eRechnungTool
PDF zu E-Rechnung
BURIM KASAMI IT-DIENSTLEISTUNGEN

Norbert-Schmid-Platz 11 · 22399 Hamburg
kontakt@erechnung-tool.de
erechnung-tool.de

Auftragsverarbeitungsvertrag

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO für die Nutzung des Dienstes eRechnung Tool

ZWISCHEN

_____

Unternehmen / Behörde

_____

Straße, Hausnummer

_____

PLZ, Ort

_____

Vertreten durch

– nachfolgend **„Verantwortlicher“** –

UND

Burim Kasami, Burim Kasami IT-Dienstleistungen
Norbert-Schmid-Platz 11, 22399 Hamburg
Betreiber des Dienstes eRechnung Tool (erechnung-tool.de)
– nachfolgend **„Auftragsverarbeiter“** –

Präambel

Der Verantwortliche nutzt die Software des Auftragsverarbeiters zur automatisierten Umwandlung von Rechnungsdokumenten in strukturierte elektronische Rechnungsformate (insbesondere XRechnung und ZUGFeRD). Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten, die der Verantwortliche als Verantwortlicher im Sinne der DSGVO bereitstellt. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien nach Art. 28 DSGVO. Er gilt ergänzend zu den Nutzungsbedingungen; bei Widersprüchen in datenschutzrechtlichen Fragen geht dieser Vertrag vor.

§ 1 Gegenstand, Art, Zweck und Dauer der Verarbeitung

(1) **Gegenstand** der Verarbeitung ist die Bereitstellung der Software zur Umwandlung der vom Verantwortlichen hochgeladenen Rechnungsdokumente (PDF) in strukturierte elektronische Rechnungsformate sowie die damit verbundene automatisierte Texterkennung, Datenextraktion und Validierung, außerdem die Prüfung von E-Rechnungen im Prüflabor einschließlich des Prüfverlaufs. Der Dienst kann über die Website, per E-Mail und über das Windows-Programm „E-Rechnungsordner“ genutzt werden. Bei Nutzung des Programms übermittelt es die vom Verantwortlichen bestimmten PDF-

Rechnungen zur Umwandlung an den Dienst; die Verarbeitung erfolgt dort nach den Regelungen dieses Vertrags (insbesondere Abs. 3 und Anlage 1).

(2) **Art und Zweck** der Verarbeitung: ausschließlich automatisierte Verarbeitung der bereitgestellten Daten (Ausnahme: Rückmeldungen nach Abs. 4) zum Zweck der vom Verantwortlichen beauftragten Formatumwandlung und deren technischer Validierung. Eine Nutzung der Daten für eigene Zwecke des Auftragsverarbeiters findet nicht statt.

(3) **Dauer**: Dieser Vertrag gilt für die Dauer der Nutzung des Dienstes (Hauptvertrag) und endet mit ihr; die Pflichten nach §§ 4 und 7 gelten bis zur vollständigen Löschung fort. Bei einem schwerwiegenden Verstoß gegen diesen Vertrag kann der Verantwortliche den Hauptvertrag fristlos kündigen. Die Verarbeitung der Rechnungsinhalte erfolgt ausschließlich für die Dauer der technischen Verarbeitung; nach deren Abschluss werden die hochgeladenen Dokumente und erzeugten Ergebnisse unverzüglich gelöscht. Eine dauerhafte Speicherung der Rechnungsinhalte findet nicht statt – außer der Verantwortliche wählt im Prüflabor für einen Prüflauf ausdrücklich „Datei speichern“. Dann werden die Datei und die Meldungstexte des Prüfprogramms (beide verschlüsselt mit AES-256-GCM) für 30 Tage (Tarif Entwickler oder Business) bzw. 90 Tage (Tarif Team) ab diesem Prüflauf gespeichert; ein erneutes Prüfen verlängert die Frist nicht. Endet das Abo für das Prüflabor oder wechselt der Verantwortliche vom Tarif Team in einen kleineren Tarif, werden sie spätestens 30 Tage danach gelöscht. Geteilte Berichte gelten höchstens 30 Tage. Das Prüfergebnis ohne Werte aus der Rechnung bleibt je nach Tarif beim Anlegen des Laufs gespeichert (kostenlos die letzten 10 Läufe, höchstens 12 Monate; Tarif Entwickler oder Business 12 Monate; Tarif Team 24 Monate). Kurzzeitige, technisch erforderliche Zwischenspeicherungen während der Verarbeitung bleiben hiervon unberührt.

