Auftragsverarbeitungsvertrag

KontoBee

gem. Art. 28 DSGVO

S2Tec GmbH | An der Schelmenhalde 32 | 71665 Vaihingen an der Enz | Deutschland
Amtsgericht Stuttgart HRB 775923 | Geschäftsführer: Dr. Jiangqin Sun, Dr. Philipp Steinemann
IBAN: DE40 1001 0123 7120 0850 04 | BIC: QNTODEB2XXX | USt.-Ident.-Nr.: DE337978368

1. Vertragsparteien und Geltung

Dieser Auftragsverarbeitungsvertrag („AVV") gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) gilt zwischen

- dem Kunden, der KontoBee nutzt („Verantwortlicher"), und
- der S2Tec GmbH, An der Schelmenhalde 32, 71665 Vaihingen an der Enz, Deutschland („Auftragsverarbeiter").

(1) Der AVV wird mit Abschluss des Nutzungsvertrags über KontoBee („Hauptvertrag"), also mit der Registrierung und der Zustimmung zu den Allgemeinen Geschäftsbedingungen, Bestandteil des Hauptvertrags. Er ist damit in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO). Einer gesonderten Unterschrift bedarf es nicht.

(2) Der AVV gilt für die gesamte Laufzeit des Hauptvertrags und darüber hinaus, solange der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen verarbeitet.

(3) Bei Widersprüchen geht dieser AVV dem Hauptvertrag in Fragen des Datenschutzes vor.

2. Gegenstand, Art und Zweck der Verarbeitung

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen die webbasierte Buchhaltungssoftware KontoBee bereit und verarbeitet dabei personenbezogene Daten ausschließlich im Auftrag des Verantwortlichen. Die Verarbeitung umfasst insbesondere:

- Erfassen von Belegen per Upload, E-Mail (eigene Eingangsadresse oder IMAP-Abruf eines Postfachs des Verantwortlichen) und WhatsApp;
- Auslesen von Belegen per Texterkennung und KI (über den eigenen Dienst Eagle Doc des Auftragsverarbeiters);
- Kontierungs-, Zuordnungs- und Duplikatvorschläge;
- Abruf und Abgleich von Bankumsätzen;
- Erstellen und Versenden von Ausgangsrechnungen und Mahnungen;
- Speichern, Archivieren, Exportieren (z. B. an DATEV oder den Steuerberater) und Löschen der Daten;
- Support und Fehlerbehebung, auch über die Feedback-Funktion (Absatz 4).

(2) Art der Verarbeitung: Erheben, Erfassen, Speichern, Auslesen, Abgleichen, Ordnen, Übermitteln auf Veranlassung des Verantwortlichen, Archivieren und Löschen.

(3) Der Auftragsverarbeiter nutzt die Daten nicht für eigene Zwecke, insbesondere nicht zum Training von KI-Modellen. Nicht unter diesen AVV fallen Daten, die er als eigener Verantwortlicher verarbeitet: Vertrags- und Abrechnungsdaten des Kunden sowie Protokolle zur Sicherheit und Missbrauchserkennung. Lernende Funktionen werten Daten ausschließlich

innerhalb des Kontos des Verantwortlichen aus. Die eingesetzten KI-Anbieter verwenden die Daten vertragsgemäß nicht zum Training ihrer Modelle.

(4) **Feedback-Funktion.** Über die Feedback-Funktion in KontoBee können Nutzer Fehler und Anfragen direkt an das Support-Team des Auftragsverarbeiters melden. Eine Meldung kann neben der Beschreibung des Nutzers auch Daten aus KontoBee (z. B. Belege, Buchungs-, Bank- und Stammdaten), Screenshots und technische Angaben (z. B. aufgerufene Seite, Browser, Fehlerprotokolle) enthalten. Das Support-Team verwendet diese Daten nur, um den gemeldeten Fehler nachzuvollziehen und zu beheben, und sieht sich dazu bei Bedarf die betroffenen Daten im Konto des Verantwortlichen direkt an.

3. Datenarten und betroffene Personen

(1) Kategorien personenbezogener Daten:

- **Nutzer- und Kontodaten:** Name, E-Mail-Adresse, Telefonnummer, Rolle, Anmelde- und Protokolldaten (z. B. IP-Adresse, Zeitstempel);
- **Geschäftspartnerdaten:** Name, Anschrift, Kontaktdaten, Steuernummer, USt-IdNr., Bankverbindung;
- **Beleg- und Buchungsdaten:** Inhalte von Rechnungen und sonstigen Belegen, Beträge, Positionen, Buchungssätze;
- **Bankdaten:** Kontoumsätze, IBAN, Gegenpartei, Verwendungszweck;
- **Kommunikationsdaten:** E-Mails und WhatsApp-Nachrichten samt Anhängen, Support-Anfragen und Meldungen über die Feedback-Funktion einschließlich Screenshots.

