrichtseinsatz eingeführt. Die Datenbearbeitung dient folgenden Zwecken:

- KI-gestützte Unterrichtsplanung, Materialerstellung und Differenzierung durch Lehrpersonen
- Datenschutzkonforme KI-Klassenräume für Schülerinnen und Schüler ab der 5. Klasse
- Erstellung eigener KI-Assistenten (Coaching-Bots) durch Lehrpersonen und Lernende
- KI-Bildgenerierung für Unterrichtsmaterialien
- Online-Fortbildungen für Lehrpersonen im Rahmen der Praxisphase

2.2 Betroffene Personen

KATEGORIE	ANZAHL (MUSTER)	ALTER	ZUGANGSART
Lehrpersonen	200	Erwachsene	Persönliches Konto (Edulog oder direkt)
SuS Zyklus 3 (Oberstufe)	300	12-16 Jahre	Pseudonym via Klassenraum-Code
SuS Zyklus 2 (ab 5. Kl.)	250	10-12 Jahre	Pseudonym via Klassenraum-Code
Dritte (indirekt)	Unbestimmt	Alle	Keine (erwähnt in Prompts)

Die Personenzahlen sind Musterwerte und durch die effektiven Verhältnisse des Schulträgers zu ersetzen.

2.3 Art der Personendaten

2.3.1 Systemseitig erhobene Daten

DATENKATEGORIE	INHALT	BESONDERS SCHÜTZENSWERT?
Kontodaten LP	Name, E-Mail, Schulzugehörigkeit	Nein
SuS-Identifikation	Pseudonym (z.B. «Schüler 7»), Klassenraum-Code	Nein (pseudonym)
Nutzungsdaten	Zeitstempel, gewähltes KI-Modell, Zeichenanzahl	Nein
Chat-Verläufe	Prompts und KI-Antworten	Potenziell
Uploads	Hochgeladene Dateien zur Verarbeitung	Potenziell
Generierte Inhalte	KI-generierte Texte, Bilder, Assistenten	Nein (maschinell)

2.3.2 Risiko durch Nutzereingaben

Die zentrale datenschutzrechtliche Herausforderung liegt nicht in den systemseitig erhobenen Daten, sondern in den Inhalten, die Nutzende in Prompts eingeben. Folgende Szenarien sind realistisch:

- Lehrperson gibt bei der Unterrichtsplanung den Namen und Förderbedarf eines Kindes ein
- Lehrperson lädt ein Dokument mit Schülerbeurteilungen zur Zusammenfassung hoch
- Schülerin oder Schüler gibt in einem KI-Chat persönliche Informationen preis (Gesundheit, familiäre Situation)
- Lehrperson erstellt ein KI-Bild mit Bezug zu einer realen, identifizierbaren Person

In diesen Fällen würden potenziell besonders schützenswerte Personendaten (Gesundheitsdaten, Massnahmen der sozialen Hilfe) an die Plattform und deren Unterauftragsbearbeiter übermittelt.

2.4 Datenfluss und Aufbewahrung

Der Datenfluss bei der Nutzung von beispielKI folgt einem mehrstufigen Proxy-Modell:

Stufe 1 - Plattform: Nutzende interagieren mit der beispielKI-Weboberfläche. Die Plattform wird auf Scalingo SAS (Strassburg, ISO 27001) gehostet. Dateiuploads werden auf AWS S3 (Luxemburg) mit kundenseitiger Verschlüsselung gespeichert.

Stufe 2 - Proxy: beispielKI empfängt den Prompt, entfernt Metadaten (inkl. IP-Adresse) und leitet den bereinigten Prompt über die API-Schnittstelle an den gewählten LLM-Anbieter weiter. Es werden keine Consumer-Produkte (z.B. ChatGPT-Webinterface) verwendet.

Stufe 3 - LLM-Verarbeitung: Der LLM-Anbieter verarbeitet den Prompt und liefert die Antwort zurück. Die Eingabedaten werden gemäss AVV

maximal 30 Tage aufbewahrt (24 Stunden bei Handschrifterkennung) und nicht für Modelltraining verwendet.

