Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag

nach Art. 28 der Verordnung (EU) 2016/679 (DSGVO) für die Nutzung der Software „AZAV 360“

Hinweis zum Ausfüllen: Bitte ergänzen Sie Ihre Angaben auf **Seite 1** (Vertragsparteien und Datum des Software-Nutzungsvertrags) und unterschreiben Sie auf **Seite 5**. Alle übrigen Angaben sind bereits vollständig; anbieterseitig ist die Vereinbarung elektronisch gezeichnet (§ 11 Abs. 3). Senden Sie das unterschriebene Dokument an info@valtrion.de.

zwischen

_____ (Firma des Bildungsträgers)
_____ (Straße, Hausnummer)
_____ (PLZ, Ort)
vertreten durch _____ (Geschäftsführung)

— nachfolgend „Verantwortlicher“ —

und

Valtrion Operations UG (haftungsbeschränkt)
Rheinpromenade 13, 40789 Monheim am Rhein
vertreten durch den Geschäftsführer Justin-Pascal Schlimnat
Amtsgericht Düsseldorf, HRB 110242 · E-Mail: info@valtrion.de

— nachfolgend „Auftragsverarbeiter“ —

Präambel

Der Verantwortliche nutzt auf Grundlage des zwischen den Parteien geschlossenen Software-Nutzungsvertrags vom _____ (Datum des Software-Nutzungsvertrags) (nachfolgend „Hauptvertrag“) die vom Auftragsverarbeiter betriebene webbasierte Verwaltungs- und Auditvorbereitungssoftware „AZAV 360“ (app.azav360.de). Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien nach Art. 28 Abs. 3 DSGVO. Die Anlagen 1 bis 3 sind Bestandteil dieser Vereinbarung.

§ 1 Gegenstand und Dauer

(1) Gegenstand des Auftrags ist der Betrieb und die Bereitstellung der Software „AZAV 360“ als Software-as-a-Service einschließlich Datenbank- und Dokumentenspeicherung, Pflege, Wartung und Support.

(2) Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags. Sie endet nicht vor der vollständigen Löschung bzw. Rückgabe der Daten nach § 10.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus **Anlage 1**.

(2) Die Verarbeitung findet grundsätzlich in Mitgliedstaaten der Europäischen Union oder des EWR statt (Rechenzentrumsregion Frankfurt am Main). Ein darüber hinausgehender Drittlandbezug besteht nur gegenüber den in **Anlage 3** genannten Unterauftragsverarbeitern (etwa durch Support-Zugriffe der US-Gesellschaften); insoweit gilt die Beauftragung nach dieser Vereinbarung als dokumentierte Weisung, und es bestehen die in Anlage 3 genannten Garantien nach Art. 44 ff. DSGVO. Jede weitere Übermittlung in ein Drittland bedarf einer vorherigen dokumentierten Weisung des Verantwortlichen.

(3) Die Verarbeitung umfasst auch besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO (insbesondere Gesundheitsdaten) sowie Angaben mit Bezug zu Art. 10 DSGVO (Zuverlässigkeitserklärungen); der Umfang ergibt sich aus Anlage 1. Der Auftragsverarbeiter trägt der besonderen Sensibilität dieser Daten durch die Maßnahmen der **Anlage 2** Rechnung.

§ 3 Weisungsrecht des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet; in einem solchen Fall teilt er dem Verantwortlichen diese Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet. Als dokumentierte Weisungen gelten diese Vereinbarung, der Hauptvertrag sowie die Nutzung der Softwarefunktionen durch den Verantwortlichen.

(2) Weitergehende Weisungen bedürfen der Textform (E-Mail genügt). Mündlich erteilte Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen verstößt, informiert er den Verantwortlichen unverzüglich. Er ist berechtigt, die Ausführung bis zur Bestätigung oder Änderung der Weisung auszusetzen.

§ 4 Vertraulichkeit und Personal

(1) Der Auftragsverarbeiter setzt für die Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort und wird auf Verlangen nachgewiesen.

