

Systembeschreibung „AZAV 360“

Funktionsumfang, Betrieb/Hosting, Datenschutz und Informationssicherheit — Dokumentation der Software-Ausstattung für AZAV-Bildungsträger (§ 8 des Software-Nutzungsvertrags)

Hinweis: Die betrieblichen Angaben zu Objektspeicher-Region (C.2 — identisch in AVV Anlage 3 nachzutragen), Sicherungsaufbewahrung, RTO und letztem Wiederherstellungstest (C.4) sowie zum Data-Privacy-Framework-Status (D.6) werden nach Verifikation im Betrieb nachgetragen; der jeweilige Stand ergibt sich aus der Änderungshistorie (A.1).

A. Identifikation und Governance

A.1 Produkt, Versionsstand und Änderungshistorie dieser Beschreibung

Produktname: „**AZAV 360**“ — webbasierte Verwaltungs- und Audit-Software für nach AZAV zugelassene Bildungsträger (Software-as-a-Service, Mehr-Mandanten-Betrieb mit strikter Mandantentrennung). Die Software wird als **kontinuierliche Auslieferung** betrieben (Rolling Release ohne kundenseitige Versionswahl); alle Kunden nutzen stets denselben, aktuellen Stand. Maßgeblich für den beschriebenen Funktionsumfang ist der Stand dieser Beschreibung.

Version	Datum	Änderung
1.0	03.06.2026	Erstfassung. Funktionsstand Juni 2026 (u. a. Klassenbuch mit Monatskalender und Dozentenplan, Erfolgsmessung pro Maßnahme/Gutschein).

Pflege: Diese Beschreibung wird von der Geschäftsführung des Anbieters gepflegt und bei wesentlichen Änderungen an Funktionsumfang, Architektur oder Unterauftragsverarbeitern aktualisiert, mindestens jedoch einmal jährlich überprüft. Die jeweils aktuelle Fassung wird dem Kunden auf Anforderung bereitgestellt (§ 8 des Software-Nutzungsvertrags), sodass der Träger seine Mitteilungspflichten gegenüber der fachkundigen Stelle erfüllen kann.

A.2 Anbieter

Valtrion Operations UG (haftungsbeschränkt), vertreten durch den Geschäftsführer Justin-Pascal Schlimnat.

Rheinpromenade 13, 40789 Monheim am Rhein, Deutschland

Handelsregister: Amtsgericht Düsseldorf, HRB 110242 · USt-IdNr. DE461314806

A.3 Ansprechpartner

Bereich	Kontakt
Technik & Betrieb	Justin-Pascal Schlimnat (Geschäftsführer) · info@valtrion.de · Telefon auf Anfrage
Support (§ 5 des Vertrags)	info@valtrion.de — Antwort an Werktagen i. d. R. innerhalb von zwei Werktagen
Datenschutz	Justin-Pascal Schlimnat (Geschäftsführer) · info@valtrion.de

B. Funktionsumfang

B.1 Produktive Module

Der produktive Funktionsumfang ist deckungsgleich mit Anlage 1 des Software-Nutzungsvertrags (Leistungsbeschreibung). Kernfunktionen im Sinne von § 1 Abs. 3 des Vertrags sind die Nummern 1–6:

- **1. Maßnahmen- und Durchführungsverwaltung** — zugelassene Maßnahmen (QCG/FbW, AVGS, Gründungsberatung) mit Durchführungen, Plätzen und Belegungssteuerung (Überbuchungsschutz).
- **2. Teilnehmerverwaltung** — vollständige Teilnehmerakte mit Stammdaten, Verlauf, Förderungen/Bildungsgutscheinen (Bewilligungs- und Auszahlungsstatus je Gutschein), Dokumenten, Audit-Reife-Prüfung und Aktenexport (PDF/ZIP).
- **3. Anwesenheits- und Unterrichtsdokumentation (Klassenbuch)** — Tageseinträge je Termin mit Datum, Uhrzeit, UE-Anzahl, Inhalt, Dozent und Anwesenheit pro Teilnehmer (inkl. Teil-Fehlzeiten, Fehlzeitart und AU-Nachweisablage); zentrale Klassenbuch-Übersicht als Monatskalender und Liste über vergangene und geplante Unterrichtseinheiten mit Filter nach Dozent, Durchführung und Teilnehmer (Dozentenplan); Teilnehmer-Bestätigungslinks (Einmal-Token, Nachweis mit IP/Zeitstempel/User-Agent); Alt-Nachträge aus der früheren Pauschal-Erfassung bleiben sichtbar und zählen weiter (doppelzählungsfreie Auswertung).
- **4. Personal- und Dozentenverwaltung** — Lehrkräfte mit Qualifikations-/Eignungsnachweisen (Eignungs-Check mit Pflichtkriterien), Fortbildungen, Honorarsätzen, UE-Einsatzauswertung; Self-Service-Portal für Dozenten-Nachweise.
- **5. Dokumentenablage** — zentrale Ablage aller Träger-, QM- und Teilnehmerdokumente mit Kategorien, automatisch vorbefüllten Geltungs-/Aufbewahrungsfristen und Wiedervorlagen; Uploads mit Dateityp-Prüfung und SHA-256-Integritätshash.
- **6. Revisionssicherer Audit-Trail** — siehe B.4.