(4) **Support und Rückmeldungen**: Übermittelt der Verantwortliche im Einzelfall eine Rechnung zur Klärung eines Fehlers – als Anhang einer Rückmeldung im Nutzerkonto oder per E-Mail –, gilt dies als Einzelweisung. Der Auftragsverarbeiter verarbeitet diese Rechnung, auch durch persönliche Einsichtnahme, ausschließlich zur Klärung und Behebung des gemeldeten Fehlers, speichert sie in einem nicht öffentlichen Speicher und löscht sie spätestens nach 90 Tagen oder auf Verlangen des Verantwortlichen früher. Eine Verwendung für andere Zwecke findet nicht statt.

§ 2 Art der Daten und Kategorien betroffener Personen

(1) **Kategorien personenbezogener Daten** (soweit in den hochgeladenen Rechnungen enthalten): Stammdaten (Namen, Firmierungen von Einzelunternehmern/natürlichen Personen); Kontaktdaten (Anschrift, Ansprechpartner, E-Mail, Telefon); Vertrags-/ Rechnungsdaten (Leistungs- und Positionsdaten, Beträge, Daten); Bank- und Zahlungsdaten (z. B. IBAN); steuerliche Kennungen (z. B. USt-IdNr., soweit natürliche Personen).

(2) **Kategorien betroffener Personen**: Geschäftspartner des Verantwortlichen (Rechnungssteller und -empfänger, deren Ansprechpartner, Einzelunternehmer und sonstige natürliche Personen), soweit deren Daten in den verarbeiteten Dokumenten enthalten sind.

§ 3 Weisungsgebundenheit

(1) Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist gesetzlich zur Verarbeitung verpflichtet; in diesem Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(2) Die Nutzung der Funktionen der Software durch den Verantwortlichen gilt als Einzelweisung. Weisungen erfolgen im Übrigen in Textform an kontakt@erechnung-tool.de und werden dokumentiert. Weisungsberechtigt sind die Inhaber des Nutzerkontos sowie vom Verantwortlichen in Textform benannte Personen; Weisungsempfänger beim Auftragsverarbeiter ist Burim Kasami.

(3) Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtlich unzulässig, informiert er den Verantwortlichen unverzüglich und ist berechtigt, die Durchführung der Weisung bis zu ihrer Bestätigung oder Änderung auszusetzen.

§ 4 Pflichten des Auftragsverarbeiters

(1) **Vertraulichkeit**: Der Auftragsverarbeiter stellt sicher, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind (Art. 28 Abs. 3 lit. b, Art. 29, 32 Abs. 4 DSGVO).

(2) **Technische und organisatorische Maßnahmen (TOMs)**: Der Auftragsverarbeiter trifft die in Anlage 1 beschriebenen Maßnahmen nach Art. 32 DSGVO und hält diese während der Vertragsdauer auf einem dem Risiko angemessenen Stand.

(3) **Unterstützung des Verantwortlichen**: Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Zumutbaren bei der Erfüllung der Betroffenenrechte (Art. 15–22 DSGVO) sowie bei den Pflichten nach Art. 32–36 DSGVO — einschließlich der Datensicherheit (Art. 32), der Meldung von Datenschutzverletzungen (Art. 33, 34), der Datenschutz-Folgenabschätzung (Art. 35) und der vorherigen Konsultation (Art. 36). Er unterstützt den Verantwortlichen zudem bei Anfragen und Prüfungen der zuständigen Aufsichtsbehörde.

(4) **Meldung von Datenschutzverletzungen**: Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 24 Stunden, spätestens jedoch 48 Stunden nach Bekanntwerden, in Textform an die im Nutzerkonto hinterlegte E-Mail-Adresse. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO (Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen); fehlende Angaben werden unverzüglich nachgereicht. Meldungen an Aufsichtsbehörden oder Betroffene nimmt der Auftragsverarbeiter nicht ohne vorherige Weisung des Verantwortlichen vor.