(2) Die Teilnehmerdaten stammen überwiegend aus Fördervorgängen nach dem SGB II/III (Bildungsgutschein, AVGS). Der Auftragsverarbeiter behandelt diese Daten mit einer dem Sozialgeheimnis (§ 35 SGB I) entsprechenden Vertraulichkeit und verarbeitet sie ausschließlich zweckgebunden im Rahmen dieses Auftrags.

(3) Zugriff auf personenbezogene Daten des Verantwortlichen erhalten nur Personen, soweit dies für Betrieb, Wartung und Support erforderlich ist (Need-to-know-Prinzip); die Berechtigungsvergabe wird dokumentiert.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und hält sie während der Laufzeit dieser Vereinbarung aufrecht.

(2) Die Maßnahmen dürfen an den Stand der Technik angepasst und weiterentwickelt werden, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert; die jeweils aktuelle Fassung der Anlage 2 wird dem Verantwortlichen auf Anfrage zur Verfügung gestellt.

§ 6 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt die allgemeine Genehmigung zur Einschaltung von Unterauftragsverarbeitern (Art. 28 Abs. 2 DSGVO). Die bei Abschluss dieser Vereinbarung eingesetzten Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt.

(2) Über beabsichtigte Änderungen (Ersetzung oder Neubeauftragung) informiert der Auftragsverarbeiter den Verantwortlichen mindestens vier Wochen im Voraus in Textform. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen. Kommt keine einvernehmliche Lösung zustande, steht dem Verantwortlichen ein Sonderkündigungsrecht für den Hauptvertrag zu.

(3) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich im Wesentlichen dieselben Datenschutzpflichten auf, wie sie in dieser Vereinbarung festgelegt sind (Art. 28 Abs. 4 DSGVO), und weist die wesentlichen Vertragsinhalte auf Verlangen nach. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Unterauftragsverarbeiters (Art. 28 Abs. 4 Satz 2 DSGVO).

(4) **Klarstellung:** Dienste, die der Verantwortliche selbst an die Software anbindet — insbesondere das eigene Google-Postfach für die optionale E-Mail-Anbindung sowie eigene Automatisierungs-Webhooks (z. B. Make.com) — sind keine Unterauftragsverarbeiter des Auftragsverarbeiters. Für den datenschutzkonformen Einsatz dieser Dienste, einschließlich des Abschlusses erforderlicher Verträge (z. B. Google-Workspace-Auftragsverarbeitungsvertrag), ist der Verantwortliche selbst verantwortlich.

§ 7 Unterstützungspflichten

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen auf Wahrnehmung ihrer Rechte (Art. 12–23 DSGVO) zu beantworten. Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet er das Ersuchen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst. Unterstützungsleistungen nach diesem Absatz erbringt der Auftragsverarbeiter unverzüglich, in der Regel innerhalb von fünf Arbeitstagen nach Anforderung in Textform.

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO (Sicherheit der Verarbeitung, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(3) Für Unterstützungsleistungen, die nicht auf Umständen aus der Sphäre des Auftragsverarbeiters beruhen und über den vertragsgemäßen Betrieb hinausgehen, kann eine angemessene Vergütung nach Aufwand vereinbart werden.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betrifft, unverzüglich nach Kenntniserlangung, spätestens innerhalb von 48 Stunden, in Textform an die vom Verantwortlichen benannte Kontaktadresse, ersatzweise an dessen Geschäftsführung. Die Meldung enthält mindestens die Angaben entsprechend Art. 33 Abs. 3 DSGVO, soweit verfügbar; nachträglich bekannt werdende Informationen werden unverzüglich nachgereicht.

(2) Die Meldung gegenüber der Aufsichtsbehörde und die Benachrichtigung betroffener Personen obliegen dem Verantwortlichen. Der Auftragsverarbeiter unterstützt ihn hierbei und dokumentiert Vorfälle im Datenpannen-Register der Software.

§ 9 Nachweise und Kontrollrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung, insbesondere durch die Dokumentation der Anlage 2, Selbstauskünfte, Prüf- und Testberichte.

