

Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

Mustervorlage – Stand: 28.06.2026. Diese Vorlage wird bei Vertragsschluss um die kundenspezifischen Daten ergänzt und von beiden Parteien unterzeichnet.

Parteien

Auftragsverarbeiter:

Jürgen Schuster, Einzelunternehmen „Bestehia – der Prüfungssimulator“
Rößlergasse 9/3, 1230 Wien, Österreich
E-Mail: gutentag@bestehia.com · Tel.: +43 664 530 2648

Verantwortlicher (Kunde):

[Name / Firma]
[Anschrift]
[Vertretungsberechtigte Person]
[E-Mail] · [Telefon]

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus der vom Auftragsverarbeiter (im Folgenden „Bestehia“) für den Verantwortlichen (im Folgenden „Kunde“) im Rahmen des Hauptvertrags (KI-gestützte Erstellung von Lern- und Prüfungssimulationen aus vom Kunden bereitgestellten Dokumenten) erbrachten Leistungen ergeben. Sie findet Anwendung auf alle Tätigkeiten, bei denen Bestehia personenbezogene Daten im Auftrag des Kunden verarbeitet.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand: Bereitstellung einer Plattform zur KI-gestützten Erstellung interaktiver Prüfungen und Lerninhalte sowie deren Auslieferung an die vom Kunden benannten Endnutzer:innen.

(2) Dauer: Die Vereinbarung gilt für die Laufzeit des Hauptvertrags. Sie endet automatisch mit dessen Beendigung, unbeschadet fortbestehender Geheimhaltungs- und Aufbewahrungspflichten.

§ 2 Art und Zweck der Verarbeitung, Datenarten, Betroffene

Art der Verarbeitung	Erheben, Speichern, Organisieren, Verändern (KI-Generierung), Abfragen, Übermitteln per E-Mail, Löschen.
Zweck	Erstellung und Auslieferung individueller Lern-/Prüfungsinhalte aus vom Kunden bereitgestellten Quellen.
Datenarten	E-Mail-Adressen der Endnutzer:innen, von Endnutzer:innen oder Kunde hochgeladene Lerndokumente (in der Regel ohne personenbezogene Daten), generierte Lerninhalte, technische Verbindungsdaten.
Kategorien Betroffener	Endnutzer:innen des Kunden (z. B. Studierende, Mitarbeitende), Ansprechpersonen des Kunden.
Besondere Kategorien	Werden grundsätzlich nicht verarbeitet. Der Kunde stellt sicher, keine besonderen Kategorien gem. Art. 9 DSGVO hochzuladen, sofern nicht ausdrücklich gesondert vereinbart.

§ 3 Weisungsrecht des Kunden

(1) Bestehia verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Kunden, es sei denn, eine Verarbeitung ist nach Unions- oder mitgliedstaatlichem Recht erforderlich, dem Bestehia unterliegt.

(2) Mündliche Weisungen sind unverzüglich in Textform (E-Mail genügt) zu bestätigen. Bestehia informiert den Kunden unverzüglich, wenn eine Weisung nach Auffassung von Bestehia gegen datenschutzrechtliche Vorschriften verstößt.

§ 4 Technische und organisatorische Maßnahmen (TOM)

Bestehia trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO und hält diese während der Vertragslaufzeit dem Stand der Technik entsprechend aktuell. Wesentliche Änderungen werden dem Kunden vorab in Textform mitgeteilt.

§ 5 Unterauftragsverarbeiter

(1) Der Kunde stimmt der Beauftragung der in **Anlage 2** aufgeführten Unterauftragsverarbeiter zu.

(2) Bestehia informiert den Kunden über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern mindestens 30 Tage vorab in Textform. Der Kunde kann innerhalb von 14 Tagen aus wichtigem datenschutzrechtlichem Grund widersprechen. Im Falle eines berechtigten Widerspruchs sind die Parteien zur außerordentlichen Kündigung berechtigt.

(3) Bestehia verpflichtet jeden Unterauftragsverarbeiter schriftlich zu Verpflichtungen, die den Verpflichtungen aus dieser Vereinbarung im Wesentlichen entsprechen (Art. 28 Abs. 4 DSGVO).

§ 6 Drittlandübermittlung

Soweit personenbezogene Daten in ein Drittland außerhalb des EWR übermittelt werden, geschieht dies ausschließlich auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO), der EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) oder einer anderen geeigneten Garantie. Eine Übersicht aktueller Übermittlungen und Garantien ist in Anlage 2 dokumentiert.

§ 7 Pflichten des Auftragsverarbeiters

- Vertraulichkeit: Verpflichtung aller zur Verarbeitung befugten Personen auf Vertraulichkeit (Art. 28 (3) lit. b, Art. 29 DSGVO).
- Unterstützung des Kunden bei der Wahrnehmung von Betroffenenrechten (Art. 12–22 DSGVO).
- Unterstützung bei Datenschutz-Folgenabschätzungen (Art. 35) und vorheriger Konsultation (Art. 36 DSGVO).
- Unverzügliche Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33) – spätestens innerhalb von 24 Stunden ab Kenntnis.
- Führung eines Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.
- Benennung einer Kontaktperson für Datenschutzfragen: Jürgen Schuster, gutentag@bestehia.com.

§ 8 Kontrollrechte des Kunden

(1) Der Kunde hat das Recht, die Einhaltung der Vereinbarung sowie der gesetzlichen Vorschriften zu überprüfen (Art. 28 Abs. 3 lit. h DSGVO). Bestehia stellt hierfür auf Anfrage in Textform alle erforderlichen Informationen zur Verfügung.

