Auftragsverarbeitungsvertrag (AVV)

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DSGVO.
Stand: Mai 2026. Diese Fassung ersetzt alle vorherigen.

Inhalt:

1. Vertragsparteien

Dieser Vertrag wird geschlossen zwischen:

Verantwortlicher (im Folgenden "Auftraggeber")

Die Kanzlei oder das Unternehmen, das die Software-Dienstleistung *Rechnungs-Kontor* als angemeldete Nutzerin verwendet. Vollständige Anschrift, vertretungsberechtigte Person und Kontaktdaten werden im Unterschriftsfeld am Ende dieses Dokumentes eingetragen.

Auftragsverarbeiter (im Folgenden "Auftragnehmer")

Anbieter	Hugo Marinho, Einzelunternehmen
Anschrift	Farnsburgerstrasse 44, 4052 Basel, Schweiz
E-Mail	kontakt@rechnungs-kontor.de
Dienst	Rechnungs-Kontor (rechnungs-kontor.de)

2. Gegenstand und Dauer der Auftragsverarbeitung

Gegenstand: Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers zum Zweck der elektronischen Erfassung, Validierung, GoBD-konformen Archivierung und Aufbereitung eingehender Rechnungen der Mandanten des Auftraggebers.

Dauer: Der Vertrag beginnt mit der Anmeldung des Auftraggebers bei Rechnungs-Kontor und läuft fortlaufend bis zur Beendigung des Hauptvertrages (Schliessung des Kontos durch den Auftraggeber oder durch den Auftragnehmer aus wichtigem Grund). Die Pflichten zur Aufbewahrung von Daten nach den gesetzlichen Aufbewahrungsfristen (insbesondere § 147 AO, § 14b UStG, § 257 HGB) bleiben über das Vertragsende hinaus bestehen.

3. Zweck und Art der Verarbeitung

Die Verarbeitung erfolgt zu folgenden Zwecken:

- Empfang von eingehenden Rechnungen der Mandanten des Auftraggebers per E-Mail oder über einen persönlichen Hochladen-Link.
- Automatische Prüfung der Rechnungen auf Pflichtangaben nach § 14 UStG.
- Erkennung der strukturierten Felder per Texterkennung (OCR) und KI-basierter Klassifikation.
- Erstellung von Kontierungsvorschlägen (SKR03 / SKR04) zur Prüfung durch den Auftraggeber.
- Revisionssichere Archivierung der Originaldateien.
- Periodenverwaltung und Erzeugung von Exporten im DATEV-Format 7.00 EXTF Buchungsstapel.
- Benachrichtigung der Mandanten über den Eingang ihrer Belege.
- Benachrichtigung der Mitarbeiter des Auftraggebers über neu eingegangene Belege.

Die Verarbeitung erfolgt automatisiert. Eine ausschliesslich automatisierte Entscheidung im Sinne von Art. 22 DSGVO findet nicht statt: Kontierungsvorschläge sind Empfehlungen, die Buchung erfolgt erst nach manueller Bestätigung durch den Auftraggeber.

4. Art der personenbezogenen Daten und Kategorien Betroffener

Datenarten

- Stammdaten (Namen, Anschriften, Telefonnummern, E-Mail-Adressen) der Mandanten und ihrer Lieferanten
- Steuerliche Identifikationsmerkmale (Steuernummer, USt-IdNr.)
- Bankverbindungen, soweit auf der Rechnung enthalten
- Rechnungsdaten (Nummer, Datum, Beträge, Positionen, Leistungsbeschreibung)
- Login- und Verbindungsdaten der Mitarbeiter des Auftraggebers (IP-Adresse, Anmeldezeitpunkt, Browser-Kennung)

Betroffenenkategorien

- Mitarbeiter und vertretungsberechtigte Personen des Auftraggebers
- Mandanten des Auftraggebers (juristische und natürliche Personen)

- Mitarbeiter und Vertreter der Mandanten
- Lieferanten der Mandanten und deren Mitarbeiter (soweit auf Rechnungen genannt)

5. Pflichten des Auftragsverarbeiters

1. Die Verarbeitung erfolgt ausschliesslich auf dokumentierte Weisung des Auftraggebers. Die vertragliche Nutzung der Software durch den Auftraggeber gilt als laufende Weisung; abweichende Einzelweisungen sind in Textform zu erteilen.
2. Der Auftragnehmer setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
3. Der Auftragnehmer hält die in Abschnitt 8 und Anlage 1 beschriebenen technischen und organisatorischen Massnahmen ein und passt sie an den Stand der Technik an.
4. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen verstösst.
5. Der Auftragnehmer ist Ansprechpartner für Datenschutz und stellt dem Auftraggeber die nach Art. 28 Abs. 3 DSGVO erforderlichen Informationen zur Verfügung.
6. Der Auftragnehmer führt ein Verzeichnis aller Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt es auf Anfrage zur Verfügung.

