wegfunke

SCHULE & BERUFSORIENTIERUNG

Vertrag zur Auftragsverarbeitung

Wegfunke · Schul-Pilot

ENTWURF

Zur Vorbereitung des Schul-Piloten

Vor Verwendung schulisch und juristisch prüfen lassen.

Answer 42

Die Antwort auf alles, naja fast.°

DIE MAPPE

Inhalt & Orientierung

01	§ 1 Gegenstand und Dauer	4
02	§ 2 Art und Zweck der Verarbeitung	4
03	§ 3 Weisungen	4
04	§ 4 Kategorien betroffener Personen	5
05	§ 5 Kategorien personenbezogener Daten	5
06	§ 6 Pflichten des Auftragsverarbeiters	6
07	§ 7 Vertraulichkeit	7
08	§ 8 Unterauftragsverarbeiter	7
09	§ 9 Betroffenenrechte	8
10	§ 10 Meldung von Verletzungen des Schutzes personenbezogener Daten	9
11	§ 11 Kontrollrechte	9
12	§ 12 Löschung und Rückgabe nach Vertragsende	9
13	§ 13 Haftung	10
14	§ 14 Schlussbestimmungen	10
15	Anlage TOM — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)	12

> ENTWURF – nicht zur Verteilung freigegeben; vor Vertragsschluss juristisch prüfen. Vertragspartner: Answer 42, Einzelunternehmen von Dr. Pascal Dehl, in Gründung.

> **Entwurf, Stand 06.10.2026 — vor Verwendung juristisch prüfen lassen.** Vertragspartner seit 06.10.2026: Answer 42 (Einzelunternehmen Dr. Pascal Dehl); in Gründung, vor Vertragsschluss. Die Anschrift ist vorläufig.

Vertrag über Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO

Pilotprojekt „Wegfunke – Berufs- und Studienorientierung", Klasse 9, Schuljahr 2026/27

zwischen

[Name der Schule], [Anschrift]
vertreten durch die Schulleitung [Name], im Einvernehmen mit dem Schulträger [Name des Schulträgers]
— nachfolgend „Verantwortliche" —

und

Answer 42, Inhaber Dr. Pascal Dehl (Einzelunternehmen)
Schloßgarten 5, 22041 Hamburg *(vorläufige Geschäftsanschrift)*
— nachfolgend „Auftragsverarbeiter" —

KAPITEL 01

§ 1 Gegenstand und Dauer

(1) Gegenstand des Vertrags ist die Bereitstellung und der Betrieb der Lernumgebung „Wegfunke" (Web-App mit Lehrkraft-Cockpit, sechs Unterrichtseinheiten und Berufs-Coach) für den Pilotbetrieb an der Schule durch den Auftragsverarbeiter.

(2) Die Leistung wird für die Schule unentgeltlich erbracht. Die Kosten des Betriebs, einschließlich der Kosten des KI-Dienstes, trägt der Auftragsverarbeiter.

(3) Der Vertrag beginnt mit Unterzeichnung und endet, wenn die Löschung nach § 12 abgeschlossen und schriftlich bestätigt ist. Geplanter Pilotzeitraum: [Startdatum] bis [Enddatum] (6 Einheiten à 90 Minuten, Begleitung über 7 Wochen).

KAPITEL 02

§ 2 Art und Zweck der Verarbeitung

(1) Zweck ist die Durchführung der Unterrichtseinheit „Berufs- und Studienorientierung" (Rahmenlehrplan Berlin-Brandenburg, Jg. 7–10) mit der Lernumgebung „Wegfunke" im Pilotbetrieb.

(2) Art der Verarbeitung: Erheben, Speichern, Anzeigen, Übermitteln an den Unterauftragsverarbeiter nach § 8 (nur Coach-Fragen, gefiltert), Sichern und Löschen.

(3) Der Berufs-Coach beantwortet Fragen der Schüler:innen zu Beruf, Studium und Zukunft. Grundlage ist ein geprüftes Wissensmodul sowie die öffentliche Jobsuche der Bundesagentur für Arbeit. An die Bundesagentur gehen nur Berufsbezeichnung und Ort, keine Pseudonyme, Antworten oder Freitexte.