Weitere produktive Module: GF-Dashboard mit Kennzahlen und Zeitraum-Auswertungen (Auslastung, Soll/Ist-Abweichungen, Förderumsätze, Dozent-Vollständigkeit, fällige Erfolgs-Follow-ups), **Erfolgsmessung** (je Maßnahme frei definierbares Erfolgskriterium mit Follow-up-Frist; Bewertung pro Gutschein in der Teilnehmerakte), Standort- und Unternehmenskontakt-Verwaltung, QM-Modul (Leitbild/Ziele/Risiken, Managementbewertung, Zuverlässigkeitserklärungen, Vertragsvorlagen-Prüfung), Beschwerdemanagement, Befragungs-Ablage (PDF), Kalkulationsmodul mit B-DKS-Abgleich (inkl. Steuerberater-Zugang), DSGVO-Modul (VVT, Datenpannen-Register), Audits & Stichproben (Wurzelregel-Ziehung, Auditbericht-Ablage je Audittermin), Wiedervorlagen/Fristen, Benutzer- und Rollenverwaltung, optionale E-Mail-Anbindung (Gmail-OAuth des Trägers) und Automatisierungs-Webhooks.

B.2 Negativliste (nicht enthalten, Beta oder nur vorbereitet)

Die folgenden Punkte sind **nicht Bestandteil** des produktiven Funktionsumfangs. Soweit der Träger diese Bereiche für seine Zulassung dokumentieren muss, hat er sie anderweitig abzudecken:

- **Kein Lernmanagementsystem (LMS)** — keine Lerninhalte, keine Online-Unterrichtsdurchführung.
- **Keine eM@w-/COSACH-Schnittstelle** zur Bundesagentur für Arbeit (COSACH-Nummern werden als Stammdatum gepflegt).
- **Kein DATEV-/FiBu-Export**; das Kalkulationsmodul ersetzt keine Buchhaltung.

- **Praktikumsverwaltung:** Datenmodell vorbereitet, Benutzeroberfläche nicht produktiv.
- **Keine grafische Stundenplan-Planung** (Planung erfolgt über zukünftig datierte Klassenbuch-Einträge).
- **Digitale Unterschrift mit Unterschriftsbild:** derzeit nicht enthalten. Die „Signatur“ eines Klassenbuch-Eintrags ist eine elektronische Kennzeichnung (Benutzer + Zeitstempel, im Audit-Trail protokolliert), kein grafisches Unterschriftsverfahren.
- **Kein Telefon-Support** und kein Support außerhalb von Werktagen (§ 5 des Vertrags).