(2) Genügen diese Nachweise nach Einschätzung des Verantwortlichen im Einzelfall nicht, kann der Verantwortliche einmal pro Kalenderjahr sowie anlassbezogen (insbesondere nach einer Verletzung nach § 8) eine Überprüfung — auch vor Ort oder im Wege des Fernzugriffs — durchführen oder durch einen zur Verschwiegenheit verpflichteten Dritten durchführen lassen. Prüfungen sind mindestens 14 Kalendertage vorher anzukündigen, erfolgen zu üblichen Geschäftszeiten und ohne unverhältnismäßige Störung des Betriebs. Jede Partei trägt ihre eigenen Kosten.

(3) Der Auftragsverarbeiter duldet Prüfungen der zuständigen Datenschutzaufsichtsbehörde und wirkt an Prüfungen mit, denen der Verantwortliche als AZAV-Bildungsträger unterliegt (insbesondere durch Zertifizierungsstellen/DAkkS und den Prüfdienst der Bundesagentur für Arbeit), indem er die erforderlichen Nachweise aus dem System bereitstellt. Über behördliche Untersuchungen, Anfragen oder Maßnahmen mit Bezug auf Daten des Verantwortlichen informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, soweit gesetzlich zulässig.

§ 10 Löschung und Rückgabe nach Auftragsende

(1) Nach Beendigung des Hauptvertrags gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten zurück (Export der Datenbankinhalte in einem gängigen, maschinenlesbaren Format sowie der gespeicherten Dokumentdateien) oder löscht sie, sofern nicht eine Rechtspflicht zur Speicherung besteht. Die Wahl ist innerhalb von 30 Tagen nach Vertragsende in Textform mitzuteilen; andernfalls erfolgt die Löschung. Der Auftragsverarbeiter weist den Verantwortlichen bei Beendigung des Hauptvertrags in Textform auf das Wahlrecht und die Frist hin; eine Löschung erfolgt frühestens 14 Tage nach diesem Hinweis.

(2) Die Löschung aus den Produktivsystemen erfolgt innerhalb von 30 Tagen nach der Rückgabe bzw. nach Ablauf der Frist nach Absatz 1. Daten in Sicherungskopien werden durch turnusmäßige

Überschreibung spätestens nach weiteren 90 Tagen gelöscht; bis dahin werden sie nicht mehr aktiv verarbeitet.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sowie Daten, für die eine gesetzliche Aufbewahrungspflicht des Auftragsverarbeiters besteht, dürfen entsprechend länger aufbewahrt werden; sie werden für die weitere Verarbeitung gesperrt.

(4) Die Löschung wird dem Verantwortlichen auf Anfrage schriftlich bestätigt.

§ 11 Haftung und Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO; im Übrigen gelten die Regelungen des Hauptvertrags.

(2) Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen in datenschutzrechtlichen Fragen die Regelungen dieser Vereinbarung vor.

(3) **Zustandekommen:** Diese Vereinbarung ist vom Auftragsverarbeiter elektronisch gezeichnet (Art. 28 Abs. 9 DSGVO — elektronisches Format). Sie kommt zustande, sobald der Verantwortliche sie unterzeichnet und in Textform an info@valtrion.de übermittelt; einer Gegenzeichnung im Einzelfall bedarf es nicht. Der Auftragsverarbeiter bestätigt den Zugang in Textform.

(4) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform.

(5) Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(6) Es gilt deutsches Recht. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragsverarbeiters.

Anlagen: Anlage 1 — Gegenstand der Verarbeitung, Datenarten und betroffene Personen · Anlage 2 — Technische und organisatorische Maßnahmen · Anlage 3 — Unterauftragsverarbeiter

Ort, Datum

Unterschrift Verantwortlicher

Name in Druckbuchstaben

Für den Auftragsverarbeiter —
elektronisch gezeichnet gemäß § 11 Abs. 3 (Art. 28 Abs. 9 DSGVO):

gez. Justin-Pascal Schlimnat, Geschäftsführer
Valtrion Operations UG (haftungsbeschränkt)
Monheim am Rhein · Fassung: Juli 2026