(4) Optional, nur bei gesonderter Weisung nach § 3 Abs. 4 („Modul Begleitstudie"): Speicherung der gefilterten Coach-Fragen und KI-Antworten unter dem Pseudonym für die pseudonymisierte Auswertung in der Begleitstudie. Ohne diese Weisung werden Coach-Gespräche nicht gespeichert.

(5) Es findet kein Profiling und keine automatisierte Entscheidung über Schüler:innen statt (Art. 22 DSGVO). KI-Ausgaben sind Lernangebote, keine Bewertungen oder Prognosen.

KAPITEL 03

§ 3 Weisungen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung der Verantwortlichen, auch hinsichtlich der Übermittlung in ein Drittland (Art. 28 Abs. 3 lit. a DSGVO). Dieser Vertrag und seine Anlagen sind die Erstweisung.

(2) Weisungsberechtigt auf Seiten der Schule: [Name, Funktion]. Weisungsempfänger beim Auftragsverarbeiter: Dr. Pascal Dehl; operative Umsetzung durch den technischen Betreiber (§ 8), kburna@gmail.com.

(3) Weisungen erfolgen in Textform. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er die Verantwortliche unverzüglich.

(4) Folgende Schaltungen erfolgen nur auf Weisung der Verantwortlichen und werden dokumentiert:

- KI-Coach für eine Klasse einschalten (Standard: aus). Abschalten kann die Lehrkraft jederzeit selbst.
- Modul Begleitstudie für ein Pseudonym einschalten — nur wenn (a) die Genehmigung der Senatsverwaltung für Bildung, Jugend und Familie vorliegt und (b) die gesonderte schriftliche Einwilligung von Erziehungsberechtigten und Schüler:in vorliegt.
- Pilotende einer Klasse festlegen (Grundlage der Löschfrist).

KAPITEL 04

§ 4 Kategorien betroffener Personen

- Schüler:innen der teilnehmenden Klasse(n) (Jahrgangsstufe 9, minderjährig)
- Lehrkräfte, die eine Klasse anlegen (nur die selbst gewählte Bezeichnung, siehe § 5 Nr. 1)

KAPITEL 05

§ 5 Kategorien personenbezogener Daten

Die Aufzählung folgt dem tatsächlichen Datenmodell der App (`pilot-app/src/db/schema.ts`).

1. Klasse (Tabelle `class_sessions`)

- Klassen-Code, Bezeichnung der Lehrkraft (frei gewählt, z. B. „[Lehrkraft]"), Bundesland, Schulform, Klasse (z. B. „9b")
- aktive Einheit, Status des KI-Coachs (an/aus), Pilotende, Vermerk über Studien-Export
- Lehrkraft-PIN nur als Hash (SHA-256), Erstellungszeitpunkt

2. Schüler:in (Tabelle `student_progress`)

- selbst gewähltes Pseudonym, Klassen-Code, Avatar-Stil, aktueller Lernschritt
- Antworten und Übungsergebnisse der sechs Einheiten (Feld `answers`):

- E1 Stärken und Interessen
- E2 recherchierte Berufe mit Bewertung, gewählter Beruf
- E3 Lebenslauf-Formular: Schule, Schulbesuch seit, angestrebter Abschluss, Fähigkeiten, Sprachen und Hobbys als freiwillige Übungsangaben. **Name, E-Mail, Telefon und Wohnort bleiben**

ausschließlich auf dem Gerät und werden vor der Serverspeicherung in App und Server herausgefiltert; im gespeicherten Anschreiben stehen Platzhalter. Live-Testbestand bereinigt; historische Testdatensicherungen rotieren bis 12.10.2026, Nachweis danach; keine Daten einer echten Klasse betroffen (Datenschutz-Protokoll Nr. 4/4a, App 1.3.3).
- E4 Anschreiben-Entwurf
- E5 Bewerbungsgespräch-Übung (Anzahl beantworteter Fragen, Selbsteinschätzung, Antwortverlauf)
- E6 gewählter Weg nach der Schule