2.4.1 Unterauftragsbearbeiter und Aufbewahrungsfristen

UNTERNEHMEN	FUNKTION	SITZ	HOSTING	AUFBEWAHRUNG	SCHUTZNIVEAU?
Scalingo SAS	Plattform-Hosting	Frankreich	Strassburg	Laufzeit	Ja
AWS EMEA SARL	Storage + LLM	Luxemburg	EU	30 Tage (LLM)	Ja
OpenAI Ireland	LLM (API)	Irland	EU	30 Tage	Ja
Microsoft Ops. Ireland	Azure LLM	Irland (Konz.: USA)	EU (Azure)	30 Tage	Eingeschränkt
Anthropic Ireland	LLM (API)	Irland	EU	30 Tage	Ja
Mistral AI	LLM (API)	Frankreich	Frankreich	30 Tage	Ja
Google Cloud EMEA	LLM (API)	Irland	EU	30 Tage	Ja

Hinweis: In diesem Muster ist Microsoft Operations Ireland Ltd Vertragspartnerin gemäss AVV (Anlage Unterauftragsbearbeiter). Die Konzernmutter Microsoft Corporation (USA) unterliegt dem US CLOUD Act, was einen potenziellen Zugriff durch US-Behörden ermöglicht. Weitere typische Subprozessoren: Scaleway (FR), OVH (DE), IONOS (DE), Nebius B.V. (NL). Die konkrete Subprozessor-Kette ist je Plattform individuell zu prüfen.

2.5 Grenzüberschreitende Datenbekanntgabe

Die Datenbearbeitung erfolgt überwiegend im EU/EWR-Raum, der gemäss Anhang 1 der Datenschutzverordnung (DSV) über ein angemessenes Datenschutzniveau verfügt. Die Bekanntgabe in den EU/EWR-Raum ist daher grundsätzlich zulässig.

Die Problematik konzentriert sich auf Microsoft: Die beispielKI-Datenschutzerklärung nennt «Microsoft Corporation» (USA), der AVV dagegen «Microsoft Operations Ireland Limited» (Dublin). Diese Diskrepanz ist klärungsbedürftig. Unabhängig von der Vertragspartnerin unterliegt die Konzernmutter dem CLOUD Act (Clarifying Lawful Overseas Use of Data Act, 2018), der US-Behörden den Zugriff auf Daten ermöglicht, die von US-Unternehmen kontrolliert werden, unabhängig vom Speicherort. Die Privatim-Resolution vom 18. November 2025 qualifiziert dieses Risiko als erhöht.

Mitigierender Faktor: Die über Microsoft Azure verarbeiteten Prompts sind pseudonymisiert (keine Zuordnung zu realen Personen möglich), von Metadaten bereinigt und werden nur 30 Tage aufbewahrt. Lehrpersonen können zudem EU-basierte Modelle (Mistral, Google Cloud EMEA) als Alternative wählen.

03 Risikoanalyse

Zehn Risiken

Eintrittswahrscheinlichkeit und Schwere, dreistufig bewertet

Die Risikoanalyse bewertet die identifizierten Risiken hinsichtlich Eintrittswahrscheinlichkeit und Schwere der möglichen Auswirkungen auf die Grundrechte der betroffenen Personen. Die Bewertung erfolgt auf einer dreistufigen Skala (gering / mittel / hoch). Die Gesamtbewertung ergibt sich aus der Kombination beider Dimensionen. Die nachstehenden Bewertungen sind als Muster zu verstehen und im Einzelfall zu prüfen.