B.3 Abbildung der AZAV-Nachweisobjekte

Nachweisobjekt	Abbildung in der Software
Maßnahme / Durchführung	Maßnahme mit Fachbereich, KldB 2010, Zulassungszeitraum, UE-Soll, Kostensatz/B-DKS; je Maßnahme beliebig viele Durchführungen (Kohorten/Einzelmaßnahmen) mit Zeitraum, Hauptdozent, Standort, Plätzen und Belegung.
Teilnehmerakte / Fördermittel	Akte je Teilnehmer mit Statusverlauf; je Gutschein (BGS/AVGS/Gründungsberatung) eigener Datensatz mit BGS-Nummer, Gültigkeit, Bewilligungs- und Auszahlungsdaten, Eignungsfeststellung (als Dokument), Zeitraum, Dokumenten und Audit-PDF pro Gutschein.
Anwesenheit / UE je Termin	Klassenbuch-Tageseintrag je Termin (Datum, Uhrzeit, UE, Inhalt, Dozent) mit Anwesenheitszeile pro Teilnehmer: anwesende/fehlende UE, Fehlzeitart (entschuldigt/unentschuldigt), AU-Quelle; Ist-UE je Durchführung doppelzählungsfrei (Tageseinträge vs. Alt-Nachträge: es zählt der höhere Wert).
Dozentenqualifikation / UE-Einsatz	Lehrkraft-Akte mit Nachweisdokumenten je Qualifikationstyp, Eignungs-Check (fachlich/pädagogisch/Berufserfahrung), Freigabe-Workflow; UE-Einsatz je Dozent aus den Tageseinträgen (inkl. Vertretungs-/Übernahme-Kennzeichnung).
Dokumentenfristen / Wiedervorlagen	Dokumente mit Geltungszeitraum und Aufbewahrungsfrist (automatisch vorbefüllt, überschreibbar); Wiedervorlagen-Modul mit Fälligkeit, Eskalation und Erledigt-Nachweis.
Erfolg / Verbleib	Vermittlungsstatus je Teilnehmer; konfigurierbare Erfolgsmessung je Maßnahme mit Follow-up-Fälligkeit und Bewertung pro Gutschein; Quoten (Abschluss/Abbruch/Integration/Erfolg) im Dashboard.

B.4 Audit-Trail im Detail

- **Protokollumfang:** jede Änderung mit Benutzer, Aktion (CREATE/UPDATE/DELETE/READ bei sensiblen Zugriffen/APPROVE), Vorher-/Nachher-Stand, Zeitstempel und IP-Adresse; zusätzlich alle An-/Abmeldevorgänge inkl. Fehlversuchen.
- **Pseudonymisierung:** besondere Kategorien (Art. 9 DSGVO) und weitere sensible Feldinhalte werden vor der Protokollierung durch SHA-256-Hashwerte ersetzt — Klartext gelangt nicht in das Protokoll.
- **Verkettung:** Einträge sind SHA-256-hash-verkettet, **eine Kette je Mandant** (die Mandanten-ID ist Bestandteil des Hashes); die Tabelle ist auf Datenbankebene gegen UPDATE/DELETE gesperrt

(append-only, serialisiertes Schreiben).

- **Integritätsprüfung:** täglich automatisch (zeitgesteuerter Job); das Ergebnis („Kette intakt · n Events“ bzw. Bruchstelle) ist im Modul Audit-Trail sichtbar. Optional wird ein Ketten-Snapshot zusätzlich an ein externes Ziel übermittelt (Anchoring), sodass auch ein vollständiges Zurücksetzen erkennbar wäre.
- **Nachträge:** rückwirkende Korrekturen sind nur mit Pflicht-Begründung möglich und werden als eigener Protokolleintrag mit Vorher-/Nachher-Stand gekennzeichnet; signierte Klassenbuch-Einträge sind nicht editierbar (Storno + Neuanlage, beides protokolliert).
- **Nachvollzug durch Auditoren:** die Auditor-Rolle sieht das Audit-Trail-Modul mit Kettenstatus und Ereignisliste (read-only); Nachweisexporte erfolgen über die Audit-Pakete (B.5). Auf Anforderung stellt der Anbieter ein Prüfprotokoll der Integritätsprüfung bereit.

