

Vereinbarung über die Auftragsverarbeitung

gemäß Art. 28 der Verordnung (EU) 2016/679 (DSGVO)

Standardfassung, Stand: 25. August 2026

zwischen

dem Unternehmen, das den Dienst e-rechnung.tools geschäftlich nutzt (bei Gegenzeichnung: das nachstehend eingetragene Unternehmen)

– nachfolgend „Verantwortlicher“ –

und

Chris Agbanyim, einzelunternehmerisch tätig unter der Bezeichnung „e-rechnung.tools“, Mittelgäustrasse 76, CH-4612 Wangen bei Olten, Schweiz

– nachfolgend „Auftragsverarbeiter“ –

Präambel

Der Verantwortliche nutzt den Dienst e-rechnung.tools (www.e-rechnung.tools) zur Konvertierung von Rechnungsdokumenten in strukturierte elektronische Rechnungsformate nach EN 16931 (XRechnung, ZUGFeRD) einschließlich zugehöriger Funktionen (Prüfung, Anzeige, optionaler Versand). Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien nach Art. 28 DSGVO. Sie ist Bestandteil der Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters und geht deren widersprechenden Regelungen vor, soweit der Datenschutz betroffen ist.

§ 1 Gegenstand, Zustandekommen und Dauer

(1) Gegenstand der Vereinbarung ist die Verarbeitung personenbezogener Daten im Rahmen der Nutzung des Dienstes e-rechnung.tools durch den Verantwortlichen. Art und Zweck der Verarbeitung, die Art der Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1.

(2) Die Vereinbarung wird in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO): Sie wird mit Beginn der geschäftlichen Nutzung des Dienstes wirksam; einer gesonderten Unterzeichnung bedarf es nicht. Auf Wunsch des Verantwortlichen können die Parteien zusätzlich eine Ausfertigung dieser Vereinbarung unterzeichnen; hierfür steht die vom Auftragsverarbeiter vorunterzeichnete Fassung zur Verfügung.

(3) Die Vereinbarung gilt für die Dauer des Nutzungsverhältnisses. Sie endet mit dessen Beendigung; § 9 gilt darüber hinaus, bis sämtliche Auftragsdaten gelöscht oder zurückgegeben sind.

§ 2 Umfang und Zweckbindung

(1) Der Auftragsverarbeiter verarbeitet die Auftragsdaten ausschließlich zur Erbringung der vereinbarten Leistungen und nach den Regelungen dieser Vereinbarung. Eine Verarbeitung zu eigenen Zwecken findet nicht statt.

(2) Die im Rahmen der Extraktion eingesetzten KI-Modelle werden nicht mit Auftragsdaten trainiert; eine Weitergabe der Auftragsdaten an den Modellanbieter erfolgt im Regelbetrieb nicht (vgl. Anlage 3).

§ 3 Weisungsrecht

(1) Der Auftragsverarbeiter verarbeitet Auftragsdaten nur auf dokumentierte Weisung des Verantwortlichen. Die Nutzung der Funktionen des Dienstes durch den Verantwortlichen und seine

berechtigten Nutzer gilt als Weisung; ergänzende Weisungen bedürfen der Textform. Ist eine ergänzende Weisung im Dienst technisch nicht umsetzbar oder für den Auftragsverarbeiter mit unverhältnismäßigem Aufwand verbunden, kann er sie ablehnen; dem Verantwortlichen bleibt in diesem Fall die Beendigung des Nutzungsverhältnisses vorbehalten.

(2) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, informiert er den Verantwortlichen unverzüglich und ist berechtigt, die Ausführung bis zur Bestätigung oder Änderung der Weisung auszusetzen.

§ 4 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass sich alle zur Verarbeitung der Auftragsdaten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 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 aufrecht.

(2) Die Maßnahmen dürfen an den Stand der Technik angepasst werden, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

§ 6 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt die allgemeine Genehmigung zum Einsatz der in Anlage 3 aufgeführten Unterauftragsverarbeiter. Die jeweils aktuelle Liste ist unter <https://www.e-rechnung.tools/sub-processors> abrufbar.

