Anhang III – Technische und organisatorische Maßnahmen

Version 2026-09. Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO für die Software „Zeugnisprogramm“, einschließlich der Maßnahmen zur Unterstützung des Verantwortlichen (Klausel 8 Buchstabe d und Klausel 9.2). Die Beschreibung folgt dem tatsächlichen Stand von Software und Betrieb; Angaben zum Rechenzentrumsbetreiber beruhen auf dessen veröffentlichten Nachweisen.

1. Betriebsumgebung

- Betrieb ausschließlich auf Microsoft Azure in der Region Microsoft Azure, Region „Germany West Central“ (Frankfurt am Main). Eine Verarbeitung außerhalb der EU findet nicht statt; Microsoft sichert dies über die „EU Data Boundary“ zu (Anhang IV).
- Komponenten: Azure App Service (Anwendung: Webserver, Anwendungsserver, Hintergrundverarbeitung), Azure Database for PostgreSQL (Datenbank), Azure Files (Zeugnisvorlagen). Es werden keine weiteren Cloud-Dienste für personenbezogene Daten genutzt.
- Getrennte Umgebungen für Entwicklung/Test und Produktion. In der Entwicklungsumgebung werden ausschließlich Testdaten und keine Produktivdaten von Schulen verwendet.

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b)

2.1 Zutrittskontrolle

Die Rechenzentren werden von Microsoft betrieben. Physische Sicherheit (Zutrittskontrolle mit mehrstufiger Authentisierung, Videoüberwachung, Sicherheitspersonal, Besucherprotokollierung) ist durch die Zertifizierungen ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1/2/3 und den BSI C5-Testat nachgewiesen; Nachweise sind über das Microsoft Service Trust Portal abrufbar. Der Auftragsverarbeiter selbst betreibt keine eigenen Serverräume; an seinem Firmensitz werden keine personenbezogenen Daten des Verantwortlichen dauerhaft gespeichert.

2.2 Zugangskontrolle (Systemzugang)

- Anmeldung der Nutzer nur mit persönlichem Benutzerkonto (E-Mail-Adresse) und Passwort.
- Passwortregeln: mindestens 8 Zeichen, mindestens eine Ziffer und ein Sonderzeichen, keine Ähnlichkeit zu Name/E-Mail, Abgleich gegen eine Liste häufiger Passwörter, keine rein numerischen Passwörter. Passwörter werden ausschließlich als Hash (PBKDF2-SHA256, Django-Standard) gespeichert.
- Zwei-Faktor-Authentisierung (TOTP nach RFC 6238 mit Authenticator-App, dazu zehn Einmal-Wiederherstellungscodes). Der Verantwortliche kann die 2FA je Schule für alle Nutzer oder für Nutzer mit Verwaltungsrechten verpflichtend machen (Übergangsfrist wählbar bis 30 Tage). Die 2FA-Geheimnisse werden mandantengetrennt gespeichert.

- Schutz vor Brute-Force-Angriffen: Drosselung der Anmeldeversuche je IP-Adresse (20 pro Minute), Drosselung von Passwort-Zurücksetzen (10 pro Stunde); Kontosperre für 15 Minuten nach 10 Fehlversuchen innerhalb von 15 Minuten. Fehlermeldungen lassen nicht erkennen, ob ein Konto existiert.
- Sitzungssteuerung: automatische Abmeldung nach 60 Minuten Inaktivität und spätestens 12 Stunden nach Anmeldung (Plattform-Obergrenzen); der Verantwortliche kann je Schule kürzere Werte einstellen (15 bis 60 Minuten bzw. 4 bis 12 Stunden), nie längere. Bei Ablauf wird die Anzeige personenbezogener Daten im Browser verdeckt. Passwortänderungen beenden alle anderen Sitzungen des Kontos.
- Sitzungs-Cookies mit den Attributen Secure, HttpOnly und SameSite=Lax; Schutz gegen Cross-Site-Request-Forgery durch CSRF-Token.
- Einladung neuer Nutzer und Passwort-Zurücksetzen ausschließlich über personalisierte, 7 Tage gültige Einmal-Links; Passwörter werden nie per E-Mail versendet.
- Administrativer Zugang des Auftragsverarbeiters: personengebundene Konten mit Zwei-Faktor-Authentisierung für Azure-Portal und Quellcodeverwaltung; Zugriff auf Produktionssysteme (Azure-Portal, Datenbank, Quellcodeverwaltung) hat ausschließlich der Geschäftsführer Vianney Lancres; Azure-Portal und GitLab sind mit Zwei-Faktor-Authentisierung gesichert.