6. Pflichten des Verantwortlichen

1. Der Auftraggeber bleibt allein verantwortlich für die Rechtmässigkeit der Verarbeitung und die Wahrung der Rechte der Betroffenen.
2. Der Auftraggeber sorgt dafür, dass seine Mandanten über die Verarbeitung ihrer Daten durch Rechnungs-Kontor informiert werden, soweit eine entsprechende Informationspflicht nach Art. 13 / Art. 14 DSGVO besteht.
3. Der Auftraggeber benennt einen oder mehrere Ansprechpartner für Datenschutzfragen. Für Konten auf Rechnungs-Kontor gilt die im Konto hinterlegte E-Mail-Adresse als Ansprechperson, sofern keine abweichende Adresse mitgeteilt wurde.

7. Unter-Auftragsverarbeiter

Der Auftraggeber gestattet dem Auftragnehmer den Einsatz von Unter-Auftragsverarbeitern. Eine vollständige Liste mit Anschrift, Standort und Verarbeitungszweck findet sich in Anlage 2 dieses Vertrages. Der Auftragnehmer informiert den Auftraggeber rechtzeitig vor der Einbeziehung weiterer oder dem Wechsel von Unter-Auftragsverarbeitern. Der Auftraggeber kann der Änderung innerhalb von 30 Tagen widersprechen; bei berechtigtem Widerspruch kann der Auftraggeber den Hauptvertrag ausserordentlich kündigen.

Der Auftragnehmer schliesst mit allen Unter-Auftragsverarbeitern eine Vereinbarung, die im Wesentlichen die Verpflichtungen dieses Vertrages spiegelt.

8. Technische und organisatorische Massnahmen (TOMs)

Der Auftragnehmer setzt geeignete technische und organisatorische Massnahmen nach Art. 32 DSGVO um. Eine detaillierte Beschreibung findet sich in Anlage 1. Wesentliche Massnahmen:

- Vertrauliche Übertragung (TLS) auf allen Kommunikationswegen
- Speicherung der Datenbank und der Originaldateien in Deutschland (Hetzner Online GmbH, Nürnberg)
- Datenbankzugang ausschliesslich über verschlüsselten Cloudflare-Tunnel; kein öffentlicher Datenbank-Port
- Passwörter werden mit PBKDF2-SHA256 nach NIST-Mindestvorgaben gehasht
- Optionale Zwei-Faktor-Authentifizierung nach RFC 6238 (TOTP)
- Brute-Force-Schutz auf Anwendungs- und Edge-Ebene
- Hash-verkettetes Audit-Log für alle sicherheitsrelevanten Aktionen
- Rollenmodell mit feingranularen Berechtigungen pro Mitglied
- Versionierte Object-Storage-Speicherung der Originaldateien (Inhaltsadressierung über SHA-256)

9. Unterstützung bei Betroffenenrechten

Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Betroffenenrechte nach Art. 12 bis Art. 22 DSGVO. Für das Konto des Auftraggebers selbst stehen folgende Selbstbedienungs-Funktionen zur Verfügung:

- **Art. 15 (Auskunft) und Art. 20 (Datenübertragbarkeit)**: Unter *Einstellungen* → *Datenschutz-Rechte* → *Datenexport herunterladen*. Ergebnis: maschinenlesbare JSON-Datei mit Profil, Kanzlei, Mandanten, Beleg-Metadaten, Audit-Einträgen, Anmeldeversuchen.
- **Art. 16 (Berichtigung)**: Profil-, E-Mail- und Mandanten-Kontaktdaten sind in den Einstellungen jederzeit änderbar.
- **Art. 17 (Löschung)**: Unter *Einstellungen* → *Datenschutz-Rechte* → *Konto schliessen*. Soweit gesetzliche Aufbewahrungsfristen entgegenstehen (10 Jahre nach § 147 AO, § 14b UStG, § 257 HGB), bleiben die betreffenden Daten bis zum Ablauf der Frist gespeichert.
- **Art. 21 (Widerspruch)**: Jede Routinemail enthält einen Abmeldelink nach RFC 8058.