(2) Über beabsichtigte Änderungen (Hinzufügen oder Ersetzen von Unterauftragsverarbeitern) informiert der Auftragsverarbeiter durch Aktualisierung der Liste unter <https://www.e-rechnung.tools/sub-processors>. Die Aktualisierung erfolgt vor dem Wirksamwerden der Änderung; ist das aus wichtigem Grund (insbesondere Sicherheit, Verfügbarkeit oder kurzfristiger Ausfall eines Unterauftragsverarbeiters) nicht möglich, wird sie unverzüglich nachgeholt. Eine individuelle Benachrichtigung einzelner Verantwortlicher erfolgt nicht; auf Verlangen richtet der Auftragsverarbeiter für den Verantwortlichen eine E-Mail-Benachrichtigung über Änderungen ein. Widerspricht der Verantwortliche einer Änderung aus datenschutzrechtlichen Gründen innerhalb von 14 Tagen nach der Aktualisierung, kann er das Nutzungsverhältnis außerordentlich beenden; nicht verbrauchte, bezahlte Kontingente werden in diesem Fall anteilig erstattet. Widerspricht er nicht oder setzt er die Nutzung fort, gilt die Änderung als genehmigt. Ein Anspruch auf Fortführung der Verarbeitung mit einem bestimmten Unterauftragsverarbeiter besteht nicht; § 9 bleibt unberührt.

(3) Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter durch Vertrag im Wesentlichen auf die Pflichten dieser Vereinbarung, insbesondere auf hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Verstöße von Unterauftragsverarbeitern hat der Auftragsverarbeiter wie eigene zu vertreten.

§ 7 Unterstützung bei Betroffenenrechten

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten Mitteln bei der Erfüllung von Betroffenenrechten (Art. 12 bis 22 DSGVO). Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet er das Ersuchen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst, sofern keine gesetzliche Pflicht besteht. Wegen der kurzen automatisierten Speicherfristen (Anlage 1) liegen Rechnungsinhalte beim Auftragsverarbeiter im Regelfall nur für Stunden vor.

§ 8 Meldepflichten und Unterstützung (Art. 32 bis 36 DSGVO)

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten, die Auftragsdaten betreffen, unverzüglich nach Kenntniserlangung, spätestens innerhalb von 48 Stunden, mit den Angaben entsprechend Art. 33 Abs. 3 DSGVO, soweit verfügbar.

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei den Pflichten aus Art. 32 bis 36 DSGVO.

§ 9 Löschung und Rückgabe

(1) Der Dienst löscht Auftragsdaten automatisiert nach kurzen Fristen (Anlage 1); erzeugte E-Rechnungen werden dem Verantwortlichen zum Abruf bereitgestellt und nicht dauerhaft gespeichert.

(2) Nach Beendigung des Nutzungsverhältnisses löscht der Auftragsverarbeiter sämtliche noch vorhandenen Auftragsdaten, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht, und bestätigt die Löschung auf Verlangen in Textform. Abrechnungsbezogene Daten des Verantwortlichen selbst (Konto, Belege) bleiben von der Löschpflicht unberührt, soweit gesetzliche Pflichten dies erfordern.

§ 10 Nachweise und Kontrollen

(1) Der Auftragsverarbeiter weist die Einhaltung dieser Vereinbarung auf Anfrage durch geeignete Informationen nach, insbesondere durch Selbstauskünfte, die Dokumentation der Maßnahmen nach Anlage 2 sowie aktuelle Nachweise und Zertifizierungen der eingesetzten Unterauftragsverarbeiter.

(2) Darüber hinaus kann der Verantwortliche nach vorheriger Ankündigung mit angemessener Frist während der üblichen Geschäftszeiten Kontrollen durchführen oder durch einen zur Verschwiegenheit verpflichteten Dritten durchführen lassen, im Regelfall höchstens einmal jährlich sowie anlassbezogen bei konkreten Anhaltspunkten. Aufwände des Auftragsverarbeiters für Kontrollen, die über die Nachweise nach Absatz 1 hinausgehen, kann der Auftragsverarbeiter dem Verantwortlichen in angemessenem Umfang in Rechnung stellen.

§ 11 Verarbeitungsorte und Drittlandübermittlung

(1) Die Verarbeitung erfolgt im Regelbetrieb in Rechenzentren innerhalb der Europäischen Union (u. a. Frankfurt am Main) sowie in der Schweiz (Validierungsdienst, Region Zürich). Für die Schweiz besteht ein Angemessenheitsbeschluss der Europäischen Kommission; dies umfasst auch den Sitz des Auftragsverarbeiters.