2.3 Zugriffskontrolle (Berechtigungen innerhalb der Software)

- Rollenmodell je Schule: „Lehrkraft“ (Standard), „Verwaltung“ (erweiterte Rechte, vom Verantwortlichen vergeben), zusätzlich je Lehrkraft eine Klassenleitungs-Zugriffsstufe (kein Zugriff / lesend / schreibend auf Beurteilungen der eigenen Klasse durch andere Fächer).
- Lehrkräfte sehen ausschließlich Schülerinnen und Schüler der Kurse und Klassen, denen sie zugeordnet sind, und können nur dort Beurteilungen erfassen. Stammdatenpflege, Import/Export, Zeugniserzeugung und Schuljahreswechsel sind Nutzern mit Verwaltungsrechten vorbehalten.
- Jede Berechtigungsänderung (Verwaltungsrolle, Klassenleitungs-Zugriff, 2FA-Zurücksetzen durch Verwaltung) wird protokolliert (Ziffer 5).
- Plattformadministration durch den Auftragsverarbeiter über gesonderte Administratorkonten, ausschließlich für Einrichtung, Support und Störungsbeseitigung.

2.4 Trennungskontrolle (Mandantentrennung)

- Jede Schule erhält ein eigenes Datenbankschema in der PostgreSQL-Datenbank (schema-basierte Mandantentrennung mit django-tenants). Benutzerkonten, Sitzungen, 2FA-Geheimnisse, Fachdaten und Protokolle liegen vollständig im Schema der jeweiligen Schule.
- Die Zuordnung eines Aufrufs zum Schema erfolgt serverseitig über den Hostnamen der schulindividuellen Subdomain; Datenbankabfragen werden auf das aktive Schema beschränkt. Ein schemaübergreifender Zugriff ist in der Anwendung nicht vorgesehen. Hintergrundaufgaben (z. B. Zeugniserzeugung) laufen ebenfalls schemagebunden.
- Erzeugte Zeugnisdateien werden in schulindividuellen, zugriffsbeschränkten Verzeichnissen (Rechte 0700) abgelegt.
- Demo-/Testumgebung für Interessenten in einem gesonderten Schema mit fiktiven Daten, ohne Verbindung zu Schuldaten.

2.5 Pseudonymisierung und Datensparsamkeit

- Es werden nur die für Zeugnisse erforderlichen Datenfelder vorgehalten (Anhang II); keine Adress-, Eltern-, Gesundheits- oder Herkunftsdaten.
- IP-Adressen im Anmeldeprotokoll werden gekürzt gespeichert (IPv4: letztes Oktett entfernt; IPv6: auf /48 gekürzt); keine Speicherung von Browserkennungen.
- Importdaten werden nach Abschluss des Imports aus der Auftragsverwaltung entfernt; die hochgeladene Datei wird nicht gespeichert.
- Eine Pseudonymisierung der Schülernamen ist wegen des Zwecks (Zeugnisdokument) nicht möglich; für Lehrkräfte können vom Verantwortlichen funktionale E-Mail-Adressen verwendet werden.

2.6 Verschlüsselung

- Transport: ausschließlich HTTPS mit TLS 1.2 oder höher (mindestens TLS 1.2 auf App Service und Datenbank erzwungen); HTTP wird auf HTTPS umgeleitet; HSTS mit einjähriger Gültigkeit inklusive Subdomains und Preload. Verbindung Anwendung–Datenbank ebenfalls TLS-verschlüsselt. E-Mail-Versand über TLS (STARTTLS) an den Mailserver.
- Ruhende Daten: Datenbank, Datensicherungen und Dateispeicher sind auf Azure-Seite mit AES-256 verschlüsselt (Storage Service Encryption, von Microsoft verwaltete Schlüssel).
- Passwörter als Salted Hash (Ziffer 2.2).