Für Anfragen, die das Konto betreffende Mandanten oder deren Mitarbeiter erfasst, richtet sich der Auftraggeber zunächst an den Auftragnehmer. Der Auftragnehmer antwortet in der Regel innerhalb eines Werktages.

10. Meldung von Datenschutzverletzungen

Der Auftragnehmer benachrichtigt den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 48 Stunden, über Verletzungen des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO. Die Benachrichtigung enthält mindestens:

- Eine Beschreibung der Art der Verletzung
- Die betroffenen Kategorien und ungefähre Anzahl betroffener Personen

- Die betroffenen Kategorien und ungefähre Anzahl betroffener Datensätze
- Die wahrscheinlichen Folgen
- Die ergriffenen oder vorgeschlagenen Massnahmen zur Eindämmung

Die Meldepflicht des Auftraggebers gegenüber der zuständigen Aufsichtsbehörde nach Art. 33 DSGVO und gegenüber den Betroffenen nach Art. 34 DSGVO bleibt unberührt.

11. Kontrollrechte und Audits

Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zur Verfügung, um die Einhaltung der in diesem Vertrag festgelegten Pflichten nachzuweisen. Der Auftragnehmer ermöglicht Audits durch den Auftraggeber oder einen vom Auftraggeber beauftragten Prüfer. Audits werden mit einer angemessenen Frist (mindestens 30 Tage) angekündigt, finden während der Geschaeftszeiten statt und dürfen den Betrieb nicht unverhältnismässig beeinträchtigen. Kosten eines durch den Auftraggeber initiierten Audits trägt der Auftraggeber.

Soweit der Auftragnehmer eine anerkannte unabhängige Prüfung (z. B. IDW PS 880 Softwarebescheinigung) vorlegen kann, genügt deren Prüfbericht zur Erfüllung der Nachweispflicht.

12. Beendigung des Vertrages und Rückgabe / Löschung

Nach Beendigung des Hauptvertrages stellt der Auftragnehmer dem Auftraggeber die Daten in einem gängigen, maschinenlesbaren Format zur Verfügung (siehe Abschnitt 9, Datenexport). Nach erfolgter Bereitstellung und nach Wahl des Auftraggebers werden die Daten gelöscht oder vernichtet, soweit nicht gesetzliche Aufbewahrungsfristen entgegenstehen. Insbesondere bleiben archivierte Rechnungen für die Dauer der gesetzlichen Frist von zehn Jahren erhalten.

13. Fortbestand der Daten bei Geschäftsaufgabe oder Insolvenz

Der Auftragnehmer trifft die folgenden Vorkehrungen, damit der Auftraggeber auch im Falle einer Geschäftsaufgabe, einer Liquidation oder einer Insolvenz des Auftragnehmers ohne Datenverlust auf seine archivierten Belege und Buchungsstapel zugreifen und seinen gesetzlichen Aufbewahrungspflichten nach § 147 AO, § 14b UStG und § 257 HGB nachkommen kann:

1. **Vorankündigung.** Der Auftragnehmer informiert den Auftraggeber bei einer planmässigen Geschäftsaufgabe mit einer Frist von mindestens 90 Tagen vor Abschaltung des Dienstes per E-Mail an die im Konto hinterlegte Adresse. Bei einer Insolvenz erfolgt die Information unverzüglich nach Kenntnis des Auftragnehmers, spätestens jedoch mit der Insolvenzeröffnung.
2. **Datenherausgabe in offenen Formaten.** Der Auftraggeber kann jederzeit, spätestens bis zum Ende der Vorankündigungsfrist, einen vollständigen Datenexport auslösen. Dieser umfasst: die Originaldateien der Belege (PDF, XML, Bilddateien), die strukturierten Metadaten als JSON, die Buchungsstapel im DATEV-Format 7.00 EXTF (Windows-1252, Semikolon, CRLF), die Vorsteuer-Aufstellungen je Periode, sowie das vollständige Sicherheits-Protokoll (Audit-Log) mit zugehörigen OpenTimestamps-Quittungen. Der Export erfolgt über den Endpunkt `/api/account/export` sowie über die monatlichen ZIP-Übergabe-Pakete je Mandant. Sämtliche Formate sind herstellerunabhängig und ohne Zugang zur Software des Auftragnehmers les- und importierbar.