3.1 Risikomatrix

NR.	RISIKO	EW	SCHWERE	GESAMT	MASSNAHMEN	RESTRISIKO
R1	Eingabe besonders schützenswerter Personendaten in Prompts (LP gibt Schülernamen + Förderbedarf ein)	Hoch	Hoch	Hoch	Nutzungsregeln im Merkblatt; Schulung an der schulinternen Weiterbildung; Warnfilter bei Personendaten-Erkennung; Anonymisierungsanleitung	Mittel
R2	SuS geben persönliche/ sensible Informationen in KI-Chat ein (Gesundheit, Familie)	Mittel	Hoch	Hoch	Pseudonyme Zugänge; LP-Aufsicht bei Nutzung; Verhaltensregeln für SuS; KI-Führerschein vor Erstzugang	Mittel
R3	Zugriff durch US-Behörden auf Prompt-Daten bei Microsoft Azure (CLOUD Act)	Gering	Mittel	Mittel	Metadaten-Stripping; Pseudonymisierung; Wahlmöglichkeit EU-basierter Modelle (Mistral, Google Cloud); 30-Tage-Löschfrist	Gering
R4	Datenverlust oder -panne bei Unterauftragsbearbeiter (Breach bei LLM-Anbieter)	Gering	Mittel	Mittel	ISO-27001-Hosting; verschlüsselte Speicherung; AVV mit Meldepflicht; begrenzte Aufbewahrungsfrist	Gering
R5	Nutzung von KI-Ausgaben für Beurteilungsentscheide ohne menschliche Prüfung	Mittel	Mittel	Mittel	KI-Konzept verankert: KI als Werkzeug, nicht Entscheider; LP behält Verantwortung; Beurteilung in der Weiterbildung thematisiert	Gering
R6	Upload von Dokumenten mit Personendaten (Zeugnisse, Berichte, Förderpläne)	Mittel	Hoch	Hoch	Klare Verbotsliste im Merkblatt; technische Sensibilisierung; kein automatischer Upload-Scan durch beispielKI	Mittel
R7	Fehlendes Schweizer Recht im AVV (deutscher Gerichtsstand, DSGVO-Fokus)	Sicher	Mittel	Mittel	Vertragsanhang Schweizer Datenschutzrecht abgeschlossen (siehe separates Dokument); Edulog-Vertrag als ergänzende Grundlage	Gering
R8	Halluzinationen: KI liefert falsche Informationen, die als Fakten übernommen werden	Hoch	Gering	Mittel	Schulung kritisches Denken; KI-Konzept betont Verifikationspflicht; altersgerechte Einführung	Gering

NR.	RISIKO	EW	SCHWERE	GESAMT	MASSNAHMEN	RESTRISIKO
R9	Unzureichende Transparenz gegenüber Eltern über KI-Einsatz und Datenflüsse	Mittel	Mittel	Mittel	KI-Konzept (Elternkommunikation); Elterninformation vor Schuljahresbeginn; Merkblatt als öffentliches Dokument	Gering
R10	Veränderung der Subprocessor-Kette durch beispielKI ohne Kenntnis der Schule	Mittel	Mittel	Mittel	30-Tage-Vorinformation und Antwort-/Zustimmungsfiktion gemäss Art. 3 Vertragsanhang; ausserordentliches Kündigungsrecht mit anteiliger Rückerstattung (Art. 3 Abs. 4); jährliche Überprüfung der Subprocessor-Liste	Gering

Legende Gering Mittel Hoch EW = Eintrittswahrscheinlichkeit. «Sicher» = höchste Eintrittsstufe (rot).

3.2 Gesamtbewertung der Risiken

Die Risikoanalyse identifiziert drei hohe Bruttoisiken (R1, R2, R6), die alle aus dem gleichen Grundproblem resultieren: der Eingabe personenbezogener Daten in KI-Prompts oder Uploads. Diese Risiken lassen sich durch technische Massnahmen allein nicht vollständig eliminieren, da sie vom Verhalten der Nutzenden abhängen. Die vorgeschlagenen Massnahmen (Nutzungsregeln, Schulung, technische Warnfilter) reduzieren das Restrisiko auf mittel.

Die verbleibenden Risiken (R3-R5, R7-R10) sind nach Umsetzung der Massnahmen überwiegend als gering einzustufen. Das ursprünglich mittlere Restrisiko R7 (fehlendes Schweizer Recht im AVV) ist mit dem Abschluss des Vertragsanhangs Schweizer Datenschutzrecht auf gering reduziert.



Fazit: Das Gesamtrisiko ist nach Massnahmenumsetzung vertretbar. Der Vertragsanhang mit beispielKI ist abgeschlossen; die verbleibenden organisatorischen und technischen Massnahmen (insbesondere Merkblatt, Elterninformation und Schulung an der schulinternen Weiterbildung) werden vor dem produktiven Start zum Schuljahresbeginn umgesetzt.