(5) **Löschung/Rückgabe**: Nach Abschluss der Verarbeitung werden die Rechnungsinhalte unverzüglich gelöscht (siehe § 1 Abs. 3). Eine gesonderte Rückgabe ist aufgrund der transienten Verarbeitung nicht erforderlich; auf Wunsch bestätigt der Auftragsverarbeiter die Löschung. Ausnahme Prüflabor: Auf Wunsch gespeicherte Dateien und Meldungstexte werden nach den Fristen in § 1 Abs. 3 gelöscht, ebenso mit dem Löschen des Nutzerkontos; bis dahin kann der Verantwortliche sie herunterladen.

(6) **Nachweis**: Der Auftragsverarbeiter stellt dem Verantwortlichen die zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO erforderlichen Informationen zur Verfügung und ermöglicht Überprüfungen gemäß § 6.

(7) **Ansprechpartner, Verzeichnis, Datenschutzbeauftragter**: Ansprechpartner für Datenschutz ist Burim Kasami, kontakt@erechnung-tool.de. Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO. Ein Datenschutzbeauftragter wurde nicht bestellt, da die gesetzlichen Voraussetzungen (§ 38 BDSG) nicht vorliegen.

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt die **allgemeine schriftliche Genehmigung** (Art. 28 Abs. 2 DSGVO) zur Beauftragung der in Anlage 2 genannten Unterauftragsverarbeiter.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters mindestens 30 Tage vorab in Textform an die im Nutzerkonto hinterlegte E-Mail-Adresse und aktualisiert Anlage 2. Der Verantwortliche kann der Änderung innerhalb von 14 Tagen nach Zugang aus datenschutzrechtlichen Gründen in Textform widersprechen. Kann der Auftragsverarbeiter dem Widerspruch nicht abhelfen, ist der Verantwortliche berechtigt, den Hauptvertrag und diesen Vertrag zum Zeitpunkt des Wirksamwerdens der Änderung außerordentlich zu kündigen; bereits gezahlte Entgelte für den nicht genutzten Zeitraum werden anteilig erstattet. In

dringenden Fällen (z. B. Sicherheitsvorfall, Wegfall eines Anbieters) kann die Frist verkürzt werden; der Verantwortliche wird dann unverzüglich informiert.

(3) Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, die diesem Vertrag zugrunde liegen (Art. 28 Abs. 4 DSGVO), insbesondere auf hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes Unterauftragsverarbeiters (Art. 28 Abs. 4 Satz 2 DSGVO).

(4) **Ort der Verarbeitung**: Die Verarbeitung und Speicherung der Daten erfolgt ausschließlich in Rechenzentren in Mitgliedstaaten der EU bzw. des EWR (Anlage 2). Eine Verlagerung in ein Drittland erfolgt nur auf dokumentierte Weisung des Verantwortlichen bzw. nach dem Verfahren in § 5 Abs. 2 und nur bei Vorliegen der Voraussetzungen der Art. 44 ff. DSGVO. Soweit Unterauftragsverarbeiter mit Sitz oder Muttergesellschaft in den USA im Einzelfall Zugriff auf Daten erhalten können (z. B. Fernwartung), ist dies durch einen Angemessenheitsbeschluss (EU-US Data Privacy Framework, Art. 45 DSGVO) und/oder EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) abgesichert.

§ 6 Kontrollrechte

(1) Der Verantwortliche ist berechtigt, sich von der Einhaltung dieses Vertrags zu überzeugen. Der Auftragsverarbeiter erteilt hierzu die erforderlichen Auskünfte und weist die getroffenen Maßnahmen nach — vorrangig durch Vorlage geeigneter Dokumentation (z. B. TOM-Beschreibung, Nachweise/Zertifikate der eingesetzten Rechenzentren).

(2) Soweit der Auftragsverarbeiter aktuelle Zertifizierungen, Prüf- oder Auditberichte (z. B. ISO 27001 oder SOC 2 der eingesetzten Infrastruktur-Anbieter) zur Verfügung stellt, sollen diese Vor-Ort-Kontrollen vorrangig ersetzen.

(3) Vor-Ort-Kontrollen erfolgen mit angemessener Vorankündigung, während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs.