3. Integrität (Art. 32 Abs. 1 lit. b)

3.1 Weitergabekontrolle

- Datenübertragung nur über TLS (Ziffer 2.6). Keine Übermittlung an Dritte außer an die Unterauftragsverarbeiter nach Anhang IV.
- Datenexporte (Zeugnis-PDF, Excel) nur durch Nutzer mit Verwaltungsrechten; Exportdateien nur nach Anmeldung abrufbar; Excel-Exporte mit Schutz gegen Formel-Injektion.
- E-Mails des Systems enthalten keine Beurteilungs- oder Schülerdaten, sondern nur Namen der Empfänger, Klassenbezeichnungen und Links.
- Support erfolgt ausschließlich durch Mitarbeitende des Auftragsverarbeiters; keine Fernwartungssoftware auf Endgeräten des Verantwortlichen.

3.2 Eingabekontrolle

- Anmeldeprotokoll je Schule: Anmeldung, fehlgeschlagene Anmeldung, Abmeldung, Sitzungsablauf, Passwortänderung, 2FA-Änderungen, Kontosperre und Berechtigungsänderungen, jeweils mit Zeitstempel, Konto und gekürzter IP-Adresse; Aufbewahrung 90 Tage; Nutzer können ihre eigene Anmeldehistorie einsehen.
- Beurteilungen speichern den zuletzt ändernden Nutzer; Änderungen an Stammdaten über die Verwaltungsoberfläche werden mit Nutzer und Zeitpunkt protokolliert.
- Sicherheitshinweis per E-Mail an den Nutzer bei Passwort- und 2FA-Änderungen.

- Versionierte Quellcodeverwaltung mit Änderungshistorie; Auslieferung nur über die automatisierte Build-Pipeline (Build einmal, Ausrollen auf Test, dann Produktion).

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c)

- Datensicherung: automatische, stündliche Sicherungen der PostgreSQL-Datenbank durch Azure mit Point-in-Time-Wiederherstellung; Aufbewahrung 35 Tage. Sicherungen der Anwendungsumgebung (App Service) mit Aufbewahrung 30 Tage. Sicherungen sind verschlüsselt (Ziffer 2.6) und werden innerhalb der Region Frankfurt am Main vorgehalten (keine Georedundanz, keine Speicherung außerhalb Deutschlands).
- Wiederherstellbarkeit: Wiederherstellung eines Datenbankstands ist über das Azure-Portal jederzeit möglich; Ein Wiederherstellungstest (Rücksicherung eines Sicherungsstands auf einen Testserver und Prüfung auf Vollständigkeit) wird jährlich durchgeführt und dokumentiert.
- Infrastruktur: Rechenzentren mit redundanter Strom- und Netzanbindung, Klimatisierung, Brandschutz und unterbrechungsfreier Stromversorgung (Nachweis über Zertifizierungen, Ziffer 2.1).
- Betriebsüberwachung: Überwachung der Verfügbarkeit und Fehler über Azure-Bordmittel und Anwendungsprotokolle; Rate-Limiting gegen Überlastung durch einzelne Quellen.
- Zeugniserzeugung als Hintergrundaufgabe mit Statusverfolgung; hängende Aufgaben werden automatisch als fehlgeschlagen markiert und können erneut angestoßen werden.
- Aktualisierungen: regelmäßige Sicherheitsaktualisierungen von Betriebssystem-Images, Laufzeitumgebung und Bibliotheken über die Build-Pipeline; Wartungsfenster vorzugsweise zwischen 20 und 8 Uhr.

5. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d)

- Jährliche Überprüfung dieses Anhangs und der Subunternehmerliste anhand des tatsächlichen Softwarestands; Änderungen werden versioniert und dem Verantwortlichen mitgeteilt (Ergänzende Vereinbarung E.5).
- Sicherheitsprüfung des Quellcodes bei wesentlichen Änderungen (Code Review nach Checkliste: Eingabevalidierung, Berechtigungsprüfung, Pfadvalidierung, Fehlerbehandlung, Protokollierung ohne Inhaltsdaten); letzte umfassende Sicherheitsüberprüfung Juli/August 2026 mit dokumentierter Nachverfolgung der Befunde.
- Automatisierte Tests (u. a. für Berechtigungen und Mandantentrennung) laufen bei jeder Auslieferung in der Build-Pipeline.
- Auftragskontrolle: Mit den Unterauftragsverarbeitern bestehen Verträge zur Auftragsverarbeitung (Anhang IV); ihre Zertifizierungen werden jährlich geprüft.
- Vertraulichkeitsverpflichtung aller Personen, die Zugang zu Daten des Verantwortlichen haben, nach Art. 28 Abs. 3 lit. b und Art. 32 Abs. 4 DSGVO; Derzeit hat ausschließlich der Geschäftsführer Zugriff auf Daten des Verantwortlichen; er unterliegt der Verschwiegenheitspflicht aus diesem Vertrag. Weitere Personen erhalten Zugriff erst nach schriftlicher Verpflichtung auf Vertraulichkeit und Datengeheimnis.