- Sitzungsschlüssel nur als Hash (SHA-256)
- Vermerk Studien-Einwilligung (ja/nein, Standard nein), Woche eines KI-Bonus durch die Lehrkraft
- Zeitstempel

3. Rückmeldungen (Tabelle `student_feedback`)

- Klassen-Code, Einheit, Rückmelde-Symbol, optionaler Freitext-Kommentar (ohne Pseudonym gespeichert)

4. KI-Nutzungszähler (Tabelle `llm_nutzung`)

- interne Schüler-ID, Klassen-Code, Tag, Woche, Tokenzahlen, Kosten — **keine Inhalte**

5. Coach-Gespräche (Tabelle `chat_verlauf`) — nur Modul Begleitstudie

- Pseudonym, Klassen-Code, Frage (nach Personendaten-Filter), KI-Antwort, Zeitstempel

6. Ohne Speicherung in der Datenbank

- Coach-Fragen ohne Studien-Einwilligung: nur flüchtig verarbeitet (Wissensmodul, Filter, Sprachmodell), nicht gespeichert. Krisen-Eingaben werden nie gespeichert und nicht an das Sprachmodell übermittelt.
- IP-Adressen beim Abruf: technisch notwendig; im Arbeitsspeicher der App für Missbrauchsbremsen (Zeitfenster bis 1 Stunde). Aufbewahrung in Zugriffsprotokollen: siehe Anlage TOM, offener Punkt O-4.
- Auf dem Gerät der Schüler:in (Browser-Speicher): Sitzungsschlüssel, Antworten, Lernschritt. Auf diese Daten hat der Auftragsverarbeiter keinen Zugriff.

Nicht verarbeitet werden: Fotos, Noten, Zeugnisse. Besondere Kategorien nach Art. 9 DSGVO werden nicht erhoben. Schreibt eine Schüler:in solche Angaben von sich aus in den Coach, gelten § 2 Abs. 4 und die Krisen-Regel in der Anlage TOM.

KAPITEL 06

§ 6 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet die Daten ausschließlich in der Bundesrepublik Deutschland (Berlin), vorbehaltlich § 8 Abs. 3 (Zugangsweg).

(2) Er trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß **Anlage TOM** und passt sie dem Stand der Technik an. Wesentliche Änderungen teilt er der Verantwortlichen vorab mit.

(3) Er unterstützt die Verantwortliche bei der Datenschutz-Folgenabschätzung (Art. 35, 36 DSGVO) und stellt hierfür den Entwurf `DSFA-Entwurf.md` bereit.

(4) Er führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO (`VVT-Answer42.md`).

(5) Einen Datenschutzbeauftragten hat der Auftragsverarbeiter [benannt: Name, Kontakt / nicht benannt, da keine Benennungspflicht — prüfen].

KAPITEL 07

§ 7 Vertraulichkeit

(1) Der Auftragsverarbeiter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Zugriff auf die Daten haben ausschließlich Dr. Pascal Dehl und technischer Betreiber als technischer Betreiber (§ 8).

(2) Die Lehrkraft sieht im Cockpit nur eine Klassenübersicht ohne Inhalte der Schüler:innen. Auf Coach-Gespräche hat sie keinen Zugriff. Niemand liest Coach-Gespräche live mit.

(3) Die Pflicht zur Vertraulichkeit gilt über das Vertragsende hinaus.

KAPITEL 08

§ 8 Unterauftragsverarbeiter

(1) Die Verantwortliche stimmt dem Einsatz folgender Unterauftragsverarbeiter zu:

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Daten	Status
technischer Betreiber, Mainzer Straße 21a, 10247 Berlin	Technischer Betrieb: Web-App, Datenbank, Wissensmodul, Sicherungen, Administration	eigene Server in Berlin	alle Daten nach § 5	**Offen:** Vertrag nach Art. 28 Abs. 4 DSGVO zwischen Auftragsverarbeiter und technischem Betreiber ist vor Unterzeichnung dieses Vertrags abzuschließen.