(4) Die Kontrollen kann der Verantwortliche selbst oder durch einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer durchführen, der kein Wettbewerber des Auftragsverarbeiters ist. Die Rechte der zuständigen Aufsichtsbehörden bleiben unberührt. Der Auftragsverarbeiter trägt seinen eigenen Aufwand; außergewöhnlichen Aufwand für Vor-Ort-Kontrollen, die nicht durch einen Verstoß veranlasst sind, kann er angemessen in Rechnung stellen.

§ 7 Löschung nach Vertragsende

Aufgrund der transienten Verarbeitung bestehen nach Beendigung des Vertrags keine beim Auftragsverarbeiter gespeicherten Rechnungsinhalte des Verantwortlichen. Ausnahme Prüflabor: Im Prüflabor auf Wunsch gespeicherte Dateien und Meldungstexte werden mit dem Löschen des Nutzerkontos gelöscht, bei Ende des Abos für das Prüflabor spätestens nach 30 Tagen; bis dahin kann der Verantwortliche sie herunterladen. Nach Wahl des Verantwortlichen werden diese Daten vor der Löschung zum Herunterladen bereitgestellt oder unmittelbar gelöscht. In den automatischen Sicherungen des Anbieters enthaltene, verschlüsselte Kopien werden mit Ablauf der Aufbewahrungsfrist dieser Sicherungen überschrieben. Ausnahme Tresor: Die verschlüsselten Tresor-Kopien bleiben bis zum Ende ihrer Aufbewahrungsfrist gesperrt gespeichert, damit der Verantwortliche seine Belege bis dahin herunterladen kann, und werden danach gelöscht; eine frühere Löschung ist technisch ausgeschlossen. Die Löschung wird auf Verlangen in Textform bestätigt. Kontodaten des Verantwortlichen werden gemäß der Datenschutzerklärung und den gesetzlichen Aufbewahrungsfristen behandelt.

§ 8 Haftung

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO; der Ausgleich zwischen den Parteien richtet sich nach Art. 82 Abs. 5 DSGVO. Haftungsbeschränkungen der Nutzungsbedingungen gelten nicht für Ansprüche betroffener Personen und nicht für Schäden, die auf einer vorsätzlichen oder grob fahrlässigen Verletzung dieses Vertrags beruhen; im Übrigen gelten sie, soweit datenschutzrechtlich zulässig.

§ 9 Schlussbestimmungen

(1) Änderungen und Ergänzungen bedürfen der Textform.

(2) Wird dieser Vertrag von beiden Parteien unterzeichnet (auch elektronisch, Art. 28 Abs. 9 DSGVO), gilt im Verhältnis zu diesem Verantwortlichen die unterzeichnete Fassung. Änderungen dieser Fassung bedürfen der Zustimmung beider Parteien in Textform; Ziffer 11 der Nutzungsbedingungen (Zustimmung durch Schweigen) findet auf diesen Vertrag keine Anwendung. Änderungen der Unterauftragsverarbeiter richten sich ausschließlich nach § 5.

(3) Bei Widersprüchen zwischen diesem Vertrag und den Nutzungsbedingungen gehen in datenschutzrechtlichen Fragen die Regelungen dieses Vertrags vor.

(4) Es gilt das Recht der Bundesrepublik Deutschland.

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

Bestandteile dieses Vertrags sind **Anlage 1** (Technische und organisatorische Maßnahmen) und **Anlage 2** (Genehmigte Unterauftragsverarbeiter).

Ort, Datum	Ort, Datum
Der Verantwortliche Name, Funktion, Unterschrift	**Der Auftragsverarbeiter** Burim Kasami, Burim Kasami IT-Dienstleistungen

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

Datenminimierung / Speicherbegrenzung: Verarbeitung der Rechnungsinhalte ausschließlich für die Dauer der technischen Verarbeitung; keine dauerhafte Speicherung; unverzügliche Löschung nach Umwandlung. Keine Protokollierung von Rechnungsinhalten. Ausnahme Prüflabor: Datei und Meldungstexte nur auf ausdrücklichen Wunsch je Prüflauf, mit festen Löschfristen und täglichem automatischem Löschlauf; ohne diesen Wunsch wird nur das Prüfergebnis ohne Werte aus der Rechnung gespeichert (u. a. Regelkennungen, Fundstellen ohne Werte, Zähler und eine Prüfsumme).