Technische und organisatorische Massnahmen

Drei Ebenen

technisch, organisatorisch, vertraglich; dazu drei verhandelte Abweichungen

4.1 Technische Massnahmen (durch beispielKI)

- **API-only-Zugang zu LLMs:** Keine Nutzung von Consumer-Produkten; separate, restriktivere Datenverarbeitungsbedingungen
- **Metadaten-Stripping:** IP-Adressen und weitere Metadaten werden vor der Weiterleitung an LLM-Anbieter entfernt
- **Pseudonyme SuS-Zugänge:** Keine persönlichen Konten, keine Registrierung, keine personenbezogenen Daten bei Zugang

- **Personendaten-Erkennung:** Automatische Warnung bei Verdacht auf Eingabe personenbezogener Daten
- **Verschlüsselung:** Dateiuploads auf AWS S3 mit kundenseitiger Verschlüsselung (Customer Master Keys bei beispielKI)
- **Modellwahl:** Lehrpersonen können zwischen verschiedenen LLM-Anbietern wählen, inkl. rein EU-basierter Optionen
- **Aufbewahrungsbegrenzung:** 30 Tage bei LLM-Anbietern, danach automatische Löschung

Die technischen und organisatorischen Massnahmen der Auftragnehmerin sind in der beispielKI-Dokumentation «Technische und organisatorische Massnahmen zur Gewährleistung der Sicherheit der Daten gem. Art. 32 DSGVO» (TOM v2.5, Juni 2025) im Detail aufgeführt. Sie umfassen Zutritts-, Zugangs-, Zugriffs- und Trennungskontrolle, SSL-Verschlüsselung, automatisierte Protokollierung von Änderungen und Löschungen sowie einen definierten Meldeprozess für Datenpannen über den externen Datenschutzbeauftragten der beispielKI GmbH.

4.2 Technische Massnahmen (durch den Schulträger)

- **Eduolog-Integration:** Login über die Schweizer Bildungsidentität mit pseudonymisiertem Identifikator (TechID)
- **Klassenraum-Steuerung:** Lehrpersonen aktivieren und deaktivieren KI-Klassenräume gezielt; Einsicht in SuS-Eingaben möglich
- **Zugangssteuerung:** SuS erhalten nur über LP-freigegebene Klassenraum-Codes Zugang, kein eigenständiger Zugriff

4.3 Organisatorische Massnahmen

- **Merkblatt / Nutzungsregeln:** Verbindliche Nutzungsregeln mit konkreter Verbotsliste (welche Daten nie eingegeben werden dürfen)
- **Schulinterne Weiterbildung:** Dedizierter Datenschutz-Block mit Fallbeispielen, Anonymisierungsübungen und Do's/Don'ts
- **KI-Führerschein:** Obligatorische Einführung für SuS vor Erstzugang (Regeln, Risiken, verantwortungsvolle Nutzung)
- **Anonymisierungsanleitung:** Konkrete Anleitung für LP zur Anonymisierung von Schülerdaten vor KI-Eingabe
- **Elterninformation:** Transparente Kommunikation über KI-Einsatz, Datenflüsse und Schutzmassnahmen vor Schuljahresbeginn
- **Rollen und Verantwortlichkeiten:** RACI-Matrix für KI-Einsatz (Leitung ICT, ICTA, Schulleitungen, LP) im KI-Konzept verankert

4.4 Vertragliche Massnahmen

- **AVV mit beispielKI:** Auftragsverarbeitungsvertrag regelt Weisungsgebundenheit, Unterauftragsbearbeiter, Meldepflichten, Löschung
- **No-Training-Klausel:** Vertragliche Garantie, dass Nutzungsdaten nicht für KI-Modelltraining verwendet werden

- **Vertragsanhang Schweizer Datenschutzrecht:** Abgeschlossen - regelt Anwendbarkeit Schweizer Recht, Gerichtsstand am Sitz des Schulträgers, Schutz von Daten Minderjähriger, Werbeverbot, CLOUD-Act-Klärung, 72-Stunden-Meldepflicht und Kooperationspflicht mit der Datenschutzstelle Kanton Zug
- **Edulog-Föderationsvertrag:** Regelt die pseudonymisierte Authentifizierung und Datenminimierung beim Login