B.5 Exporte

Export	Format · Berechtigung · Protokollierung
Teilnehmer-Aktenexport	PDF/ZIP je Teilnehmer bzw. je Gutschein (Stammdaten, Förderung, Anwesenheit, Dokumente). Restriktiver berechtigt als der Lesezugriff (eigene Export-Berechtigung, mengenbegrenzt); jeder Export wird einzeln protokolliert.
Audit-PDFs	Lehrkraft-Audit-Paket, Maßnahmen-PDF, Träger-Audit-Paket — in sich geschlossene PDF-Dokumente für Prüfungssituationen.
Dokumentdateien	Download im Originalformat über die berechtigungsgeprüfte Proxy-Route.
REST-API (v1)	JSON; Endpunkte für Teilnehmer (Liste/Detail/Anlage), Lehrkräfte und Maßnahmen; API-Schlüssel trägergebunden, nur als Hash gespeichert; Aufrufe protokolliert.
Vollexport (Migrationsfall)	Nach § 10 AVV bei Vertragsende (auf Wunsch auch während der Laufzeit): sämtliche Datenbankinhalte des Mandanten in einem gängigen, maschinenlesbaren Format (JSON/CSV, relationale Struktur entsprechend dem Datenmodell — Schemabeschreibung mit Tabellen- und Feldliste wird dem Export beigelegt) sowie alle Dokumentdateien im Originalformat.

B.6 Modul-Rollen-Matrix

Zwölf Rollen: Administrator (Plattformbetreiber), Geschäftsführung (GF), Pädagogische Leitung, Maßnahmeleitung, Lernbegleitung, Dozent:in, Verwaltung, QM, Datenschutzbeauftragte:r (DSB), Steuerberater:in, Auditor:in, Teilnehmer:in. Die Rollen **Auditor, DSB, Steuerberater und Teilnehmer sind strikt lesend** — schreibende Aktionen werden serverseitig in jeder Änderungsaktion zusätzlich geprüft (nicht nur in der Oberfläche).

Modul	GF	Päd.-Ltg.	Maßn.-Ltg.	Lernbegl.	Dozent	Verwaltung	QM	DSB	StB	Auditor	TN
Träger/Standorte	✓	✓	–	–	–	✓	✓	–	–	L	–
Maßnahmen	✓	✓	✓	–	✓	–	✓	–	–	L	–
Durchführungen	✓	✓	✓	–	✓	–	✓	–	–	L	–
Teilnehmer	✓	✓	✓	✓	✓	✓	✓	–	–	L	–

Klassenbuch (UE)	✓	✓	✓	–	✓	✓	✓	–	–	L	–
Personal/Lehrkräfte	✓	✓	–	–	–	✓	✓	–	–	L	–
Dokumentenablage	✓	✓	✓	–	–	✓	✓	L	–	L	–
Audits/Audit-Trail	✓	–	–	–	–	–	✓	–	–	L	–
Akten-/Audit-Export	✓	✓	✓	–	–	✓	✓	–	–	L	–
QM / Beschwerden	✓	✓	–	–	–	–	✓	–	–	–	–
Kalkulation	✓	–	–	–	–	–	–	–	L	–	–
DSGVO-Modul	✓	–	–	–	–	–	✓	L	–	–	–
Benutzerverwaltung	✓	–	–	–	–	–	–	–	–	–	–
Dozenten-Portal	–	–	–	–	✓	–	–	–	–	–	–

✓ = Zugriff gemäß Rolle (Schreibrechte je Aktion zusätzlich serverseitig gated, z. B. Geld-/Statusänderungen nur GF) · L = nur lesend · – = kein Zugriff. Der Administrator (Plattformbetreiber) hat technisch Vollzugriff; seine Zugriffe werden protokolliert (D.3). **Art.-9-Felder** (Reha-Status, Behinderung) sind at-rest verschlüsselt und nur in der Teilnehmerakte für Rollen mit Teilnehmer-Zugriff sichtbar; im Audit-Trail erscheinen sie ausschließlich pseudonymisiert. **Vollexporte** löst nur die Export-Berechtigung (Zeile „Akten-/Audit-Export“) aus – Lernbegleitung und Dozenten sind bewusst ausgeschlossen (Datenminimierung).

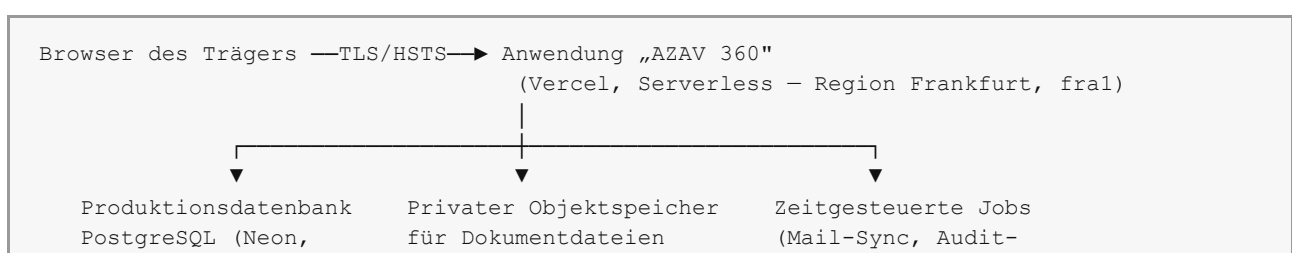
B.7 Schnittstellen und Verantwortungsgrenze