(2) Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) werden nicht bestimmungsgemäß verarbeitet. Soweit sie in Belegen oder Bankumsätzen enthalten sind (z. B. Kirchensteuer, Gewerkschaftsbeiträge, Arztrechnungen), gelten für sie dieselben Schutzmaßnahmen.

(3) Kategorien betroffener Personen: Nutzer und Beschäftigte des Verantwortlichen, seine Kunden, Lieferanten und sonstigen Geschäftspartner sowie deren Ansprechpartner, sein Steuerberater, Absender von E-Mails und Nachrichten an KontoBee.

4. Weisungen

(1) Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats dazu verpflichtet; in diesem Fall teilt er dem Verantwortlichen dies vorher mit, sofern das Recht dies nicht verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(2) Weisungen sind dieser AVV, der Hauptvertrag und die Nutzung der Funktionen von KontoBee durch den Verantwortlichen. Weitere Weisungen erteilt der Verantwortliche in Textform an support@kontobee.com.

(3) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich und darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.

5. Pflichten des Verantwortlichen

(1) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Rechtsgrundlage und die Information der betroffenen Personen.

(2) **Konten für Dritte.** Legt der Verantwortliche Konten für Mandanten oder Kunden an oder verarbeitet er deren Daten in KontoBee (z. B. als Steuerberater oder Buchhaltungsbüro), stellt er sicher, dass er dazu berechtigt ist. Ist er selbst Auftragsverarbeiter, gilt dieser AVV entsprechend; die S2Tec GmbH ist dann weiterer Auftragsverarbeiter.

(3) **Berufsgeheimnis.** Unterliegt der Verantwortliche einer beruflichen Verschwiegenheitspflicht (§ 203 StGB), verarbeitet er davon erfasste Daten in KontoBee nur, wenn der jeweilige Mandant der Nutzung von KontoBee einschließlich der Unterauftragsverarbeiter nach Anlage 2 vorher in Textform zugestimmt hat. Verlangt das Berufsrecht des Verantwortlichen weitergehende Anforderungen an den Vertrag mit Dienstleistern (z. B. § 62a StBerG), muss der Mandant zusätzlich ausdrücklich auf deren Einhaltung verzichtet haben (§ 62a Abs. 6 StBerG). Mit den Unterauftragsverarbeitern bestehen keine gesonderten Vereinbarungen nach § 203 StGB. Der Verantwortliche bewahrt die Erklärungen auf.

6. Pflichten des Auftragsverarbeiters

(1) **Vertraulichkeit.** Mit der Verarbeitung befasste Personen sind auf Vertraulichkeit verpflichtet oder unterliegen einer gesetzlichen Verschwiegenheitspflicht (Art. 28 Abs. 3 lit. b DSGVO). Gegenüber Verantwortlichen, die einer beruflichen Verschwiegenheitspflicht unterliegen, verpflichtet sich der Auftragsverarbeiter selbst zur Verschwiegenheit über fremde Geheimnisse und verschafft sich nur insoweit Kenntnis davon, wie es zur Vertragserfüllung erforderlich ist. Ihm ist bekannt, dass die unbefugte Offenbarung eines solchen Geheimnisses nach § 203 Abs. 4 StGB strafbar ist.

(2) **Sicherheit.** Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß Anlage 1. Er darf sie an den Stand der Technik anpassen, sofern das Schutzniveau nicht sinkt.

(3) **Datenschutzverletzungen.** Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, in der Regel innerhalb von 48 Stunden nach Kenntnis, in Textform mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit verfügbar. Er ergreift unverzüglich Maßnahmen zur Eindämmung.

(4) **Unterstützung.** Der Auftragsverarbeiter unterstützt den Verantwortlichen im angemessenen Rahmen bei

- der Beantwortung von Anträgen betroffener Personen (Art. 12 bis 23 DSGVO); Anträge, die ihn direkt erreichen, leitet er unverzüglich weiter;
- den Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

Auskunft, Berichtigung, Export und Löschung kann der Verantwortliche in der Regel selbst über die Funktionen von KontoBee vornehmen. Für Unterstützung, die darüber hinausgeht und nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückgeht, kann dieser eine angemessene Vergütung verlangen.

(5) **Ansprechpartner.** Ansprechpartner für Datenschutzfragen ist Dr. Philipp Steinemann, erreichbar unter support@kontobee.com.

(6) **Aufsichtsbehörde.** Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Maßnahmen der Aufsichtsbehörde, soweit sie diese Verarbeitung betreffen, sowie über Zugriffe Dritter auf die Daten (z. B. Pfändung, Beschlagnahme). Die Kontrollrechte der Aufsichtsbehörde bleiben unberührt.

7. Unterauftragsverarbeiter

(1) Der Verantwortliche genehmigt die in Anlage 2 genannten Unterauftragsverarbeiter. Der Auftragsverarbeiter darf weitere Unterauftragsverarbeiter einsetzen oder bestehende ersetzen (allgemeine Genehmigung nach Art. 28 Abs. 2 DSGVO).