4.5 Verhandelte Abweichungen und ihre Beurteilung

Der ursprüngliche Entwurf des Vertragsanhangs wurde im Dialog mit beispielKI an drei Stellen pragmatisch angepasst. Die Abweichungen sind aus datenschutzrechtlicher Sicht vertretbar; ihre Beurteilung wird hier festgehalten.

a) Newsletter für Lehrpersonen (Art. 6 Abs. 3). Abweichung vom strikten Werbeverbot durch ein freiwilliges Opt-in. Lehrpersonen können sich innerhalb der Plattform für den beispielKI-Newsletter anmelden und erhalten danach Informationen zu Plattformneuerungen und Fortbildungsangeboten. Die Abweichung ist eng begrenzt: Sie betrifft ausschliesslich Lehrpersonen (keine Schülerinnen und Schüler), setzt eine aktive Anmeldung voraus und entspricht der gängigen Praxis bei EdTech-Plattformen. Das Risiko ist gering.

b) Subprocessor-Modell (Art. 3 Abs. 2-4). Ursprünglich war ein striktes ZustimmungsmodeLL vorgesehen (positive Einwilligung vor jeder Änderung gemäss § 6 Abs. 4 DSG ZG). Ausgehandelt wurde stattdessen ein pragmatisches Modell aus 30-Tage-Vorinformation, 14-Tage-Antwortfrist und Zustimmungsfiktion bei Schweigen. Als Ausgleich wurde ein ausserordentliches Kündigungsrecht mit anteiliger Rückerstattung verankert (Art. 3 Abs. 4): Verweigert die Auftraggeberin die Zustimmung zu einer geplanten Subprocessor-Änderung aus datenschutzrechtlich begründeten Gründen, kann der Hauptvertrag mit 30 Tagen auf den Wirksamkeitszeitpunkt der Änderung gekündigt werden. Die Schule bleibt damit auch bei einer ungünstigen Entwicklung der Subprocessor-Kette handlungsfähig.

c) Löschung bei Vertragsende (Art. 7 Abs. 2). Ursprünglich war eine automatische Löschung sämtlicher Daten bei Vertragsende vorgesehen. Verhandelt wurde stattdessen eine Löschung auf Aufforderung innert 90 Tagen. Hintergrund auf Seite beispielKI: Lehrpersonen sollen die Möglichkeit haben, selbst erstellte Materialien (Arbeitsblätter, Präsentationen) privat weiterzunutzen, analog zu eigenen Unterlagen im Arbeitszimmer. Da Schülerdaten ohnehin pseudonym und nur 30 Tage bei den LLM-Unterauftragsbearbeitern aufbewahrt werden, betrifft die Klausel primär lehrpersonen-eigene Materialien. Die institutionelle Absicherung erfolgt über die Handover-Checkliste der Leitung ICT: Bei Beendigung des Hauptvertrags wird die Löschung der schulträgerseitigen Daten zwingend mit einem schriftlichen Datenlöschantrag verbunden und intern

dokumentiert. Damit ist das Risiko einer versäumten Löschung praktisch ausgeschlossen.

05

Offene Punkte und Handlungsbedarf

Sieben Massnahmen

je mit Verantwortung, Frist und Status

NR.	MASSNAHME	VERANTWORTLICH	FRIST	STATUS
1	Vertragsanhang Schweizer Datenschutzrecht mit beispielKI abgeschlossen	Leitung ICT	[Monat Jahr]	Erledigt
2	Nutzungsregeln im Merkblatt finalisieren (Verbotsliste, Anonymisierung)	Leitung ICT / ICTA	[Monat Jahr]	In Arbeit
3	Elterninformation zum KI-Einsatz erstellen und versenden	Rektorat / Leitung ICT	[Monat Jahr]	Offen
4	Vertragsanhang gegenzeichnen und Unterschriftsexemplar an beispielKI senden	Leitung ICT	[Monat Jahr]	Offen
5	KI-Führerschein für SuS konzipieren	ICTA / LP	[Monat Jahr]	Offen
6	Schulinterne Weiterbildung: Datenschutz-Block mit Fallbeispielen vorbereiten	Leitung ICT / Referent	[Monat Jahr]	In Planung
7	ISDS-Konzept erstellen (ergänzend zur DSFA)	Leitung ICT / [IT-Dienstleister]	[Monat Jahr]	Offen

06

Beurteilung Vorabkonsultation

§ 7b Abs. 3 DSG ZG

Kein hohes Restrisiko, keine Vorabkonsultation

Gemäss § 7b Abs. 3 DSG ZG ist eine Vorabkonsultation mit der Datenschutzstelle des Kantons Zug erforderlich, wenn die DSFA ergibt, dass die geplante Bearbeitung trotz der vorgesehenen Massnahmen ein hohes Restrisiko für die betroffenen Personen aufweist.