- **REST-API v1** (Teilnehmer, Lehrkräfte, Maßnahmen): Authentifizierung über trägergebundene API-Schlüssel, die nur als Hash gespeichert werden; mandantengebundener Datenzugriff, Aufruf-Protokollierung.
- **Eingehende Webhooks** (z. B. Lead-Anlage aus Webformularen): HMAC-SHA256-signiert, Replay-Schutz.
- **Ausgehende Webhooks** (z. B. Automatisierung über Make.com): vom Träger konfiguriert; Datenumfang bestimmt der Träger.
- **Google-Workspace-Anbindung (optional)**: E-Mail-Sync über das OAuth-autorisierte Postfach des Trägers; Tokens werden verschlüsselt gespeichert.
- **Zeitgesteuerte Jobs**: Mail-Sync (30-Minuten-Takt), Audit-Integritätsprüfung (täglich), Datenpannen-Fristenüberwachung (stündlich) – abgesichert über zeitkonstant geprüfte Geheimnisse.

Verantwortungsgrenze (§ 6 Abs. 4 AVV): Dienste, die der Träger selbst anbindet – insbesondere das eigene Google-Postfach und eigene Automatisierungs-Webhooks – sind keine Unterauftragsverarbeiter des Anbieters; für Auswahl und Rechtsgrundlage dieser Dienste ist der Träger verantwortlich.

C. Betrieb und Hosting

C.1 Architektur



AWS eu-central-1 = Frankfurt am Main)	(Vercel Blob, Region siehe C.2)	Integritätsprüfung, Fristen-Überwachung)
--	------------------------------------	---

Optionale, vom Träger angebundene Dienste (Verantwortung Träger, § 6 Abs. 4 AVV):
Google-Postfach (OAuth) · Automatisierungs-Webhooks (z. B. Make.com)

Alle Zugriffe laufen über die Anwendung (Server-seitige Berechtigungs- und Mandantenprüfung je Anfrage); es gibt keinen Direktzugriff des Trägers auf Datenbank oder Objektspeicher. Dokument-Downloads laufen über eine authentifizierte Proxy-Route.

C.2 Speicherorte

Anwendungsbetrieb: Vercel, Region Frankfurt am Main (fra1). Produktionsdatenbank: Neon („Vercel Postgres“), Rechenzentrumsregion Frankfurt am Main (AWS eu-central-1). **Objektspeicher für Dokumentdateien:** Region _____ (verbindlich; identisch in AVV Anlage 3 einzutragen — dieser Eintrag schließt den dort offen gelassenen Punkt).

C.3 Verfügbarkeit, Wartung, Störungen

Zugesagt sind 98,5 % Verfügbarkeit im Monatsmittel am Übergabepunkt des Rechenzentrums (§ 5 des Vertrags). Die Messung stützt sich auf die Verfügbarkeits- und Vorfalldaten der Infrastruktur-Dienstleister (Vercel-/Neon-Status und Deploy-/Funktionsprotokolle); eine eigene öffentliche Statusseite besteht nicht. Geplante Wartungen werden — soweit möglich — außerhalb üblicher Geschäftszeiten durchgeführt und in Textform oder in der Software angekündigt; Störungen und deren Behebung kommuniziert der Anbieter per E-Mail an die benannten Ansprechpartner des Trägers.