Verschlüsselung: Transportverschlüsselung (TLS) für alle Verbindungen zwischen Nutzer und Diensten. Im Prüflabor gespeicherte Dateien und Meldungstexte werden zusätzlich anwendungsseitig mit AES-256-GCM verschlüsselt; der Schlüssel wird getrennt von Datenbank und Dateispeicher verwaltet.

Verarbeitungsort: Verarbeitung in Rechenzentren innerhalb der EU: Web-Anwendung bei Vercel in Frankfurt am Main; Datenbank und Dateispeicher (alle Kontodaten sowie das Prüflabor) bei Supabase in Irland; Prüfdienst bei Hetzner in Falkenstein, Deutschland; Texterkennung wie in Anlage 2 angegeben. Die Rechenzentren sind durch die eingesetzten Infrastruktur-Anbieter nach ISO 27001 zertifiziert.

Zugriffs- und Berechtigungskontrolle: Zugriff nur für berechtigte Personen über authentifizierte, verschlüsselte Verbindungen; Rollen- und Berechtigungskonzept nach dem Prinzip der geringsten Rechte; Mehr-Faktor-Authentifizierung (MFA) für alle administrativen Zugänge zu Hosting, Datenbank, Servern und Quellcode; Verpflichtung der mit der Verarbeitung befassten Personen auf Vertraulichkeit.

Integrität: technische Validierung der erzeugten Formate gegen die offiziellen Standards (XRechnung/ZUGFeRD).

Verfügbarkeit und Belastbarkeit: Betrieb auf redundanter Cloud-Infrastruktur der eingesetzten Anbieter; Backup- Konzept für Kontodaten (Rechnungsinhalte werden nicht gespeichert – außer auf ausdrücklichen Wunsch im Prüflabor – und nicht gesondert gesichert; in den automatischen Sicherungen des Anbieters können die verschlüsselten Prüflabor-Daten bis zu deren Ablauf enthalten sein).

Betrieb und Überwachung: Patch- und Update-Management (überwiegend durch die verwalteten Cloud-Dienste); Monitoring sowie Protokollierung administrativer Zugriffe; Prozess zur Behandlung von Sicherheitsvorfällen und Datenschutzverletzungen (Incident Response) einschließlich Meldung an den Verantwortlichen.

Trennungskontrolle: Mandantentrennung in der Datenbank durch Zeilenrechte (Row Level Security); jeder Verantwortliche sieht ausschließlich eigene Daten.

Eingabekontrolle: Protokollierung von Anmeldungen und administrativen Änderungen; Rechnungsinhalte werden nicht protokolliert.

Texterkennung: Beim Dienstleister für die Texterkennung ist die Protokollierung der Eingaben abgeschaltet; die übermittelten Inhalte werden dort weder gespeichert noch zum Training von Modellen verwendet. Der Zugriff erfolgt ohne dauerhafte Zugangsschlüssel über kurzlebige, rollenbasierte Zugangsdaten.

Arbeitsplatz und Endgeräte: Administrative Zugriffe nur von Geräten mit vollständiger Datenträgerverschlüsselung, automatischer Bildschirmsperre und aktuellem Betriebssystem.

Wiederherstellbarkeit: Tägliche Sicherung der Datenbank durch den Anbieter; die Wiederherstellung wird regelmäßig geprüft.

Überprüfung: Die Wirksamkeit der Maßnahmen wird mindestens jährlich sowie anlassbezogen überprüft und dokumentiert.

Windows-Programm „E-Rechnungsordner“: Die Übertragung der Rechnungen zwischen Programm und Dienst erfolgt ausschließlich verschlüsselt (TLS) an die Adresse des Dienstes; das Anmeldefenster des Programms zeigt nur Seiten des Dienstes an. Programm-Aktualisierungen der direkten Fassung sind kryptografisch signiert und werden vor dem Einspielen geprüft. Die lokale Speicherung auf dem Rechner des Verantwortlichen (offene Aufträge mit Kopie der PDF, Liste „Zuletzt umgewandelt“, Kopien von Ausdrucken, Protokoll) liegt in dessen Verantwortung; der Auftragsverarbeiter hat darauf keinen Zugriff. Übersprungene Aufträge löscht das Programm nach 30 Tagen.

