Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

zwischen

_____

(Name/Firma des Kunden)

_____

(Anschrift)

– nachfolgend „Verantwortlicher" –

und

khuwawa-invent GmbH, Pfälzer Ufer 4, 06108 Halle (Saale)

Amtsgericht Stendal, HRB 38400, vertreten durch den Geschäftsführer Alf Kraus

– nachfolgend „Auftragsverarbeiter" –

– gemeinsam die „Parteien" –

Präambel: Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien, die sich aus der Nutzung des Dienstes „khuwawa-invoice" durch den Verantwortlichen im Rahmen des zwischen den Parteien bestehenden Nutzungsvertrags (nachfolgend „Hauptvertrag") ergeben, und gilt ergänzend zu den Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters.

§ 1 Gegenstand und Dauer der Vereinbarung

(1) Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der Nutzung des Dienstes zur Erstellung, Verwaltung und zum Versand von Rechnungen.

(2) Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags.

§ 2 Art und Zweck der Verarbeitung, Art der Daten, Kategorien betroffener Personen

(1) Art und Zweck der Verarbeitung: Speicherung, Erfassung, Verwaltung und Übermittlung von Rechnungs- und Kundendaten zum Zweck der Rechnungserstellung, -verwaltung und des -versands, einschließlich der Erzeugung elektronischer Rechnungsformate (ZUGFeRD/Factur-X) und des optionalen automatisierten Versands wiederkehrender Rechnungen per E-Mail.

(2) Art der Daten: Name, Anschrift, Kontaktdaten (E-Mail, Telefon), Bankverbindung, Rechnungs- und Zahlungsdaten, Leistungsbeschreibungen sowie sonstige vom Verantwortlichen im Rahmen der Nutzung eingegebene personenbezogene Daten.

(3) Kategorien betroffener Personen: Kunden, Ansprechpartner und sonstige natürliche Personen, deren Daten der Verantwortliche im Rahmen der Nutzung des Dienstes verarbeitet.

§ 3 Weisungsrecht des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist.

(2) Der Verantwortliche erteilt Weisungen grundsätzlich durch die Nutzung des Dienstes gemäß dessen bestimmungsgemäßer Funktionalität. Darüberhinausgehende Weisungen bedürfen der Textform.

(3) Hält der Auftragsverarbeiter eine Weisung des Verantwortlichen für rechtswidrig, teilt er dies dem

Verantwortlichen unverzüglich mit.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen dieser Vereinbarung und der Weisungen des Verantwortlichen.

(2) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Zumutbaren bei der Erfüllung von dessen Pflichten gemäß Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung).

(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Zumutbaren mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflicht des Verantwortlichen, Anträge auf Wahrnehmung der Betroffenenrechte nach Kapitel III der DSGVO zu beantworten.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die in Anhang 1 dieser Vereinbarung dargestellten technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Der Auftragsverarbeiter ist berechtigt, die technischen und organisatorischen Maßnahmen anzupassen, solange das vereinbarte Schutzniveau nicht unterschritten wird.

§ 6 Unterauftragsverhältnisse

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zur Beauftragung von Unterauftragsverarbeitern gemäß der in Anhang 2 aufgeführten Liste.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen diese Änderungen Einspruch zu erheben.

(3) Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter im Wege einer Vereinbarung zur Einhaltung der in dieser Vereinbarung genannten Pflichten.

§ 7 Kontrollrechte des Verantwortlichen

Der Verantwortliche hat das Recht, sich vor Beginn der Verarbeitung und danach regelmäßig von der Einhaltung der in dieser Vereinbarung getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu auf Anfrage die zur Kontrolle erforderlichen Informationen zur Verfügung.

§ 8 Mitteilungspflichten bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Kenntniserlangung, und unterstützt ihn im Rahmen des Zumutbaren bei der Erfüllung von dessen Meldepflichten nach Art. 33, 34 DSGVO.

§ 9 Löschung und Rückgabe von Daten

Nach Beendigung der Erbringung der Verarbeitungsleistungen ist der Auftragsverarbeiter verpflichtet, nach Wahl des Verantwortlichen sämtliche personenbezogenen Daten zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

§ 10 Haftung

Es gelten die Haftungsregelungen des Hauptvertrags (AGB des Auftragsverarbeiters), soweit diese Vereinbarung keine abweichenden Regelungen trifft. Für Schäden, die einer betroffenen Person infolge einer nicht der DSGVO entsprechenden Verarbeitung entstehen, haften die Parteien nach Maßgabe von Art. 82 DSGVO.

§ 11 Schlussbestimmungen

(1) Diese Vereinbarung unterliegt deutschem Recht.

(2) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, berührt dies die Wirksamkeit der übrigen Regelungen sowie des Hauptvertrags nicht.

(3) Bei Widersprüchen zwischen dieser Vereinbarung und Bestimmungen aus dem Hauptvertrag oder sonstigen Vereinbarungen zwischen den Parteien geht diese Vereinbarung vor, soweit es die Verarbeitung personenbezogener Daten betrifft.

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

Vertraulichkeit: Zugangskontrolle durch Authentifizierung mit gehashten Passwörtern (bcrypt); Zugriffskontrolle durch mandantengetrennte Datenhaltung auf Anwendungsebene; Übertragungskontrolle durch TLS-Verschlüsselung sämtlicher Verbindungen.

Integrität: Protokollierung sicherheitsrelevanter Vorgänge bei den eingesetzten Hosting- und Datenbankdienstleistern; kontrollierte, versionierte Softwareauslieferung.

Verfügbarkeit und Belastbarkeit: Redundante, vom Hosting- und Datenbankdienstleister betriebene Infrastruktur; regelmäßige automatisierte Datensicherungen auf Ebene des Datenbankdienstleisters.

Verfahren zur regelmäßigen Überprüfung: Regelmäßige Aktualisierung eingesetzter Software-Komponenten und Abhängigkeiten; Beschränkung des administrativen Zugriffs auf den Auftragsverarbeiter selbst.

Anhang 2 – Genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Sitz	Leistung
Vercel Inc.	USA	Hosting der Anwendung
Neon Inc.	USA	Datenbank-Hosting
Stripe Payments Europe, Ltd. / Stripe, Inc.	Irland / USA	Zahlungsabwicklung
Resend, Inc.	USA	Versand von E-Mails

Unterschriften

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Verantwortlicher	Auftragsverarbeiter (khuwawa-invent GmbH)