Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

zwischen

dem Kunden gemäß Hauptvertrag (Registrierung auf kud.tax)

– nachfolgend „Verantwortlicher“ –

und

KudTax GmbH, Mertensstr. 26, 13587 Berlin, eingetragen beim Amtsgericht Charlottenburg, HRB 272323 B

– nachfolgend „Auftragsverarbeiter“ –

§ 1 Gegenstand und Dauer der Verarbeitung

1. Dieser Vertrag regelt die Verarbeitung personenbezogener Daten gemäß Art. 28 DSGVO durch den Auftragsverarbeiter im Auftrag des Verantwortlichen.

2. Die Verarbeitung erfolgt ausschließlich zur Erfüllung der im Hauptvertrag definierten Leistungen (Abrechnung, Reporting, Datenvalidierung, Matching, Berechnung, Export sowie weitere definierte Funktionsbausteine gemäß der Leistungsbeschreibung des Hauptvertrags/der AGB).

3. Die Dauer dieses Vertrags entspricht der Laufzeit des Hauptvertrags.

§ 2 Art der Daten und Kategorien betroffener Personen

1. Der Auftragsverarbeiter verarbeitet folgende Kategorien personenbezogener Daten:

- Endkundendaten (z. B. Namen, Adressen, Kontakt- oder Transaktionsdaten, soweit erforderlich)
- Transaktionsdaten, Retoureninformationen und plattformspezifische Abrechnungsdaten
- technische Daten (z. B. Protokolle, IDs)

2. Kategorien betroffener Personen:

- Endkunden des Verantwortlichen
- Ansprechpartner beim Verantwortlichen (geschäftliche Kontaktdaten)

§ 3 Umfang, Zweck und Weisungsbindung

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Leistungen und gemäß dokumentierter Weisungen des Verantwortlichen.

2. Der Verantwortliche kann Weisungen jederzeit in Textform erteilen.

3. Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen unverzüglich zu informieren, wenn er der Ansicht ist, dass eine Weisung gegen Datenschutzrecht verstößt.

§ 4 Technische und organisatorische Maßnahmen (TOMs)

1. Der Auftragsverarbeiter verpflichtet sich zur Einhaltung der in Anhang 1 beschriebenen technischen und organisatorischen Maßnahmen (Art. 32 DSGVO).

2. Zu den implementierten Maßnahmen gehören insbesondere:

- Transportverschlüsselung (TLS)

- verschlüsselte Speicherung produktiver Daten
- rollen- und berechtigungsbasiertes Zugriffskonzept (least privilege)
- Protokollierung sicherheitsrelevanter Systemereignisse
- regelmäßige Backups
- systemseitige Nachvollziehbarkeit (GoBD-Aspekte)

3. Änderungen an den TOMs, die das Sicherheitsniveau nicht reduzieren, bleiben dem Auftragsverarbeiter vorbehalten.

§ 5 Unterauftragsverarbeiter

1. Der Verantwortliche erteilt die allgemeine Genehmigung zur Einschaltung der in Anlage 2 aufgeführten Unterauftragsverarbeiter (Art. 28 Abs. 2 DSGVO).

2. Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen (Hinzuziehung oder Ersetzung) mindestens 30 Tage vor Wirksamwerden in Textform. Der Verantwortliche kann aus wichtigem datenschutzrechtlichen Grund innerhalb von 14 Tagen widersprechen; gelingt keine zumutbare Lösung, ist jede Partei zur außerordentlichen Kündigung des Hauptvertrags berechtigt.

3. Der Auftragsverarbeiter stellt sicher, dass Unterauftragsverarbeiter vertraglich mindestens das gleiche Datenschutzniveau gewährleisten.

§ 6 Rechte des Verantwortlichen

Der Verantwortliche hat das Recht:

- Auskünfte zu erhalten,
- Prüfungen/Audits nach Ankündigung durchzuführen,
- TOMs zu kontrollieren,
- Weisungen zu erteilen,
- Datenlöschung zu verlangen (sofern keine gesetzlichen Aufbewahrungspflichten bestehen).

§ 7 Meldung von Datenschutzverletzungen

1. Bei einer Verletzung des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter diese unverzüglich – spätestens innerhalb von 24 Stunden – an den Verantwortlichen.

2. Die Meldung enthält alle nach Art. 33 DSGVO geforderten Informationen.

§ 8 Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei:

- der Erfüllung von Betroffenenrechten (Art. 12–23 DSGVO),
- Datenschutz-Folgenabschätzungen (Art. 35 DSGVO),
- Meldungen an Aufsichtsbehörden (Art. 33, 34 DSGVO),
- technischen Fragestellungen, soweit möglich und zumutbar.

§ 9 Löschung und Rückgabe der Daten

1. Der Auftragsverarbeiter verfügt über ein internes Lösch- und Aufbewahrungskonzept gemäß DSGVO (§ 13).

2. Auf Anfrage stellt der Auftragsverarbeiter dem Verantwortlichen eine übersichtsartige Beschreibung der Löschprozesse und Fristen bereit. Interne Sicherheits- oder Betriebsdokumentationen werden nicht herausgegeben.