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Daten	Status
IONOS SE, [Anschrift laut IONOS-AVV]	Sprachmodell (IONOS AI Model Hub, Modell Mistral Small)	Rechenzentrum Berlin (BSI C5)	Coach-Frage nach Personendaten-Filter, die letzten Gesprächswechsel, Auszüge aus dem Wissensmodul. Kein Pseudonym, kein Klassen-Code, keine IP-Adresse der Schüler:in (der Server ruft auf, nicht das Gerät).	**Offen:** AVV zwischen Auftragsverarbeiter und IONOS ist noch abzuschließen; die Angabe „keine Speicherung der Eingaben, kein Training" ist aus dem IONOS-Vertrag zu belegen. Bis dahin ist der KI-Dienst nicht angebunden (Testmodus ohne Sprachmodell).
Tailscale Inc., [Anschrift], USA	derzeitiger öffentlicher Zugangsweg zur App (Weiterleitung „Funnel") sowie privates Netz zwischen den Servern des technischen Betreibers	Server des Anbieters, Drittland USA	Verbindungsdaten (IP-Adresse) der Abrufe. Inhalte bleiben per TLS bzw. WireGuard Ende-zu-Ende verschlüsselt.	**Wird vor Pilotstart abgelöst oder hier mit Angemessenheitsgrundlage ausgewiesen:** [Art. 45 DSGVO i. V. m. EU-US Data Privacy Framework — Zertifizierung von Tailscale Inc. im Register dataprivacyframework.gov prüfen und Datum eintragen]

(2) Die Bundesagentur für Arbeit ist kein Unterauftragsverarbeiter: An sie gehen nur Berufsbezeichnung und Ort ohne Personenbezug.

(3) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf die Pflichten dieses Vertrags (Art. 28 Abs. 4 DSGVO). Den Einsatz weiterer oder den Austausch bestehender Unterauftragsverarbeiter teilt er der Verantwortlichen mindestens [14] Tage vorher in Textform mit; die Verantwortliche kann widersprechen. Im Fall des Widerspruchs kann die Verantwortliche den Vertrag kündigen.

KAPITEL 09

§ 9 Betroffenenrechte

(1) Der Auftragsverarbeiter unterstützt die Verantwortliche bei der Erfüllung der Rechte nach Art. 15 bis 21 DSGVO (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) sowie beim Widerruf einer Einwilligung (Art. 7 Abs. 3 DSGVO).

(2) Anfragen, die direkt beim Auftragsverarbeiter eingehen, leitet er unverzüglich an die Verantwortliche weiter.

(3) Bei Widerruf einer Einwilligung löscht der Auftragsverarbeiter die Daten des betreffenden Pseudonyms **binnen 3 Werktagen** nach Eingang der Weisung und bestätigt dies in Textform. Wird nur die Einwilligung in die Begleitstudie widerrufen, werden nur die Coach-Gespräche des Pseudonyms gelöscht und die Speicherung beendet.

(4) Da keine Klarnamen erhoben werden, erfolgt die Zuordnung über Klassen-Code und Pseudonym. Die Schule stellt die Zuordnung Kind ↔ Pseudonym fest; der Auftragsverarbeiter kennt sie nicht.

KAPITEL 10

§ 10 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter meldet der Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten und jeden begründeten Verdacht **innerhalb von 24 Stunden** nach Kenntnis an [Kontakt Schule, E-Mail, Telefon].

(2) Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO. Fehlende Angaben werden unverzüglich nachgereicht.

(3) Die Meldung an die Aufsichtsbehörde (Berliner Beauftragte für Datenschutz und Informationsfreiheit) innerhalb von 72 Stunden und die Benachrichtigung Betroffener (Art. 34 DSGVO) obliegen der Verantwortlichen. Der Auftragsverarbeiter unterstützt sie vollumfänglich.