6. Löschung und Datenlebenszyklus

- Löschung einzelner Datensätze (Schüler, Lehrkräfte, Kurse) durch Nutzer mit Verwaltungsrechten jederzeit; physische Löschung einschließlich verknüpfter Beurteilungen.
- Assistent für den Schuljahreswechsel: Leeren der Beurteilungen, Versetzung, Entfernen ausgeschiedener Schülerinnen und Schüler.
- Automatische Löschung: Zeugnis-PDFs spätestens 3 Stunden nach Erzeugung (Bereitstellung 2 Stunden, stündlicher Löschlauf); Anmeldeprotokoll nach 90 Tagen; Importdaten sofort nach Abschluss des Imports.
- Mandantenlöschung bei Vertragsende: Löschung des gesamten Schemas und der Dateiverzeichnisse innerhalb von 30 Tagen nach Wahl des Verantwortlichen, schriftliche Bestätigung; Datensicherungen werden nach Ablauf der Aufbewahrung (Ziffer 4) automatisch überschrieben.
- Datenträger werden vom Rechenzentrumsbetreiber nach NIST SP 800-88 gelöscht bzw. vernichtet (Nachweis über Microsoft-Dokumentation). Beim Auftragsverarbeiter werden keine Datenträger mit Daten des Verantwortlichen geführt.

7. Unterstützung des Verantwortlichen (Klausel 8 Buchstabe d)

- Betroffenenrechte: Auskunft, Berichtigung und Löschung kann der Verantwortliche über die Verwaltungsoberfläche selbst ausführen (Datensatzansicht, Bearbeitung, Löschung, Excel-Export je Datentyp). Auf Anfrage stellt der Auftragsverarbeiter innerhalb von 10 Werktagen einen Gesamtexport der Daten einer betroffenen Person bereit.
- Datenschutz-Folgenabschätzung: Der Auftragsverarbeiter stellt dieses Dokument, Anhang II und auf Anfrage eine Beschreibung der Systemarchitektur als Grundlage zur Verfügung und beantwortet Rückfragen innerhalb von 10 Werktagen.
- Informationspflichten: Die Angaben in Anhang II (Zwecke, Datenkategorien, Empfänger, Speicherdauer) und Anhang IV (Unterauftragsverarbeiter) sind so gefasst, dass der Verantwortliche sie unmittelbar in seine Informationen nach Art. 13 DSGVO übernehmen kann; Rückfragen dazu beantwortet der Auftragsverarbeiter innerhalb von 10 Werktagen.
- Richtigkeit: Unrichtige Daten, die dem Auftragsverarbeiter bei Support oder Störungsbeseitigung auffallen, werden dem Verantwortlichen mitgeteilt.

8. Meldung von Verletzungen (Klausel 9.2 – weitere Angaben)

- Meldung an die Kontaktstelle des Verantwortlichen per E-Mail und, bei hohem Risiko, zusätzlich telefonisch, spätestens 24 Stunden nach Kenntnis.
- Inhalt zusätzlich zu Klausel 9.2: Zeitpunkt und Zeitraum des Vorfalls, betroffene Systeme und Schemata, ob Daten verschlüsselt waren, ob Unterauftragsverarbeiter betroffen sind, Ansprechpartner für Rückfragen, geplante Folgemeldungen.
- Der Auftragsverarbeiter dokumentiert alle Sicherheitsvorfälle einschließlich Ursache, Auswirkung und Abhilfemaßnahmen.