Die vorliegende Risikoanalyse zeigt, dass nach Umsetzung der technischen, organisatorischen und vertraglichen Massnahmen kein Risiko im Bereich «hoch» verbleibt. Die drei mit hohem Bruttoisiko bewerteten Sachverhalte (R1, R2, R6) - alle betreffend die Eingabe personenbezogener Daten in Prompts oder Uploads - werden durch eine Kombination aus technischen Vorkehrungen (Pseudonymisierung, Metadaten-Stripping, automatische Erkennung personenbezogener Eingaben), organisatorischen Massnahmen (Merkblatt, KI-Führerschein, Schulung an der schulinternen Weiterbildung) und vertraglichen Garantien auf ein mittleres Restrisiko reduziert. Das zuvor mittlere Restrisiko R7 (fehlendes Schweizer Recht im AVV) ist mit dem Abschluss des Vertragsanhangs auf gering gesenkt.

Der Vertragsanhang Schweizer Datenschutzrecht bindet die Auftragnehmerin ausdrücklich an das Schweizerische DSG, das DSG ZG und die VIP, regelt die Kooperationspflicht mit der Datenschutzstelle des Kantons Zug (Art. 11) und sichert die 72-Stunden-Meldepflicht bei Datenschutzverletzungen (Art. 9). Damit sind die spezifischen Anforderungen, die im Standard-AVV von beispielKI nicht abgebildet waren, vertraglich geschlossen.



Beurteilung: Die Voraussetzungen für eine Vorabkonsultation nach § 7b Abs. 3 DSG ZG sind nicht erfüllt. Die DSFA und der mit beispielKI abgeschlossene Vertragsanhang bilden zusammen einen tragfähigen Rahmen für den produktiven Einsatz ab Schuljahresbeginn. Die DSFA wird als lebendes Dokument geführt: Bei wesentlichen Änderungen (Ausweitung der Nutzergruppen, Änderungen in der Subprocessor-Kette, neue rechtliche Rahmenbedingungen oder einschlägige Datenschutzvorfälle) wird die Risikoanalyse aktualisiert und - falls erforderlich - die Datenschutzstelle des Kantons Zug einbezogen.

07

Überprüfung und Fortschreibung

Lebendes Dokument

Überprüfung spätestens ein Jahr nach Erstfassung

Die DSFA ist ein lebendes Dokument und wird bei wesentlichen Änderungen aktualisiert. Auslöser für eine Überprüfung sind insbesondere:

- Änderung der Unterauftragsbearbeiter-Kette durch beispielKI (neue LLM-Anbieter, geänderte Hosting-Standorte)
- Ausweitung des Einsatzes auf weitere Stufen oder Anwendungsfälle (z.B. SuS-Zugang ab Zyklus 1)
- Änderungen der kantonalen oder eidgenössischen Datenschutzgesetzgebung
- Erkenntnisse aus Datenschutzverletzungen oder Beinahe-Vorfällen
- Wesentliche technische Änderungen an der beispielKI-Plattform

Die nächste planmässige Überprüfung erfolgt spätestens ein Jahr nach Erstfassung oder bei Eintritt eines der genannten Auslöser.

Freigabe

§ 5a VIP

Unterschrift der zuständigen
Amtsleitung

Diese DSFA wird durch die Leitung ICT des Schulträgers erstellt und ist
gemäss § 5a VIP durch die zuständige Amtsleitung (oder gleichwertige
Funktion) zu unterzeichnen.

ERSTELLT DURCH

[Vorname Name], Leitung ICT

Datum / Unterschrift

FREIGEgeben DURCH

[Vorname Name], Rektorat

Datum / Unterschrift