KAPITEL 11

§ 11 Kontrollrechte

(1) Die Verantwortliche und die/der von ihr beauftragte Datenschutzbeauftragte können die Einhaltung dieses Vertrags nach Absprache prüfen, auch vor Ort in den Betriebsräumen des technischen Betreibers (Anlage TOM, Zutritt).

(2) Der Auftragsverarbeiter stellt alle für den Nachweis erforderlichen Informationen zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO), insbesondere Datenschutzkonzept, DSFA-Entwurf, Verzeichnis der Verarbeitungstätigkeiten, Löschprotokolle und Testprotokolle (Wiederherstellung, Lasttest).

KAPITEL 12

§ 12 Löschung und Rückgabe nach Vertragsende

(1) Spätestens **4 Wochen nach Pilotende** löscht der Auftragsverarbeiter alle Daten der Klasse(n) vollständig: Klasse, Pseudonyme, Fortschritt und Antworten, Rückmeldungen, KI-Nutzungszähler und — falls das Modul Begleitstudie eingeschaltet war — Coach-Gespräche.

(2) Ist das Modul Begleitstudie eingeschaltet, erfolgt vor der Löschung der vereinbarte pseudonymisierte Export. Die Löschung unterbleibt, solange der Export nicht dokumentiert ist; die Frist nach Abs. 1 bleibt davon unberührt, d. h. der Export ist rechtzeitig vorher durchzuführen. Der Export enthält keine Klassen-Codes, die eine Zuordnung zur Schule erlauben, sofern die Studie dies nicht ausdrücklich erfordert. Für die Verarbeitung des Exports gilt die gesondert festzulegende Rollenverteilung der Begleitstudie.

(3) Sicherungskopien werden 7 Tage aufbewahrt. Gelöschte Daten sind damit **spätestens 7 Tage nach der Löschung** auch aus den Sicherungen entfernt.

(4) Wünscht die Verantwortliche vor der Löschung eine Rückgabe (z. B. Klassenübersicht), teilt sie dies bis [Frist] in Textform mit.

(5) Der Auftragsverarbeiter bestätigt die Löschung nach Abs. 1 und Abs. 3 **schriftlich** gegenüber der Verantwortlichen.

KAPITEL 13

§ 13 Haftung

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Innenverhältnis gelten die gesetzlichen Vorschriften. [Weitere Haftungsregelungen nach juristischer Prüfung.]

KAPITEL 14

§ 14 Schlussbestimmungen

(1) Änderungen und Ergänzungen bedürfen der Textform.

(2) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt.

(3) Anlagen: Anlage TOM (unten); Datenschutzkonzept Version 1.1; Datenschutz-Folgenabschätzung (Entwurf).

[Ort], [Datum]

_____
Schulleitung [Name der Schule]

[Ort], [Datum]

_____
Answer 42, Dr. Pascal Dehl

KAPITEL 15

Anlage TOM – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Grundlage: Datenschutzkonzept Version 1.1, Abschnitt 10, abgeglichen mit dem Betriebsstand 05.10.2026. Was noch nicht umgesetzt ist, steht unter „Offene Punkte" und ist im Text als **offen** markiert.

Betrieb

- Web-App und Datenbank laufen auf einem eigenen Rechner des technischen Betreibers (§ 8) in Berlin. Die Datenbank ist eine eigene, von anderen Projekten getrennte Instanz nur für diesen Pilot und nur im privaten Netz erreichbar.
- Das Wissensmodul des Coachs läuft auf einem zweiten eigenen Server des technischen Betreibers in Berlin. Es erhält den Fragetext zur Suche im Wissensmodul, speichert und protokolliert ihn nicht.
- Verbindungen zwischen den Servern ausschließlich über ein verschlüsseltes privates Netz (WireGuard, derzeit über Tailscale).

Zutritt

Server in Wohn- bzw. Büroräumen des technischen Betreibers in Berlin, nicht öffentlich zugänglich.