C.4 Datensicherung und Wiederherstellung

- **Datenbank:** tägliche automatische Sicherungen durch den Datenbank-Dienstleister (Neon) gemäß dessen Leistungsbeschreibung; Aufbewahrung der Sicherungen: _____ Tage (gemäß gebuchtem Neon-Plan eintragen).
- **Zielwerte:** RPO $\leq$ 24 Stunden (tägliche Sicherung), RTO-Ziel _____ Stunden. Letzter erfolgreich getesteter Restore: _____ (Datum eintragen; Test mindestens jährlich).
- **Dokumentdateien:** werden im redundanten Objektspeicher vorgehalten; eine darüber hinausgehende Sicherung der Dokumentdateien erfolgt **nicht**. Deshalb sichert der Träger wichtige Auswertungen und Dokumente zusätzlich über die Export- und Downloadfunktionen (§ 6 Abs. 3 des Vertrags).

C.5 Release-, Änderungs- und Incident-Management

- **Änderungen** werden versioniert entwickelt (Git); jede Änderung durchläuft vor der Produktivsetzung eine Vorschau-Umgebung (Preview-Deployment) und die automatisierten **Sicherheits-Regressionstests** der kritischen Schutzmechanismen (Berechtigungsmatrix, Protokollkette, Verschlüsselung, Mandantentrennung, Upload-Härtung — vgl. AVV Anlage 2 Nr. 8). Schlägt ein Test oder der Build fehl, wird nicht ausgeliefert.
- **Rollback:** jede vorherige Produktivversion kann über den Hosting-Dienstleister unmittelbar wieder aktiviert werden; Datenbankmigrationen werden idempotent ausgeführt und dokumentiert.
- **Incidents:** Meldung an info@valtrion.de; Reaktion an Werktagen i. d. R. innerhalb von zwei Werktagen (§ 5 des Vertrags), Eskalation an die Geschäftsführung. Verletzungen des Schutzes personenbezogener Daten werden abweichend hiervon unverzüglich, spätestens innerhalb von 48 Stunden gemeldet (§ 8 AVV) und im Datenpannen-Register mit 72-Stunden-Fristüberwachung dokumentiert.

C.6 Unterauftragsverarbeiter und Support-Zugriffe

Eingesetzte Unterauftragsverarbeiter: Vercel Inc. (Hosting, Objektspeicher) und Neon Inc. (Produktionsdatenbank) — Details, Verarbeitungsorte und Garantien in AVV Anlage 3. Der Anbieter überwacht die Subprozessorenlisten der Dienstleister (Vercel-DPA) und informiert den Träger über Änderungen mindestens vier Wochen im Voraus (§ 6 AVV). Support-Zugriffe des Anbieters selbst erfolgen aus Deutschland; Support-Zugriffe der US-Gesellschaften der Dienstleister sind möglich und über EU-Standardvertragsklauseln abgesichert (D.6).

D. Datenschutz und Informationssicherheit

D.1 Datenkategorien und Zwecke

Datenkategorien, betroffene Personen und Zwecke sind vollständig und deckungsgleich in **AVV Anlage 1** beschrieben: Teilnehmer- und Fördervorgangsdaten aus SGB-II/III-Kontext (Bildungsgutschein/AVGS), Anwesenheits- und Fehlzeitdaten inkl. AU-Nachweisen, Personal-/Dozentendaten, Benutzer- und Protokolldaten sowie Ansprechpartner- und Beschwerdedaten. Die Verarbeitung umfasst **besondere Kategorien nach Art. 9 DSGVO** (insbesondere Gesundheitsdaten: Reha-Status, AU-Nachweise) und Angaben mit Bezug zu **Art. 10 DSGVO** (Zuverlässigkeitserklärungen der gesetzlichen Vertreter).

D.2 Technische und organisatorische Maßnahmen (Kurzfassung)

Vollständig in AVV Anlage 2; für die Auditpraxis die wichtigsten Punkte:

- **Transport:** durchgehend TLS, HSTS mit Preload; strikte Content-Security-Policy und Sicherheits-Header.
- **Feldverschlüsselung:** Art.-9-Felder, 2FA-Geheimnisse und OAuth-Tokens anwendungsseitig AES-256-GCM-verschlüsselt. Schlüsselverwaltung: der Schlüssel liegt ausschließlich als Umgebungsvariable in der abgesicherten Konfigurationsverwaltung des Hosting-Dienstleisters; Zugriff hat nur die Geschäftsführung des Anbieters; Rotation anlassbezogen (mindestens bei Personalwechsel mit Zugriff); ohne konfigurierten Schlüssel verweigert die Anwendung den Start (*fail-closed*).
- **Anmeldung:** bcrypt-Passwort-Hashes (Kostenfaktor 12), Brute-Force-Schutz, Zwei-Faktor-Authentifizierung (TOTP nach RFC 6238, Erzwingung bei eingerichteter 2FA), Session-Härtung (http-Only/Secure/SameSite=strict, 12-Stunden-Fenster, serverseitige Sofort-Invalidierung bei Abmeldung/Passwort-Reset/Rollenwechsel/Deaktivierung).
- **Protokoll-Pseudonymisierung:** sensible Feldinhalte erscheinen im Audit-Trail nur als SHA-256-Hash.
- **Mandantentrennung:** jede Abfrage und Änderung mandantengebunden, auch bei Datei-Up-/Downloads; getrennte Protokollketten je Mandant.