3. Nach Vertragsende werden personenbezogene Daten gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten bestehen.

4. Eine langfristige Archivierung (z. B. 10-Jahres-Archiv) kann als zubuchbares Add-on beauftragt werden.

5. Die gesetzliche Aufbewahrungspflicht des Verantwortlichen bleibt unberührt.

§ 10 Vertraulichkeit

1. Der Auftragsverarbeiter stellt sicher, dass alle mit der Verarbeitung betrauten Personen zur Vertraulichkeit verpflichtet sind.

2. Etwaige gesondert geschlossene Geheimhaltungsvereinbarungen bleiben unberührt.

§ 11 Datenschutzkontrollen

1. Der Verantwortliche ist berechtigt, Audits oder Kontrollen nach vorheriger Abstimmung durchzuführen.

2. Der Auftragsverarbeiter führt interne Kontrollen, Monitoring und revisionssichere Protokollierung (SIEM-fähige Logs, soweit implementiert) durch.

§ 12 Mitteilungspflichten

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über:

- schwerwiegende technische Ereignisse,
- Sicherheitsvorfälle,
- wesentliche Änderungen an den TOMs,
- geplante Änderungen bei Unterauftragsverarbeitern.

§ 13 Lösch- und Aufbewahrungskonzept (Löschkonzept)

1. Grundsatz: KudTax verarbeitet personenbezogene Daten ausschließlich gemäß den Weisungen des Verantwortlichen und löscht oder anonymisiert diese nach Ablauf der vereinbarten Aufbewahrungsfristen oder auf dokumentierte Weisung des Verantwortlichen.

2. Löschfristen — sofern der Verantwortliche keine abweichenden Weisungen erteilt, gelten folgende Standardfristen:

- Produktive Daten (Transaktionen, Endkundendaten, Plattformdaten): Löschung innerhalb von 90 Tagen nach Beendigung des Hauptvertrags;
- Protokolldaten (Logs) gemäß TOMs: Aufbewahrung max. 180 Tage, anschließend automatische Löschung oder Anonymisierung;
- Backups: automatische Löschung nach 30 Tagen gemäß dem Backup-Rolling-Schema.

3. Sofortige Löschung auf Weisung: Der Verantwortliche kann jederzeit eine vorzeitige Löschung bestimmter Daten anweisen, sofern gesetzliche Aufbewahrungspflichten nicht entgegenstehen. KudTax bestätigt die Umsetzung schriftlich.

4. Aussetzung der Löschung: Teilt der Verantwortliche mit, dass Daten für rechtliche Auseinandersetzungen, steuerliche Prüfungen oder betriebswirtschaftliche Analysen benötigt werden, wird die Löschung bis zur Aufhebungsmitteilung ausgesetzt.

5. Nachweis & Dokumentation: KudTax dokumentiert Löschvorgänge intern und stellt auf Anfrage einen Nachweis über durchgeführte Löschungen bereit.

6. Technische Umsetzung: Die Löschung erfolgt nach Stand der Technik, u. a. durch physische, logische oder kryptografische Löschung (bei verschlüsselter Speicherung). Eine Wiederherstellung nach Abschluss des Löschvorgangs ist nicht möglich.

§ 14 Haftung

1. Die Haftung richtet sich nach den Regelungen des Hauptvertrags. Eine über den Hauptvertrag hinausgehende Haftung wird durch diesen AVV nicht begründet.

2. Der Auftragsverarbeiter haftet dem Verantwortlichen nur für Verstöße gegen Datenschutzrecht oder diesen Vertrag, soweit er diese mindestens fahrlässig verursacht hat.

3. Eine Freistellung von Bußgeldern erfolgt nicht, da diese nach DSGVO grundsätzlich den Verantwortlichen treffen.

4. Bei Mitverschulden haften beide Parteien anteilig (§ 254 BGB).

§ 15 Beendigung des Vertrags

1. Nach Vertragsende sind personenbezogene Daten gemäß § 9 zu löschen oder zurückzugeben.

2. Der Auftragsverarbeiter ist nicht berechtigt, Daten ohne Weisung aufzubewahren.

§ 16 Schlussbestimmungen

1. Änderungen des Verarbeitungsgegenstandes oder Verfahrensänderungen, einschließlich Nebenabreden, sind zwischen dem Verantwortlichen und dem Auftragsverarbeiter vorab abzustimmen und schriftlich oder in dokumentierter elektronischer Form festzuhalten.

2. Vereinbarungen zu den technischen und organisatorischen Maßnahmen (TOMs) sowie etwaige Kontroll- und Prüfungsunterlagen (einschließlich Unterlagen zu Unterauftragsverarbeitern) sind von beiden Parteien für die Dauer ihrer Gültigkeit sowie darüber hinaus für drei volle Kalenderjahre aufzubewahren, soweit keine längeren gesetzlichen Aufbewahrungsfristen bestehen.

3. Sollte das Eigentum oder die beim Auftragsverarbeiter verarbeiteten personenbezogenen Daten des Verantwortlichen durch Maßnahmen Dritter gefährdet werden (z. B. Pfändung, Beschlagnahme, Insolvenzverfahren oder sonstige Eingriffe), informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, sofern dem keine gesetzlichen Vorgaben entgegenstehen.