Zugang

- Administration nur per SSH-Schlüssel über das private Netz.
- Zugangsdaten zum KI-Dienst nur auf dem Server, nie in der App; geplant: eigener IONOS-Benutzer nur für den KI-Dienst, Token mit 60 Tagen Laufzeit.
- Zugangsdaten der Datenbank nur in Konfigurationsdateien mit eingeschränkten Dateirechten (chmod 600), nicht im Quellcode-Archiv.

Zugriff

- Kein Konto, keine Registrierung, keine E-Mail-Adresse.
- Schüler:in: Zugang über Klassen-Code + Pseudonym. Jedes Pseudonym erhält einen eigenen Sitzungsschlüssel, der nur auf dem Gerät liegt; der Server speichert nur dessen Hash. Fremde Einträge sind ohne Schlüssel weder les- noch änderbar.
- Lehrkraft: Klassen-Code + Lehrkraft-PIN (Server speichert nur den Hash). Das Cockpit zeigt eine Klassenübersicht ohne Inhalte. Die Lehrkraft kann den KI-Coach abschalten und einmalig ein zusätzliches Kontingent geben, aber nicht einschalten.
- Administration: nur der technische Betreiber im Auftrag des Auftragsverarbeiters über einen geheimen Admin-Schlüssel.

- Höchstens 40 Pseudonyme je Klasse; Bremsen gegen massenhaftes Anlegen und Abfragen (u. a. je IP-Adresse 80 neue Pseudonyme / 10 Minuten, 10 neue Klassen / Stunde, 30 Fehlversuche / 10 Minuten).

Pseudonymisierung und Datensparsamkeit

- Für den Zugang wird kein Klarname abgefragt. Freiwillige Kontaktfelder im Lebenslauf bleiben nur auf dem Gerät; Serverfilter und Platzhalter im Anschreiben verhindern ihre Speicherung (Datenschutz-Protokoll Nr. 4/4a).
- Keine Cookies, keine Tracking- oder Analysedienste, keine Werbung, keine Schriftarten oder Skripte von Drittanbietern.
- An die Bundesagentur für Arbeit gehen nur Berufsbezeichnung und Ort.

KI-Coach

- Je Klasse standardmäßig **aus**; Einschalten nur durch den Auftragsverarbeiter auf Weisung, Abschalten jederzeit durch die Lehrkraft.
- Krisen-Erkennung vor allem anderen: Bei Hinweisen auf Suizid, Selbstverletzung, Mobbing, Gewalt oder Missbrauch antwortet keine KI, sondern ein fester Hinweis (Nummer gegen Kummer 116 111, Vertrauenslehrkraft, Notruf 112). Die Eingabe wird nicht gespeichert und nicht an das Sprachmodell übermittelt.
- Personendaten-Filter vor jeder Übermittlung an das Sprachmodell: E-Mail-Adressen, Links, @-Namen, Straße + Hausnummer, PLZ + Ort, Telefonnummern sowie Wendungen wie „ich heiße ...". Restrisiko: Namen im Fließtext erkennt der Filter nicht zuverlässig; die App weist darauf hin, keine Namen zu schreiben.
- Kein Pseudonym und kein Klassen-Code im Prompt.
- Kennzeichnung in der App: „Du schreibst hier mit einer KI. Sie kann Fehler machen ..." (Art. 50 KI-Verordnung).
- Berufe, Stellen und Quellen werden nicht von der KI erzeugt, sondern aus dem geprüften Wissensmodul angezeigt.
- Eingaben höchstens 500 Zeichen.

Kostenschutz KI (Schutz vor Missbrauch)

- Kontingent 30 Nachrichten je Kind und Woche; danach antwortet der Coach ohne KI aus dem geprüften Wissen.
- Kosten werden vor jedem Aufruf reserviert; feste Obergrenzen je Klasse und gesamt; ohne erreichbare Datenbank kein KI-Aufruf.
- Zweiter, unabhängiger Tageszähler im Programm.
- Automatischer Not-Aus bei ungewöhnlicher Nutzung (u. a. mehr als 30 Aufrufe einer Klasse in 5 Minuten); Wiedereinschalten nur von Hand. Die Alarmmeldung enthält keine personenbezogenen

Daten.

