Vertrag zur Auftragsverarbeitung (AVV)

gemäß Art. 28 DSGVO · Version 1.0 · Stand: Juli 2026 · simplybills.de/avv

Präambel

Dieser Vertrag zur Auftragsverarbeitung (nachfolgend "AVV") wird geschlossen zwischen dem Nutzer der Plattform SimplyBills (nachfolgend "Verantwortlicher") und David Kogan IT Consulting, Engernweg 79, 33100 Paderborn (nachfolgend "Auftragsverarbeiter").

Der AVV ist gemäß § 8 der Allgemeinen Geschäftsbedingungen Bestandteil des Nutzungsvertrags über die Plattform SimplyBills. Er kommt mit Abschluss des Nutzungsvertrags zustande und bedarf keiner gesonderten Unterschrift (Art. 28 Abs. 9 DSGVO, elektronisches Format).

§ 1 Gegenstand und Dauer der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Rahmen der Bereitstellung der Plattform SimplyBills (Erstellung, Versand und Archivierung von E-Rechnungen sowie damit verbundene Funktionen). Die Dauer der Verarbeitung entspricht der Laufzeit des Nutzungsvertrags.

§ 2 Art, Zweck und Umfang der Verarbeitung

Art und Zweck der Verarbeitung ergeben sich aus dem Nutzungsvertrag: Speicherung, Strukturierung, Übermittlung (E-Mail-Versand von Rechnungen) und Archivierung von Geschäftsdaten des Verantwortlichen. Die betroffenen Datenarten und Kategorien betroffener Personen sind in Anlage 1 beschrieben.

§ 3 Weisungsrecht des Verantwortlichen

Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Die Nutzung der Plattform-Funktionen durch den Verantwortlichen gilt als Weisung. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich; er ist berechtigt, die Ausführung bis zur Bestätigung auszusetzen.

§ 4 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass sich alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

§ 5 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO und entwickelt sie unter Berücksichtigung des Stands der Technik

fort. Wesentliche Änderungen dürfen das Schutzniveau nicht unterschreiten.

§ 6 Unterauftragsverarbeiter

Der Verantwortliche erteilt die allgemeine Genehmigung zum Einsatz der in Anlage 3 aufgeführten Unterauftragsverarbeiter. Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen (Hinzuziehung oder Ersetzung) in Textform, z. B. per E-Mail; der Verantwortliche kann der Änderung innerhalb von 30 Tagen aus wichtigem datenschutzrechtlichen Grund widersprechen. Mit jedem Unterauftragsverarbeiter bestehen Verträge gemäß Art. 28 Abs. 4 DSGVO.

§ 7 Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Betroffenenrechten (Art. 12–23 DSGVO) sowie bei den Pflichten aus Art. 32–36 DSGVO (Sicherheit, Meldepflichten, Datenschutz-Folgenabschätzung). Betroffenenanfragen, die direkt beim Auftragsverarbeiter eingehen, leitet er unverzüglich an den Verantwortlichen weiter.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten, die die Auftragsdaten betreffen, unverzüglich nach Bekanntwerden und stellt die für die Meldung nach Art. 33 DSGVO erforderlichen Informationen bereit.

§ 9 Löschung und Rückgabe

Nach Beendigung des Nutzungsvertrags kann der Verantwortliche seine Daten für 30 Tage exportieren. Anschließend löscht der Auftragsverarbeiter die Auftragsdaten, spätestens 90 Tage nach Vertragsende, sofern keine gesetzliche Aufbewahrungspflicht des Auftragsverarbeiters entgegensteht.

§ 10 Nachweis und Kontrollrechte

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung dieses AVV zur Verfügung. Der Verantwortliche kann Auskünfte in Textform verlangen; Vor-Ort-Kontrollen sind nach Terminvereinbarung während der üblichen Geschäftszeiten möglich, soweit sie erforderlich sind und den Geschäftsbetrieb nicht unverhältnismäßig stören.

§ 11 Schlussbestimmungen

Es gilt deutsches Recht. Bei Widersprüchen zwischen diesem AVV und den AGB geht dieser AVV hinsichtlich datenschutzrechtlicher Regelungen vor. Sollten einzelne Bestimmungen unwirksam sein, bleiben die übrigen Bestimmungen davon unberührt.

Anlage 1: Datenarten und Kategorien betroffener Personen

Datenarten:

- Stammdaten der Kunden des Verantwortlichen (Name, Firma, Anschrift)
- Kontaktdaten (E-Mail-Adresse, Telefonnummer)

- Vertrags- und Rechnungsdaten (Rechnungsnummern, Positionen, Beträge, Zahlungsziele)
- Zahlungsinformationen (Bankverbindung, soweit auf Rechnungen angegeben)
- Inhalte hochgeladener Belege (bei Nutzung von KI-Scan)

Kategorien betroffener Personen:

- Kunden und Geschäftspartner des Verantwortlichen
- Ansprechpartner und Mitarbeiter dieser Kunden und Geschäftspartner

Anlage 2: Technische und organisatorische Maßnahmen (TOMs)

- **Zutritts- und Zugangskontrolle:** Hosting in zertifizierten EU-Rechenzentren; Zugang zu Systemen nur über personalisierte Konten mit starker Authentifizierung.
- **Zugriffskontrolle:** Mandantentrennung über Row-Level-Security (RLS) auf Datenbankebene; jeder Nutzer kann ausschließlich auf die eigenen Daten zugreifen; Zugriff auf Produktionssysteme nur für den Auftragsverarbeiter.
- **Übertragungskontrolle:** Verschlüsselte Übertragung sämtlicher Daten (TLS 1.2+); verschlüsselte Speicherung (Encryption at Rest) bei den eingesetzten Hosting-Anbietern.
- **Eingabekontrolle:** Protokollierung sicherheitsrelevanter Ereignisse und administrativer Zugriffe.
- **Verfügbarkeitskontrolle:** Tägliche automatische Backups der Datenbank; redundante Infrastruktur der Hosting-Anbieter; Fehlerüberwachung.
- **Trennungskontrolle:** Logische Trennung der Daten je Nutzerkonto; getrennte Umgebungen für Entwicklung und Produktion.
- **Datenminimierung und Löschkonzept:** Automatische Löschung von KI-Scan-Uploads nach 30 Tagen, Server-Logs nach 30 Tagen, Kontodaten spätestens 90 Tage nach Vertragsende.

Anlage 3: Unterauftragsverarbeiter

- **Supabase, Inc.** (970 Toa Payoh North #07-04, Singapur): Datenbank, Authentifizierung und Datei-Speicher. Verarbeitungsort: EU (Frankfurt am Main).
- **Hostinger International Ltd.** (61 Lordou Vironos Street, 6023 Larnaca, Zypern): Server-Hosting der Anwendung. Verarbeitungsort: EU.
- **Resend, Inc.** (2261 Market Street #5039, San Francisco, CA 94114, USA): Versand von E-Mails (z. B. E-Rechnungen an Empfänger). Übermittlung auf Basis von Standardvertragsklauseln (SCCs).
- **Mistral AI SAS** (15 rue des Halles, 75001 Paris, Frankreich): OCR-Verarbeitung hochgeladener Belege bei Nutzung von KI-Scan. Verarbeitungsort: EU.