3. **Unabhängige Prüfbarkeit.** Die im Audit-Log enthaltene SHA-256-Hash-Kette wird einmal täglich in der Bitcoin-Blockchain über das offene OpenTimestamps-Protokoll verankert (siehe Abschnitt 8 sowie der öffentliche Endpunkt `/integrity`). Diese Verankerung ist auch nach Geschäftsaufgabe des Auftragnehmers durch jeden unabhängigen Bitcoin-Knoten oder Block-Explorer prüfbar. Die Quittungen sind Teil jedes ZIP-Übergabe-Paketes und somit eigenständig nutzbar.
4. **Bezugsquelle der Originaldateien.** Die Belege selbst liegen ausschliesslich in dem S3-kompatiblen Objektspeicher der Hetzner Online GmbH, Nürnberg. Die Zugangsdaten zu diesem Bucket können im Falle einer geordneten Geschäftsaufgabe nach Wahl des Auftraggebers in eine vom Auftraggeber selbst betriebene oder durch einen Dritten betriebene Storage-Lokation verlagert werden, ohne dass eine Migration der Dateien notwendig ist.
5. **Insolvenzverwalter / Sachwalter.** Im Falle einer Insolvenz hat der Insolvenzverwalter (bzw. Sachwalter) gegenüber den Auftraggebern dieselbe Mitwirkungspflicht hinsichtlich der Datenherausgabe wie der Auftragnehmer. Diese Pflicht ergibt sich bereits unmittelbar aus Art. 28 Abs. 3 lit. g DSGVO sowie aus den handels- und steuerrechtlichen Aufbewahrungspflichten des Auftraggebers, ist aus Klarheitsgründen hier jedoch ausdrücklich vereinbart.

14. Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform.
2. Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam. Anstelle der unwirksamen Bestimmung gilt eine wirksame Bestimmung, die dem Sinn und Zweck der unwirksamen Bestimmung wirtschaftlich am nächsten kommt.
3. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Ausschliesslicher Gerichtsstand ist Basel, Schweiz, soweit gesetzlich zulässig.
4. Im Falle von Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrages vor.

Unterschriften

Mit der Unterzeichnung erklären beide Parteien ihr Einverständnis mit dem Inhalt dieses Vertrages.

Auftraggeber (Verantwortlicher)

Kanzlei: _____

Anschrift: _____

Vertretungsberechtigte Person: _____

_____

Ort, Datum, Unterschrift

Auftragnehmer (Auftragsverarbeiter)

Anbieter: Hugo Marinho

Anschrift: Farnsburgerstrasse 44, 4052 Basel, Schweiz

_____

Ort, Datum, Unterschrift

Anlage 1: Detaillierte technische und organisatorische Massnahmen

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Zutrittskontrolle:** Rechenzentrum Hetzner Online GmbH, Nürnberg, Deutschland, mit zertifizierten Zugangsmassnahmen (ISO 27001).
- **Zugangskontrolle:** Login mit E-Mail und Passwort (PBKDF2-SHA256, NIST-Mindestvorgaben), optionale Zwei-Faktor-Authentifizierung (TOTP), Anmeldesperre nach fünf Fehlversuchen je E-Mail, zusätzliches Rate-Limit pro IP-Adresse am Cloudflare-Edge.
- **Zugriffskontrolle:** Rollenmodell mit Inhaber- und Mitglieder-Rollen sowie vier feingranularen Berechtigungs-Schaltern (Mandanten anlegen, Periode abschliessen, Export, Kontierung).
- **Trennungskontrolle:** Jede Kanzlei arbeitet auf eigener logischer Trennung; Mandanten- und Belegdaten sind über die Kanzlei-Zugehörigkeit gefiltert.
- **Pseudonymisierung:** Belegdateien sind über ihren SHA-256-Hash adressiert, ohne Bezug zur ursprünglichen Dateiverwaltung.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Hash-verkettetes Audit-Log: jede Zeile referenziert die vorherige mit SHA-256.
- Täglicher externer Zeitanker der Audit-Log-Hash-Kette per OpenTimestamps mit Verankerung in der Bitcoin-Blockchain. Nachweis nachträglicher Manipulation ist gegenüber Aufsichtsbehörden und Auditor:innen ohne zusätzliches Vertrauen in den Auftragsverarbeiter prüfbar. Sämtliche Anker mit Quittung und Anleitung zur Selbstüberprüfung öffentlich abrufbar unter rechnungs-kontor.de/integrity.
- Postgres-Trigger sperren Belege in abgeschlossenen Buchhaltungs-Perioden vor Änderungen.
- Webhook-Validierung mittels HMAC-Signatur (Mailgun, Stripe).