Verschlüsselung

- TLS bei der Übertragung zwischen Gerät und App.
- Verbindungen zwischen Servern im verschlüsselten privaten Netz.
- **Erledigt (O-2):** Datenbank und lokale Sicherungen liegen im LUKS2-Container; externe Sicherungen sind mit age verschlüsselt. Umsetzung und Prüfung: Datenschutz-Protokoll Nr. 7.

Trennung

Eigene Datenbank-Instanz nur für den Pilot; Daten je Klassen-Code logisch getrennt.

Verfügbarkeit und Belastbarkeit

- Nächtliches Backup (02:30 Uhr) auf den zweiten Server in Berlin, 7 Tage Aufbewahrung. Wiederherstellung am 05.10.2026 erfolgreich getestet.
- Lasttest mit 35 gleichzeitigen Nutzer:innen am 05.10.2026 bestanden (0 Fehler).
- Fällt das Wissensmodul aus, antwortet der Coach über eine einfache Stichwortsuche weiter; fällt der KI-Dienst aus, antwortet er ohne KI.
- Kein zweiter Rechner als Ausfallreserve; ein Ausfall des Rechners unterbricht die App bis zur Wiederherstellung.

Löschung

- Täglicher automatischer Prüflauf (03:00 Uhr) meldet Klassen, deren Löschfrist erreicht ist. Die Löschung selbst führt der Auftragsverarbeiter nach dem Studien-Export (falls vereinbart) aus und protokolliert sie.
- **Widerruf je Pseudonym:** Funktion „Daten löschen“ für die Lehrkraft im Cockpit (mit PIN) und für den Auftragsverarbeiter per Admin-Zugang; löscht Fortschritt und gespeicherte Gespräche, KI-Kostenzähler bleiben ohne Personenbezug; Antwort mit Zeitstempel als Löschnachweis (seit App 1.3.4).

Überprüfung

Vor Pilotstart und bei Änderungen des Verfahrens Information an Schule und schulische:n Datenschutzbeauftragte:n.

Offene Punkte (vor Unterzeichnung zu klären)

Nr.	Punkt
O-1	**Live behoben; Backup-Nachweis nach 12.10.2026 offen:** Name, E-Mail, Telefon und Wohnort bleiben im Lebenslauf nur auf dem Gerät; Filter in App und Server, Platzhalter im gespeicherten Anschreiben, Live-Testbestand bereinigt; historische Testdatensicherungen rotieren bis 12.10.2026, Nachweis danach; keine Daten einer echten Klasse betroffen. Nachweis: Datenschutz-Protokoll Nr. 4/4a, App 1.3.3.
O-2	Erledigt: LUKS2-Container für Datenbank und age für Sicherungen; siehe Datenschutz-Protokoll Nr. 7. Nachweise vor Abnahme prüfen.
O-3	Öffentlicher Zugang ohne Tailscale-Weiterleitung (eigene Domain, Eingang bei einem Anbieter im EWR) oder Tailscale mit Angemessenheitsgrundlage in § 8 ausweisen. Auch das private Netz zwischen den Servern läuft derzeit über Tailscale.
O-4	Aufbewahrung von Zugriffsprotokollen mit IP-Adressen (Webserver, Weiterleitung) prüfen und festlegen (Vorschlag Konzept: höchstens 7 Tage).
O-5	~~Löschfunktion für einzelne Pseudonyme~~ — erledigt (App 1.3.4).
O-6	AVV mit IONOS abschließen; „keine Speicherung, kein Training" aus dem Vertrag belegen; KI-Dienst erst danach anbinden.
O-8	Vertrag nach Art. 28 Abs. 4 DSGVO zwischen Answer 42 (Dr. Pascal Dehl) und dem technischen Betreiber technischer Betreiber abschließen; Gewerbeanmeldung von Answer 42 vor Unterzeichnung; endgültige Geschäftsanschrift eintragen.
O-7	Rollen und Rechtsgrundlage der Begleitstudie mit der/dem schulischen DSB klären; Genehmigung der Senatsverwaltung einholen.