(2) Rechnungsinhalte werden ausschließlich in Rechenzentren in der Europäischen Union und der Schweiz verarbeitet. Soweit einzelne Unterauftragsverarbeiter ihren Sitz in einem Drittland haben (Anlage 3), erfolgt die Verarbeitung gleichwohl in den genannten Regionen; Grundlage sind EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO).

§ 12 Haftung und Schlussbestimmungen

(1) Für die Haftung der Parteien gilt Art. 82 DSGVO.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt; an die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung.

(3) Im Übrigen gelten die Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters in ihrer jeweils gültigen Fassung.

Für den Auftragsverarbeiter:

Wangen bei Olten, den 20. August 2026

gez. Chris Agbanyim

Chris Agbanyim (e-rechnung.tools)

Für den Verantwortlichen (bei gewünschter Gegenzeichnung):

_____, den _____

(Unternehmen, Name und Funktion in Druckbuchstaben, Unterschrift)

Anlage 1: Gegenstand der Verarbeitung

Zweck und Verarbeitungen

Konvertierung vom Verantwortlichen hochgeladener Rechnungsdokumente (PDF, Word, Excel; einzeln, als Stapel oder als Sammel-PDF, optional mit beigelegten PDF-Anlagen) in E-Rechnungsformate nach EN 16931 (XRechnung, ZUGFeRD). Umfasst sind: Entgegennahme der Dokumente, automatisierte Extraktion der Rechnungsdaten, Aufbereitung und Korrektur durch den Nutzer, Erzeugung und Konformitätsprüfung der E-Rechnung, Bereitstellung zum Abruf sowie auf Veranlassung des Nutzers der Versand über das vom Verantwortlichen verbundene Microsoft-365-Postfach.

Art der personenbezogenen Daten

Rechnungsinhalte: Namen und Anschriften von Rechnungsstellern und -empfängern (z. B. Mieter, Lieferanten), Kontaktdaten von Ansprechpartnern, Rechnungs- und Referenznummern, Vertrags-, Abrechnungs- und Verbrauchsdaten, Zahlungsinformationen des Rechnungsstellers (IBAN, BIC). Daneben Konto- und Nutzungsdaten der berechtigten Nutzer des Verantwortlichen (E-Mail-Adresse, Kontingente, optional hinterlegte Stammdaten wie Ansprechpartner und Firmenlogo).

Kategorien betroffener Personen

Kunden bzw. Mieter des Verantwortlichen, Lieferanten und Dienstleister, Ansprechpartner und Beschäftigte der beteiligten Unternehmen sowie die Nutzer des Dienstes beim Verantwortlichen.

Speicher- und Löschfristen

- Verarbeitungszustände von Konvertierungsvorgängen: automatische Löschung spätestens 24 Stunden nach Erstellung.
- Für die Übernahme des Original-Layouts zwischengespeicherte Quelldateien: automatische Löschung spätestens 48 Stunden nach Upload (privater Speicher, Region Frankfurt).
- Erzeugte E-Rechnungen: Bereitstellung zum Abruf; keine dauerhafte Speicherung beim Auftragsverarbeiter.
- Konto- und Abrechnungsdaten: für die Dauer des Nutzungsverhältnisses bzw. gesetzlicher Aufbewahrungsfristen.

Hinweis zum E-Mail-Versand

Der Versand erzeugter E-Rechnungen per E-Mail erfolgt wahlweise über den Versanddienst des Auftragsverarbeiters (Scaleway Transactional Email, Verarbeitung und Versand in der EU (Frankreich)); keine dauerhafte Speicherung der Inhalte nach Zustellung, vgl. Anlage 3) oder über das vom Verantwortlichen selbst verbundene Microsoft-365-Konto; im letzteren Fall handelt Microsoft im Verhältnis zum Verantwortlichen und ist insoweit nicht Unterauftragsverarbeiter des Auftragsverarbeiters. Zugriffstoken für das Microsoft-Konto werden serverseitig gespeichert und ausschließlich für den vom Nutzer veranlassten Versand verwendet.