9. Rückgabe und Löschung bei Vertragsende (Klausel 10 Buchstabe d)

- Rückgabeformat: Excel-Dateien je Datentyp (Schüler, Lehrkräfte, Kurse, Textbausteine) über die Exportfunktion sowie auf Anfrage ein vollständiger Datenbankexport des Schemas (SQL-Dump) und die Zeugnisvorlagen.
- Löschung: Schema, Dateiverzeichnisse und Benutzerkonten innerhalb von 30 Tagen; Bestätigung in Textform mit Datum; Sicherungen laufen nach spätestens 35 Tagen aus.

Anhang IV – Liste der Unterauftragsverarbeiter

Version 2026-09. Der Verantwortliche hat die Beauftragung der folgenden Unterauftragsverarbeiter genehmigt (Klausel 7.7 Buchstabe a). Die Dauer der Unterauftragsverarbeitung entspricht der Dauer des Hauptvertrags. Die jeweils aktuelle Liste ist unter www.zeitfuerschule.de/datenschutz/avv abrufbar.

Unterauftragsverarbeiter	Anschrift	Gegenstand und Art der Verarbeitung	Ort der Verarbeitung	Vertrag und Garantien nac Kapitel V DSGVO
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Cloud-Infrastruktur (Microsoft Azure): App Service, Azure Database for PostgreSQL, Azure Files, Datensicherung	Rechenzentrumsregion Microsoft Azure, Region „Germany West Central“ (Frankfurt am Main); Speicherung und Verarbeitung von Kundendaten innerhalb der EU („EU Data Boundary“)	Vertragspartner ist die irisch Microsoft-Gesellschaft. Auftragsverarbeitungsvertra „Datenschutznachtrag für Produkte und Services von Microsoft“ (DPA, Stand 22. Mai 2026), Bestandteil der Azure-Nutzungsbedingungen; er enthält die Standardvertragsklauseln d Kommission von 2021 (Auftragsverarbeiter-zu-Auftragsverarbeiter) für etwaigen Zugriff durch Microsoft Corporation (USA Microsoft ist zudem unter dem EU-US Data Privacy Framework zertifiziert. Speicherung und Verarbeitung der Kundendaten innerhalb der EU nach Microsofts „EU Da Boundary“-Zusage für Azur Zertifizierungen: ISO/IEC 27001, 27017, 27018, SOC 2, BSI C5. DPA liegt dem Auftragsverarbeiter vor und wird auf Anfrage bereitgestellt.

Unterauftragsverarbeiter	Anschrift	Gegenstand und Art der Verarbeitung	Ort der Verarbeitung	Vertrag und Garantien nac Kapitel V DSGVO
STRATO GmbH	Otto-Ostrowski-Straße 7, 10249 Berlin, Deutschland	Versand von System-E-Mails (SMTP-Relay über das E-Mail-Postfach des Auftragsverarbeiters)	Deutschland	Anbieter mit Sitz in Deutschland (IONOS-Gruppe). Vereinbarung zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO mit STRATO (Version 3.6, abgeschlossen am 24.09.2026). Für den E-Mai Dienst setzt STRATO laut seiner Subunternehmerliste Dienstleister in Deutschland ein (IONOS SE, Montabaur Betrieb der Plattform; Eleve GmbH, Berlin: Spamfilter); die dort für andere STRATO Produkte genannten Drittlanddienstleister (Mail-Archivierung, Malware-Scan für Webhosting) werden von Auftragsverarbeiter nicht genutzt. E-Mails enthalten Empfängername, E-Mail-Adresse und Links, keine Schülerdaten.

Keine Unterauftragsverarbeitung liegt vor bei: GitLab (Quellcodeverwaltung und Build-Pipeline; verarbeitet keine personenbezogenen Daten des Verantwortlichen), Microsoft Corporation als Konzernmutter (kein eigener Vertragspartner; siehe Garantien oben).

Änderungshistorie

Version	Änderung
2026-09	Fehlermonitoring-Dienst Sentry (Functional Software, Inc., USA) und externe Schriften-/ Icon-Bereitstellung (rsms.me, fontawesome.com) aus der Anwendung entfernt; Schriften werden selbst gehostet. STRATO als E-Mail-Dienstleister ergänzt. Microsoft-Angaben um DPA, Region und Garantien konkretisiert.
2025-02 (Altfassung)	Microsoft Ireland Operations Limited (Azure), Standorte Frankfurt, Berlin