Anlage 1 — Gegenstand der Verarbeitung, Datenarten und betroffene Personen

1. Art und Zweck der Verarbeitung

Speicherung, Organisation, Auswertung, Bereitstellung und Löschung personenbezogener Daten im Rahmen der Nutzung der Software „AZAV 360“ durch den Verantwortlichen zu folgenden Zwecken: Verwaltung von Maßnahmen und Durchführungen nach §§ 45, 81 ff. SGB III (AZAV), Teilnehmer- und Förderverwaltung (Bildungsgutschein/AVGS), Anwesenheits- und Unterrichtsdokumentation, Personal- und Dozentenverwaltung, Dokumentenablage, Qualitätsmanagement, Beschwerdemanagement, Vorbereitung von Audits und Prüfungen sowie optional E-Mail-Kommunikation über vom Verantwortlichen angebundene Postfächer.

2. Kategorien betroffener Personen und Datenarten

Betroffene Personen	Datenarten
Teilnehmende und Interessenten des Verantwortlichen	Stammdaten (Name, Geburtsdatum/-ort, Geschlecht, Staatsangehörigkeit, Anschrift), Kontaktdaten; Teilnahme- und Verlaufsdaten (Status, Ein-/Austritt, Ergebnis, Akquisequelle); Eignungs- und Profildaten; Förderdaten (Bildungsgutschein-/AVGS-Nummer, Kostenträger, Bewilligungs- und Abrechnungsdaten); Anwesenheits- und Fehlzeitdaten (inkl. AU-Nachweisen); Vertrags-, Praktikums-, Vermittlungs- und Verbleibsdaten; Einwilligungen; Dokumente der Teilnehmerakte; ggf. E-Mail-Korrespondenz (Nr. 4)
Lehrkräfte und Dozierende	Stamm- und Kontaktdaten; Beschäftigungs- und Honorardaten; Qualifikations-, Eignungs- und Fortbildungsdaten inkl. Nachweisdokumenten; Einsatz-, Vertretungs- und Beurteilungsdaten; Personaldokumente
Mitarbeitende und Benutzer des Verantwortlichen (inkl. externer Rollen wie Steuerberatung, Datenschutzbeauftragte, Auditoren)	Konto- und Anmeldedaten (E-Mail, Passwort-Hash, Rolle, Zwei-Faktor-Daten), Funktions- und Beschäftigungsdaten, Protokoll- und Nutzungsdaten (Audit-Trail inkl. IP-Adresse)
Gesetzliche Vertreter / Geschäftsführung des Verantwortlichen	Stammdaten; Zuverlässigkeitserklärungen inkl. Nachweisdokumenten (Angaben mit Bezug zu Art. 10 DSGVO)
Ansprechpersonen von Kostenträgern, Unternehmen, Praktikumsbetrieben und Kooperationspartnern	Name, Funktion, geschäftliche Kontaktdaten, Vorgangsbezug (z. B. Sachbearbeitung beim Kostenträger)
Beschwerdeführende (ggf. anonym)	Name und Kontaktdaten (optional), Beschwerdegegenstand und Bearbeitungsverlauf
Kommunikationspartner angebundener E-Mail-Postfächer (nur bei aktivierter E-Mail-Anbindung)	Absender-/Empfängerangaben, Betreff, Nachrichteninhalt, Metadaten von Anhängen

3. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)

Gesundheitsdaten: Reha-Status und Angaben zu Behinderung (anwendungsseitig verschlüsselt gespeichert), krankheitsbedingte Fehlzeiten und Arbeitsunfähigkeitsnachweise sowie ggf. gesundheitsbezogene Angaben in Freitextfeldern und hochgeladenen Dokumenten. Daneben werden Zuverlässigkeitserklärungen der gesetzlichen Vertreter verarbeitet (Angaben zu Straffreiheit, Art. 10 DSGVO).

4. Herkunft der Daten

Die Daten werden vom Verantwortlichen und seinen Benutzern in die Software eingegeben bzw. hochgeladen; Teilnehmerdaten stammen überwiegend aus Fördervorgängen der Agenturen für Arbeit und Jobcenter (SGB II/III). Bei aktivierter E-Mail-Anbindung werden Nachrichten aus den vom Verantwortlichen verbundenen Postfächern in die Software übernommen.