D.3 Zugriff auf Produktivdaten beim Anbieter

Zugriff auf Produktivdaten haben ausschließlich die Geschäftsführung und die mit Betrieb/Support betrauten Personen des Anbieters nach dem Need-to-know-Prinzip; die Berechtigungsvergabe wird dokumentiert (§ 4 Abs. 3 AVV), alle Personen sind schriftlich zur Vertraulichkeit verpflichtet (interne Vertraulichkeitsverpflichtung, Sozialgeheimnis-Niveau). Administrative Zugriffe über das Plattform-Administratorkonto werden im Audit-Trail protokolliert; Supportzugriffe auf Trägerdaten erfolgen nur anlassbezogen auf Anforderung oder Weisung des Trägers.

D.4 Löschkonzept und Datenpannenprozess

- **Im Betrieb:** fachliche Aufbewahrungsfristen je Dokumentbereich (automatisch vorbefüllt, überschreibbar); Archivierung statt Hard-Delete für nachweisrelevante Objekte (revisionssicher); Löschung von Teilnehmerdaten durch den Träger im Rahmen seiner Verantwortlichkeit.
- **Nach Vertragsende (§ 10 AVV):** Wahlrecht Rückgabe oder Löschung binnen 30 Tagen (mit Hinweis und 14-Tage-Schonfrist); Löschung aus Produktivsystemen innerhalb von 30 Tagen, aus Sicherungen durch turnusmäßige Überschreibung spätestens nach weiteren 90 Tagen.
- **Datenpannen (§ 8 AVV):** Meldung an den Träger unverzüglich, spätestens binnen 48 Stunden; Dokumentation im Datenpannen-Register der Software mit automatischer Überwachung der 72-Stunden-Frist (Art. 33 DSGVO); die Meldung an Aufsichtsbehörde/Betroffene obliegt dem Träger, der Anbieter unterstützt.

D.5 Prüfnachweise

Für die Anwendung liegt eine dokumentierte **Sicherheitsüberprüfung (Application-Security-Audit) vom Mai 2026** vor: unabhängige werkzeuggestützte Prüfung von Berechtigungsmodell, Mandantentrennung, Authentifizierung, Injection-Flächen und Abhängigkeiten; Ergebnis: keine kritischen und keine hohen Feststellungen; die mittleren und niedrigen Feststellungen wurden nachweislich im Code behoben. Der Bericht wird im Rahmen der Kontrollrechte nach § 9 AVV zur Verfügung gestellt. Prüfzyklus: Wiederholung mindestens jährlich sowie anlassbezogen nach wesentlichen Architekturänderungen; die Sicherheits-Regressionstests (C.5) laufen fortlaufend. Eine eigene ISO-27001-/SOC-2-Zertifizierung des Anbieters besteht nicht (ehrliche Selbstauskunft); die Infrastruktur-Dienstleister verfügen über branchenübliche Zertifizierungen gemäß ihren veröffentlichten Nachweisen.

D.6 Drittlandtransfer

Die Daten ruhen in Rechenzentren in Frankfurt am Main (C.2). Ein Drittlandbezug besteht ausschließlich über mögliche Support-Zugriffe der US-Gesellschaften der Unterauftragsverarbeiter. Grundlage: Auftragsverarbeitungsverträge (DPA) mit Vercel und Neon jeweils einschließlich EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO); Data-Privacy-Framework-Status der US-Gesellschaften:

(bei Abschluss der DPAs prüfen und eintragen). **Transferbewertung**

(Kurzfassung, zitierfähig): Verarbeitung und Speicherung erfolgen in der EU; Transportwege und ruhende Daten sind verschlüsselt, besonders sensible Felder zusätzlich anwendungsseitig (AES-256-GCM); ein etwaiger Drittlandzugriff beschränkt sich auf administrative Supportfälle der Dienstleister und ist durch SCC nebst technischer Maßnahmen abgesichert; ein unverhältnismäßiges Restrisiko ist nicht ersichtlich.