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

Zugangs- und Zugriffskontrolle

Zugriff auf den Dienst nur über Konto-Anmeldung (E-Mail-Einmalcodes). Serverseitige Berechtigungsprüfung bei jedem Zugriff auf Verarbeitungsvorgänge (Bindung an das jeweilige Konto); Sammel-Vorgänge sind zusätzlich an den konkreten Vorgang gebunden. Administrative Funktionen sind durch ein separates Geheimnis geschützt; administrative Änderungen werden mit Begründung protokolliert.

Übertragungs- und Transportkontrolle

Transportverschlüsselung (TLS) für sämtliche Verbindungen. Zwischengespeicherte Quelldateien liegen in einem privaten, nicht öffentlich erreichbaren Speicher (Region Frankfurt); die Auslieferung erfolgt ausschließlich über autorisierte Serverzugriffe.

Integritäts- und Eingabekontrolle

Integritätsprüfung hochgeladener Quelldateien über kryptographische Prüfsummen (SHA-256) vor der Weiterverarbeitung. Erzeugte E-Rechnungen werden gegen die amtlichen Prüfregelein (KoSIT-Validator) geprüft.

Verfügbarkeits- und Löschkontrolle

Automatisierte Löschläufe für Verarbeitungszustände (24 Stunden) und zwischengespeicherte Quelldateien (48 Stunden). Betrieb auf redundanter Cloud-Infrastruktur etablierter Anbieter; getrennte Produktions- und Vorschauumgebungen.

Trennungs- und Auftragskontrolle

Logische Trennung der Verarbeitungsvorgänge je Konto und Vorgang. Unterauftragsverarbeiter werden nach Anlage 3 gebunden; Zugriffsschlüssel folgen dem Prinzip der geringsten Berechtigung. Konfigurationsgeheimnisse werden über die Umgebungsverwaltung der Hosting-Plattform verwaltet und nicht im Quellcode abgelegt.

Anlage 3: Genehmigte Unterauftragsverarbeiter

Stand: 25.08.2026. Jeweils aktuelle Fassung: <https://www.e-rechnung.tools/sub-processors>

Unternehmen	Sitz / Ort	Leistung	Datenkategorien	Übermittlungsgrundlage
Amazon Web Services EMEA SARL (Amazon Bedrock)	Luxemburg; Verarbeitung EU (u. a. Frankfurt)	KI-gestützte Extraktion der Rechnungsdaten (keine Weitergabe an den Modellanbieter, kein Training mit Auftragsdaten)	Aus Dokumenten extrahierter Text	Verarbeitung in der EU; AWS GDPR DPA
Scaleway SAS (Transactional Email)	Frankreich; Verarbeitung und Versand EU (Paris)	E-Mail-Versand erzeugter E-Rechnungen (keine dauerhafte Speicherung nach Zustellung)	Zu versendende E-Rechnung samt Anhängen; E-Mail-Adresse des Empfängers	Verarbeitung in der EU; Scaleway DPA
Vercel Inc.	USA; Dateispeicher Region Frankfurt	Hosting, Schlüssel-Wert-Speicher (Verarbeitungszustände), Dateispeicher (Quelldateien)	Verarbeitungszustände, Quelldateien, Kontingente	EU-Standardvertragsklauseln
Oracle Corporation (Oracle Cloud)	Schweiz (Region Zürich)	Selbst betriebener KoSIT-Validierungsdienst	Erzeugte E-Rechnung (XML) zur Prüfung	Angemessenheitsbeschluss Schweiz
openiban.com	k. A.	Optionale BIC-Ermittlung, nur auf ausdrückliche Nutzeraktion	Die zu prüfende IBAN	Vertragserfüllung; Übermittlung nur auf Veranlassung

Nicht Teil der Auftragsverarbeitung: Stripe und PayPal (Zahlungsabwicklung für die eigene Abrechnung des Auftragsverarbeiters gegenüber dem Verantwortlichen), PostHog (Produktanalysen ausschließlich auf Grundlage einer Einwilligung der jeweiligen Nutzer; keine Verarbeitung von Rechnungsinhalten) sowie Resend (Versand eigener Konto- und Benachrichtigungs-E-Mails des Auftragsverarbeiters, z. B. Anmeldecodes, sowie der Rechnungen des Auftragsverarbeiters für seine eigenen Leistungen; vom Dienst erzeugte E-Rechnungen und hochgeladene Rechnungsdokumente werden darüber nicht versendet – deren Versand erfolgt über Scaleway bzw. das Microsoft-365-Konto des Verantwortlichen).