4. Die Einrede des Zurückbehaltungsrechts nach § 273 BGB ist hinsichtlich der im Auftrag des Verantwortlichen verarbeiteten Daten sowie der entsprechenden Datenträger ausgeschlossen. Dies gilt nicht für andere vertragliche oder gesetzliche Ansprüche des Auftragsverarbeiters.

5. Sollten einzelne Bestimmungen dieses Vertrags unwirksam oder nicht durchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Regelungen unberührt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck der ursprünglichen Regelung möglichst nahe kommt.

§ 17 Elektronischer Vertragsschluss

1. Dieser AVV wird im Rahmen des Registrierungsprozesses auf kud.tax in elektronischer Form (Textform) geschlossen. Die dokumentierte Annahme (Zeitstempel, akzeptierte Fassung) ersetzt die Unterschrift.

2. Die jeweils gültige Fassung wird dem Verantwortlichen dauerhaft abrufbar bereitgestellt.

Anhang 1 – Technische und organisatorische Maßnahmen (TOM)

§ 1 Verschlüsselung

Sämtliche Client-Server-Kommunikation wird über HTTPS verschlüsselt, um sicherzustellen, dass sensible Informationen wie Benutzerpasswörter und Zugangsdaten sicher übertragen werden. Darüber hinaus werden diese Zugangsdaten verschlüsselt im System gespeichert, um unbefugten Zugriff zu verhindern.

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

Zutrittskontrolle: Es ist kein unbefugter Zutritt zu Datenverarbeitungsanlagen möglich. Dies wird wie folgt sichergestellt (ausgeführt durch Hetzner Online GmbH):

- Elektronisches Zutrittskontrollsystem mit Protokollierung
- Dokumentierte Vergabe von Zutrittsmedien
- Flächendeckende Videoüberwachung
- Richtlinie zum Besuchermanagement
- Hochsicherheitszaun mit Übersteig- & Untergrabeschutz um das gesamte Datacenter
- Separierte Colocation-Bereiche mit abschließbaren Racks

Mehr Informationen: https://docs.hetzner.com/de/general/others/technical-and-organizational-measures/

Keine unbefugte Systembenutzung — verhindert durch:

- (sichere) verschlüsselte Kennwörter,
- automatische Sperrmechanismen,
- Zwei-Faktor-Authentifizierung

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

Weitergabekontrolle: Unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport wird verhindert durch: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

Eingabekontrolle: Aktivitäten im System werden in einem festen Modell in der Datenbank gespeichert und können zurückverfolgt werden.

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

- Backup-Strategie (online/offline),
- unterbrechungsfreie Stromversorgung (USV),
- Virenschutz, Firewall,
- rasche Wiederherstellbarkeit,
- Zutrittskontrollen mit einem Höchstmaß an Sicherheit (ISO/IEC 27001)

§ 5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DSGVO)

Datenschutz-Management: KudTax führt regelmäßige interne Datenschutz-Audits durch, dokumentiert Verarbeitungstätigkeiten nach Art. 30 DSGVO und schult Mitarbeitende jährlich.

Incident-Response-Management: etabliert, inkl. interner Meldewege, Protokollierung, Risikobewertung und fristgerechter Meldung innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde sowie Information der betroffenen Kunden.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO): Es werden ausschließlich die für den jeweiligen Verarbeitungszweck erforderlichen Daten erhoben. Zugriffsrechte werden strikt nach dem Need-to-know-Prinzip vergeben. Alle Daten werden standardmäßig verschlüsselt gespeichert und übertragen. Die Verarbeitung erfolgt ausschließlich innerhalb der zentralen Datenbank; ein Export oder eine Speicherung auf lokalen Endgeräten ist ausgeschlossen (außer physisches Backup). Der Zugriff auf die Daten ist nur über das interne VPN möglich; externe Zugriffe ohne VPN werden blockiert.

Auftragskontrolle: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

§ 6 Wiederherstellung der Verfügbarkeit nach einem Zwischenfall

Die Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall wird durch Speicherung der Daten in einem physischen und virtuellen Backup gewährleistet.

§ 7 Dokumente zu den technisch-organisatorischen Maßnahmen

Es liegen schriftlich vor: interne Verhaltensregeln, Risikoanalyse, allgemeine Datensicherheitsbeschreibung, umfassendes Datensicherheitskonzept.

Anlage 2 – Genehmigte Unterauftragsverarbeiter

- Hetzner Online GmbH, Deutschland — Hosting der Server- und Datenbankinfrastruktur (gemäß Anhang 1); Verarbeitung in DE/EU.
- Cloudflare, Inc., USA — CDN/WAF/Spam-Schutz (Übertragungsdaten, IP-Adressen); Garantien: EU-US Data Privacy Framework bzw. EU-Standardvertragsklauseln.
- Google Ireland Limited, Irland — Versand transaktionaler E-Mails (SMTP).

Die jeweils aktuelle Fassung dieser Anlage ist unter https://kud.tax/avv.pdf abrufbar; Änderungen werden nach § 5 mitgeteilt.