Anlage 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Stand: Juli 2026. Die Maßnahmen werden fortlaufend an den Stand der Technik angepasst (§ 5 Abs. 2 der Vereinbarung).

1. Zugangskontrolle (Authentifizierung)

- Zugriff nur über persönliche Benutzerkonten; Passwörter werden ausschließlich als bcrypt-Hash (Kostenfaktor 12) gespeichert.
- Mehrstufiger Brute-Force-Schutz beim Login (Begrenzung pro IP und Konto) und Schutz vor Account-Enumeration durch zeitkonstante Prüfungen.
- Server-signierte, verschlüsselte Session-Cookies (httpOnly, Secure, SameSite=strict) mit automatischem Sitzungsablauf nach 12 Stunden Inaktivität (gleitendes Fenster); sofortige serverseitige Invalidierung aller Sitzungen bei Abmeldung, Passwort-Zurücksetzung, Rollenwechsel oder Deaktivierung eines Kontos.
- Erzwungener Passwortwechsel nach Erst- und Reset-Passwörtern; erneute Passwortabfrage vor privilegierten Administrations-Aktionen.
- Zwei-Faktor-Authentifizierung (TOTP nach RFC 6238) steht je Benutzerkonto zur Verfügung und wird bei eingerichteter 2FA beim Login erzwungen; die 2FA-Geheimnisse werden verschlüsselt gespeichert.

2. Zugriffskontrolle (Berechtigungen)

- Rollenbasierte Zugriffskontrolle mit zentraler Modul-Rollen-Matrix über zwölf Rollen (u. a. Geschäftsführung, QM, Datenschutzbeauftragte, externe Auditoren, Steuerberatung); jede Seite und jede Änderungsaktion wird serverseitig geprüft.
- Der Vollexport von Teilnehmerakten (inkl. Art.-9-Daten) ist restriktiver berechtigt als der Lesezugriff und zusätzlich mengenbegrenzt; jeder Export wird einzeln protokolliert.

3. Trennungskontrolle (Mandantentrennung)

- Strikte Mandantentrennung: jede Datenbankabfrage und jede Änderung ist an den Mandanten (Träger) gebunden; mandantenübergreifende Zugriffe werden serverseitig blockiert, auch bei Datei-Uploads und -Downloads.
- Getrennte, kryptografisch verkettete Protokollketten je Mandant.

4. Verschlüsselung und Pseudonymisierung

- Transportverschlüsselung durchgehend per TLS; HSTS mit Preload erzwungen.
- Besondere Kategorien personenbezogener Daten (Reha-Status, Behinderung) sowie technische Geheimnisse (2FA-Geheimnisse, OAuth-Tokens) werden anwendungsseitig mit AES-256-GCM verschlüsselt gespeichert; ohne konfigurierten Schlüssel verweigert die Anwendung den Betrieb (fail-closed).
- Speicherung der Datenbank- und Dateiinhalte bei den Unterauftragsverarbeitern erfolgt zusätzlich auf verschlüsselter Infrastruktur (Anbietermaßnahme).
- Pseudonymisierung im Änderungsprotokoll: sensible Feldinhalte (u. a. Gesundheitsdaten, Kontaktdaten, Geburtsdaten) werden vor der Protokollierung durch SHA-256-Hashwerte ersetzt; Klartext gelangt nicht in das Protokoll.

5. Eingabekontrolle (Nachvollziehbarkeit)

- Manipulationssicheres, revisionssicheres Änderungsprotokoll (Audit-Trail): jede Änderung wird mit Benutzer, Aktion, Vorher-/Nachher-Stand und Zeitstempel protokolliert; die Einträge sind SHA-256-hash-verkettet und auf Datenbankebene gegen nachträgliche Änderung und Löschung gesperrt (append-only).
- Tägliche automatische Integritätsprüfung der Protokollketten; nachträgliche Einträge sind nur mit Pflicht-Begründung möglich und werden als Nachtrag gekennzeichnet.
- Protokollierung aller An- und Abmeldevorgänge einschließlich Fehlversuchen, jeweils mit IP-Adresse.