Tresor (E-Rechnungsordner, Tarife Professional und Business): Die Belege werden auf dem Rechner des Verantwortlichen mit dem offenen Verfahren age (X25519, ChaCha20-Poly1305) verschlüsselt, bevor sie ihn verlassen. Der Schlüssel liegt ausschließlich beim Verantwortlichen (Windows-Schlüsselspeicher und Ausdruck). Die Kopien werden mit Object Lock im Modus COMPLIANCE bis zum Ende der Aufbewahrungsfrist gegen Löschen und Änderung gesperrt; diese Sperre kann auch der Auftragsverarbeiter nicht aufheben. Übertragen wird direkt vom Rechner des Verantwortlichen zum Speicher (TLS); die Server des Dienstes erhalten nur Objektnamen, Größen und Fristen.

Auftragskontrolle: Abschluss von Auftragsverarbeitungsverträgen mit allen eingesetzten Unterauftragsverarbeitern; regelmäßige Überprüfung und Aktualisierung der Maßnahmen.

Anlage 2 — Genehmigte Unterauftragsverarbeiter

Verarbeitung der **Rechnungsinhalte** (Controller-Daten des Verantwortlichen):

UNTERAUFTRAGSVERARBEITER	ZWECK	VERARBEITUNGSORT	TRANSFERGRUNDLAGE
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855 Luxemburg	Automatisierte Texterkennung und Datenextraktion aus den hochgeladenen Rechnungen	Rechenzentren in der EU (Frankfurt, Irland, Paris, Stockholm, Mailand, Spanien); Zuordnung ausschließlich innerhalb der EU	Daten bleiben in der EU. Für etwaigen Zugriff aus den USA: Konzernmutter Amazon.com, Inc. nach dem EU-US Data Privacy Framework zertifiziert (Art. 45 DSGVO), zusätzlich EU-Standardvertragsklauseln (Art. 46 DSGVO)
Vercel Inc.	Bereitstellung der Webanwendung sowie Serverless-Ausführung der Anwendung	Frankfurt (EU)	US-Unternehmen; nach dem EU-US Data Privacy Framework zertifiziert (Art. 45 DSGVO), zusätzlich EU-Standardvertragsklauseln (Art. 46 DSGVO)
Supabase Inc.	Speicherung der Prüfläufe sowie der im Prüflabor auf Wunsch gespeicherten Dateien und Meldungstexte (verschlüsselt)	Irland (EU)	US-Unternehmen; nicht nach dem Data Privacy Framework zertifiziert – EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) gemäß Auftragsverarbeitungsvertrag des Anbieters
Hetzner Online GmbH	Server für unsere eigenen Dienste: Prüfung von E-Rechnungen nach dem amtlichen Regelwerk, Umwandlung in PDF/A-3, Annahme der an die Eingangsadresse gesendeten E-Mails samt Anhängen (kurzzeitige Zwischenspeicherung bis zur Weitergabe an die Web-Anwendung); Speicherung der Tresor-Kopien des E-Rechnungsordners (Tarife Professional und Business, nur wenn der Verantwortliche den Tresor einrichtet) – Belege, die vor dem Hochladen auf dem Rechner des Verantwortlichen verschlüsselt werden; weder Hetzner noch der Auftragsverarbeiter haben einen Schlüssel	Falkenstein (Deutschland)	keine Drittlandübermittlung
STRATO AG Otto-Ostrowski-Straße 7, 10249 Berlin	Versand der Antwort-E-Mails mit der erzeugten E-Rechnung (E-Mail-Eingang) sowie Betrieb des Postfachs kontakt@erechnung-tool.de, über das Weisungen und Support-Anfragen eingehen	Deutschland	keine Drittlandübermittlung

Hinweis / Abgrenzung: Die folgenden Dienstleister verarbeiten – abgesehen von der oben genannten Speicherung im Prüflabor durch Supabase – keine Rechnungsinhalte des Verantwortlichen, sondern Daten, für die der Auftragsverarbeiter selbst Verantwortlicher ist (Kontoverwaltung, Zahlung, Reichweitenmessung). Sie sind insoweit nicht Gegenstand dieses AVV, sondern in der Datenschutzerklärung dargestellt: Supabase (Kontodaten), Stripe (Zahlungsabwicklung), PostHog (cookielose Reichweitenanalyse).

Stand: Oktober 2026. Wortgleich mit der Fassung auf erechnung-tool.de/avv.