(2) Vor-Ort-Kontrollen sind mit einer Vorankündigungsfrist von 30 Tagen während der üblichen Geschäftszeiten, höchstens einmal jährlich (außer im Fall begründeter Anlässe) zulässig. Berechtigte Aufwände können dem Kunden in Rechnung gestellt werden, wobei der Stundensatz vorab mitgeteilt wird.

(3) Anstelle eigener Kontrollen kann Bestehia aktuelle Zertifikate, Berichte von Auditoren oder Selbstauskünfte vorlegen.

§ 9 Löschung und Rückgabe nach Vertragsende

Nach Beendigung des Hauptvertrags hat Bestehia nach Wahl des Kunden alle personenbezogenen Daten zurückzugeben oder zu löschen (Art. 28 Abs. 3 lit. g DSGVO), soweit nicht gesetzliche Aufbewahrungspflichten (insb. § 132 BAO – 7 Jahre für Rechnungs- und Zahlungsdaten) entgegenstehen. Die Löschung wird dem Kunden auf Anfrage in Textform bestätigt.

§ 10 Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO sowie den Regelungen des Hauptvertrags. Bestehia haftet gegenüber dem Kunden nur für eigene schuldhafte Verstöße gegen diese Vereinbarung oder die DSGVO.

§ 11 Schlussbestimmungen

- (1) Es gilt österreichisches Recht unter Ausschluss kollisionsrechtlicher Verweisungen.
- (2) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden die unwirksame Bestimmung durch eine zulässige Regelung ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.
- (3) Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen die Regelungen dieser Vereinbarung in datenschutzrechtlichen Fragen vor.
- (4) Gerichtsstand ist Wien, soweit gesetzlich zulässig.

Verantwortlicher (Kunde)

Ort, Datum: _____

Unterschrift / Stempel:

Auftragsverarbeiter (Bestehia)

Ort, Datum: Wien, _____

Unterschrift:

Jürgen Schuster

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. Vertraulichkeit

- **Zutrittskontrolle:** Betrieb in zertifizierten EU-Rechenzentren der Unterauftragsverarbeiter (Frankfurt, EU). Kein physischer Zutritt durch Bestehia.
- **Zugangskontrolle:** Passwortgeschützte Admin-Konsole, Multi-Faktor-Authentifizierung für Administratorzugänge; Service-Konten mit individuellen Schlüsseln.
- **Zugriffskontrolle:** Row-Level-Security auf Datenbankebene; Rollenmodell mit Trennung von Endnutzer-, Admin- und Service-Rolle; Least-Privilege-Prinzip.
- **Trennungskontrolle:** Logische Mandantentrennung über Tokens und Foreign-Keys; getrennte Speicherung von Inhalten und Rechnungsdaten.
- **Pseudonymisierung:** Endnutzer-Inhalte werden über zufällig generierte Zugangstokens adressiert; keine Verknüpfung zu Profildaten.

2. Integrität

- **Weitergabekontrolle:** Transportverschlüsselung TLS 1.2+ für alle Verbindungen.
- **Eingabekontrolle:** Serverseitige Validierung aller Eingaben; Audit-Logs für sicherheitsrelevante Aktionen.

3. Verfügbarkeit und Belastbarkeit

- Tägliche automatisierte Backups der Datenbank durch den Hosting-Anbieter mit Point-in-Time-Recovery.
- Automatisches Monitoring und Alerting bei Verfügbarkeitsproblemen.
- Automatische Löschung nicht bezahlter Inhalte nach 30 Tagen; bezahlte Inhalte nach 7 Jahren.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management: Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO).
- Incident-Response: definierter Prozess zur Meldung von Datenschutzvorfällen innerhalb von 24 h.
- Auftragskontrolle: schriftliche AV-Verträge mit allen Unterauftragsverarbeitern.
- Regelmäßige Sicherheits-Reviews der eingesetzten Komponenten und Patch-Management.

Anlage 2 – Genehmigte Unterauftragsverarbeiter

Stand: 28.06.2026. Aktuelle Liste jederzeit auf Anfrage; Änderungen werden gem. § 5 angekündigt.

Anbieter / Sitz	Leistung	Verarbeitungsort	Garantie
Supabase / Lovable Cloud (Supabase Inc., USA; Hosting EU)	Hosting, Datenbank, Auth, Edge Functions	Frankfurt (EU)	Art. 28 DSGVO, SCC für Konzernzugriffe
Google LLC (über Lovable AI Gateway)	KI-Generierung (Gemini-Modelle)	EU-Gateway, Verarbeitung global	SCC + EU-US Data Privacy Framework (DPF-zertifiziert)
Resend Inc. (USA)	Transaktionaler E-Mail-Versand (notify.bestehia.com)	USA	Art. 28 DSGVO + SCC
Stripe Payments Europe Ltd. / Stripe Inc.	Zahlungsabwicklung, Rechnung	Irland; Konzernmutter USA	Art. 28 DSGVO + SCC + DPF
Intuition Machines Inc. (hCaptcha) USA	Bot-/Missbrauchsschutz Kontaktformular	USA	Art. 28 DSGVO + SCC

Hinweis: Diese Vorlage ist eine sorgfältig erstellte Mustervorlage. Für konzern- oder branchenspezifische Anforderungen passen wir den Vertrag auf Anfrage gerne an (gutentag@bestehia.com).