E. AZAV-Verwendbarkeit

E.1 Mapping „Funktion → Prüfpunkt“

Prüfpunkt (AZAV / SGB III)	Funktion in AZAV 360
Maßnahmezulassung, Kostensätze (§§ 179, 180 SGB III; § 3 AZAV)	Maßnahmenverwaltung mit Zulassungsdaten, Fachbereich, KldB; Kalkulationsmodul mit B-DKS-Abgleich und Beleg-Ablage für die FKS-Stellungnahme.

Unterrichts- und Anwesenheitsnachweis (§ 2 Abs. 4 AZAV; Prüfdienst der BA)	Klassenbuch: Tageseinträge mit UE, Inhalt, Dozent, Anwesenheit/Fehlzeiten je Teilnehmer, AU-Nachweisablage, Teilnehmer-Bestätigungslinks, elektronische Kennzeichnung („Signatur“) je Eintrag.
Dozenteneignung (§ 2 Abs. 3 AZAV)	Lehrkraft-Akte mit Nachweisdokumenten, Eignungs-Check (fachlich/pädagogisch/Berufserfahrung), Freigabe-Workflow, Lehrkraft-Audit-Paket.
Teilnehmerbezogene Förder-Dokumentation (Bildungsgutschein/AVGS)	Gutschein-Datensätze mit BGS-Nummer, Gültigkeit, Bewilligung, Abrechnungsstatus; Audit-PDF pro Gutschein; Audit-Reife-Prüfung der Akte.
QM-Dokumentation (§ 2 Abs. 4 AZAV; § 178 Nr. 4 SGB III)	QM-Modul (Leitbild, Ziele, Risiken), jährliche Managementbewertung, Vertragsvorlagen-Prüfung, Befragungs-Ablage, Erfolgsmessung mit Follow-up.
Zuverlässigkeit des Trägers (§ 2 Abs. 1 AZAV)	Zuverlässigkeitserklärungen der gesetzlichen Vertreter mit Nachweisdokumenten und Wiedervorlage.
Beschwerdemanagement (§ 2 Abs. 4 AZAV)	Beschwerde-Modul mit Workflow-Bearbeitung und Auswertung.
Einsichts- und Auskunftsfähigkeit (§ 183 SGB III; FKS/DakS-Audits)	Read-only-Auditorenrolle, Audit-Pakete (Teilnehmer/Lehrkraft/Maßnahme/Träger), revisionssicherer Audit-Trail mit sichtbarem Integritätsstatus, Stichprobenziehung.
Fristen- und Dokumentenmanagement	Dokumentenablage mit Geltungs-/Aufbewahrungsfristen, Wiedervorlagen mit Eskalation, Zertifikats- und AVV-Fristen des Trägers.
Datenschutz (Art. 30/33 DSGVO)	VVT, Datenpannen-Register mit Fristüberwachung, Einwilligungsverwaltung, Rollen-/Berechtigungskonzept.

E.2 Pflichtenabgrenzung

Die Software liefert die **revisionssichere Führung** der Nachweise während der Vertragslaufzeit (append-only Audit-Trail, Integritätsprüfung, berechtigungsgeprüfte Exporte). Die **Aufbewahrung über das Vertrags- bzw. Zertifikatsende hinaus** — einschließlich steuer- und handelsrechtlicher Fristen von bis zu zehn Jahren — bleibt Pflicht des Trägers und wird über die Export- und Downloadfunktionen erfüllt (§ 6 Abs. 3 und Abs. 5 des Software-Nutzungsvertrags, § 10 AVV). Die inhaltliche Richtigkeit der Dokumentation und die Erfüllung der zulassungs-, förder- und datenschutzrechtlichen Pflichten verbleiben beim Träger (§ 8 des Vertrags); die Software garantiert weder Audit- noch Zulassungs- oder Förderentscheidungen.