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Tägliche logische Datenbanksicherungen (`pg_dump` , Custom-Format), vor Upload mit GnuPG (AES-256, symmetrisch) verschlüsselt, Übertragung in einen separaten Hetzner-Object-Storage-Bucket mit dedizierten Zugangsdaten. Aufbewahrung: 30 tägliche, 12 wöchentliche, 24 monatliche Sicherungen.
- Wöchentlich automatisierter Wiederherstellungstest: Jeden Sonntag wird die jüngste Sicherung entschlüsselt und in einer temporären Datenbank wiederhergestellt; die Audit-Log-Hash-Kette wird gegen den Live-Zustand verifiziert.
- Ergänzend tägliche Hetzner-Cloud-Snapshots der Server-Instanz mit 7-Tage-Rotation.
- Versionierung des Object-Storage-Buckets. Object Lock im COMPLIANCE-Modus mit 10-Jahres-Vorhaltefrist wird zum Produktionsstart aktiviert.
- Edge-Verteilung über Cloudflare zur Bewältigung von Lastspitzen.

Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- Datenbank im Ruhezustand verschlüsselt: LUKS2-Container auf dedizierter Hetzner-Cloud-Volume (AES-XTS-Plain64, 512-Bit-Schlüssel, SHA-256, 4-KB-Sektoren). Entsperrung beim Systemstart über eine schreibgeschützte Schlüsseldatei.

- Originaldateien im Object Storage: Server-seitige Verschlüsselung durch Hetzner. Eine zusätzliche kundenseitige Verschlüsselung mit von Rechnungs-Kontor verwalteten Schlüsseln (SSE-C) wird zum Produktionsstart ergänzt.
- Sicherungen werden vor dem Upload mit GnuPG (AES-256) lokal verschlüsselt; der Schlüssel ist ausschliesslich der verantwortlichen Person bekannt.
- TLS 1.2 / 1.3 für alle Verbindungen.
- Verschlüsselter Cloudflare-Tunnel zum Datenbank-Server; kein öffentlicher Datenbank-Port.

Verfahren zur regelmässigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Automatisierte Tests (311 Unit-Tests, Stand 2026-05-21).
- Preflight-Prüfungen vor jedem Deploy (Tests, Em-Dash, Datenbank-Berechtigungen).
- Live-Smoke-Tests für die kritischen Pfade.

Anlage 2: Vollständige Subprozessoren-Liste

Stand: Mai 2026. Änderungen werden mit angemessener Vorankündigung mitgeteilt; siehe Abschnitt 7.

UNTERNEHMEN	SITZ	ZWECK	STANDORT DER VERARBEITUNG
Hetzner Online GmbH	Gunzenhausen, Deutschland	Datenbank, Originaldateien, Server-Infrastruktur	Nürnberg, Deutschland
Cloudflare, Inc.	San Francisco, USA	Edge-Auslieferung, WAF, Tunnel zur Datenbank, DNS	EU-Rechenzentren (insbesondere Frankfurt), Standardvertragsklauseln
Mailgun Technologies, Inc.	San Antonio, USA (EU-Servicebetrieb)	Empfang eingehender E-Mails der Mandanten	Belgien
Resend, Inc.	San Francisco, USA (EU-Servicebetrieb)	Versand transaktionaler E-Mails	Irland
Mistral AI SAS	Paris, Frankreich	OCR und KI-Klassifikation eingehender Belege; keine Modelltrainings-Nutzung der Kundendaten	Frankreich
Stripe Payments Europe Ltd.	Dublin, Irland	Zahlungsabwicklung, Rechnungsstellung	Irland; Standardvertragsklauseln für etwaige Konzernweitergaben

Diese Fassung des AVV wurde am 21. Mai 2026 erstellt. Eine versionierte Historie kann auf Anfrage bereitgestellt werden.