6. Weitergabekontrolle

- Dokumentdateien liegen ausschließlich in einem privaten, zugriffsgeschützten Objektspeicher; Abruf nur über eine authentifizierte Proxy-Route mit Berechtigungs- und Mandantenprüfung.
- Upload-Härtung: inhaltsbasierte Dateityp-Prüfung (Magic Bytes), Größenbegrenzung, Integritätshash (SHA-256) je Datei.
- Härtung gegen Web-Angriffe: strikte Content-Security-Policy, Sicherheits-Header, CSRF-Schutz, Schutz vor Server-Side-Request-Forgery.
- Maschinenschnittstellen nur mit Authentifizierung: zeitkonstant geprüfte Cron-Geheimnisse, API-Schlüssel nur als Hash gespeichert, signierte Webhooks (HMAC-SHA256).

7. Verfügbarkeitskontrolle

- Betrieb auf redundanter Cloud-Infrastruktur (Vercel/Neon, Region Frankfurt); tägliche automatische Datenbanksicherungen durch den Datenbank-Dienstleister gemäß dessen Leistungsbeschreibung.
- Lastbegrenzung durch persistente Rate-Limits und Ressourcen-Limits; sicherheitsrelevante Fehlkonfigurationen führen zur Betriebsverweigerung statt zu unsicherem Betrieb (fail-closed).

8. Auftragskontrolle und Organisation

- Verarbeitung nur auf dokumentierte Weisung gemäß dieser Vereinbarung; Vertraulichkeitsverpflichtung aller mit der Verarbeitung befassten Personen.
- Datenpannen-Register in der Software mit automatischer Überwachung der 72-Stunden-Frist (Art. 33 DSGVO).
- Automatisierte Sicherheits-Regressionstests der kritischen Schutzmechanismen (Berechtigungsmatrix, Protokollkette, Verschlüsselung, Mandantentrennung), die regelmäßig im Entwicklungsprozess ausgeführt werden.
- Dokumentierte Sicherheitsüberprüfung der Anwendung (Application-Security-Audit, Mai 2026) ohne kritische Feststellungen; die übrigen Feststellungen wurden im Code nachweislich behoben.

Anlage 3 — Unterauftragsverarbeiter

Bei Abschluss dieser Vereinbarung sind folgende Unterauftragsverarbeiter eingesetzt:

Unternehmen	Leistung / verarbeitete Daten	Ort der Verarbeitung	Garantien bei Drittlandbezug
Vercel Inc., 440 N Barranca Ave #4133, Covina, CA 91723, USA	Hosting und Betrieb der Anwendung (Serverless-Funktionen, Auslieferung, zeitgesteuerte Jobs) sowie privater Objektspeicher für Dokumentdateien (unter Einsatz technischer Sub-Dienstleister gemäß der Subprozessorenliste des Vercel-DPA); verarbeitet werden alle über die Anwendung laufenden Daten inkl. technischer Protokolldaten	Anwendungsbetrieb: Region Frankfurt am Main (fra1); Objektspeicher: Region _____ (trägt der Auftragsverarbeiter ein)	Auftragsverarbeitungsvertrag (Data Processing Addendum) einschließlich EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO)
Neon Inc., USA (PostgreSQL-Datenbankdienst, bezogen als „Vercel Postgres powered by Neon“; maßgeblich ist die im abgeschlossenen Data Processing Agreement genannte Vertragsentität)	Betrieb der Produktionsdatenbank (sämtliche strukturierten Anwendungsdaten) einschließlich automatischer Datensicherungen	Rechenzentrumsregion Frankfurt am Main (AWS eu-central-1)	Auftragsverarbeitungsvertrag (Data Processing Agreement) einschließlich EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO)

Hinweis: Vom Verantwortlichen selbst angebundene Dienste sind keine Unterauftragsverarbeiter (§ 6 Abs. 4 der Vereinbarung).