(2) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage vorher per E-Mail oder in KontoBee über jede beabsichtigte Änderung. Der Verantwortliche kann innerhalb von 30 Tagen nach Zugang aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Nach einem fristgerechten Widerspruch setzt der Auftragsverarbeiter den neuen Unterauftragsverarbeiter für die Daten des Verantwortlichen nicht ein, bis die Parteien eine einvernehmliche Lösung gefunden haben. Finden die Parteien keine Lösung, kann der Verantwortliche den Hauptvertrag außerordentlich kündigen. Finden sie innerhalb von 30 Tagen nach Zugang des Widerspruchs keine Lösung, kann auch der Auftragsverarbeiter den Hauptvertrag mit einer Frist von 30 Tagen außerordentlich kündigen. In beiden Fällen werden im Voraus gezahlte Entgelte anteilig erstattet.

(3) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die diesem AVV entsprechen (Art. 28 Abs. 4 DSGVO). Er haftet für dessen Pflichtverletzungen wie für eigene.

(4) Kein Unterauftragsverhältnis sind Dienste, die der Verantwortliche selbst anbindet oder für die der Auftragsverarbeiter selbst verantwortlich ist (Anlage 2, Teil B).

8. Übermittlung in Drittländer

(1) Die Daten werden in Rechenzentren innerhalb der EU bzw. des EWR gespeichert und verarbeitet, soweit Anlage 2 nichts anderes angibt. Der Verantwortliche stimmt den dort genannten Übermittlungen zu.

(2) Einzelne Unterauftragsverarbeiter gehören zu Konzernen mit Sitz in den USA. Soweit dadurch ein Zugriff aus einem Drittland möglich ist oder Daten dorthin übermittelt werden, erfolgt dies nur unter den Voraussetzungen der Art. 44 ff. DSGVO, insbesondere auf Grundlage des EU-US Data Privacy Framework oder der EU-Standardvertragsklauseln.

9. Nachweise und Kontrollen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO erforderlich sind, vorrangig durch Dokumentation, Selbstauskünfte und Nachweise der Unterauftragsverarbeiter (z. B. ISO-27001- oder SOC-2-Berichte).

(2) Reicht dies nicht aus, darf der Verantwortliche oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer, der kein Wettbewerber des Auftragsverarbeiters ist, eine Prüfung vor Ort durchführen: nach Ankündigung mit einer Frist von mindestens 30 Tagen, höchstens einmal im Kalenderjahr (außer bei einer konkreten Datenschutzverletzung), zu Geschäftszeiten und ohne unzumutbare Störung des Betriebs. Daten anderer Kunden und Geschäftsgeheimnisse sind von der Prüfung ausgenommen.

(3) Die Kosten einer Prüfung vor Ort trägt der Verantwortliche, einschließlich des Aufwands des Auftragsverarbeiters zu einem angemessenen Stundensatz. Ergibt die Prüfung einen wesentlichen Verstoß des Auftragsverarbeiters, trägt dieser die Kosten selbst.

10. Löschung und Rückgabe

(1) Der Verantwortliche kann seine Daten während der Laufzeit jederzeit über KontoBee exportieren und löschen.

(2) Endet ein kostenpflichtiges Abonnement, bleibt das Konto mit seinen Daten bestehen, damit der Verantwortliche weiter darauf zugreifen und sie exportieren kann; der Hauptvertrag und dieser AVV gelten so lange fort. Der Hauptvertrag endet, wenn der Verantwortliche sein Konto löscht oder die Löschung in Textform verlangt. Der Auftragsverarbeiter löscht die personenbezogenen Daten dann unverzüglich, spätestens nach 30 Tagen, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Die Rückgabe erfolgt über die Exportfunktion.

(3) Der Auftragsverarbeiter darf ein Konto ohne aktives Abonnement löschen, wenn es zwölf Monate nicht genutzt wurde und er die Löschung mindestens 30 Tage vorher per E-Mail angekündigt hat.

(4) Für die Erfüllung seiner eigenen Aufbewahrungspflichten (z. B. § 147 AO) ist der Verantwortliche selbst verantwortlich. Daten in Sicherungskopien werden mit Ablauf von deren Aufbewahrungsfrist gelöscht, spätestens nach 30 Tagen.

(5) Unterlagen, die dem Nachweis der ordnungsgemäßen Verarbeitung dienen, darf der Auftragsverarbeiter über das Vertragsende hinaus entsprechend den gesetzlichen Fristen aufbewahren.

11. Haftung

Für die Haftung gelten Art. 82 DSGVO und die Haftungsregeln des Hauptvertrags. Haftungsbeschränkungen des Hauptvertrags gelten nicht für Vorsatz, grobe Fahrlässigkeit und die Verletzung von Leben, Körper oder Gesundheit.

12. Schlussbestimmungen

(1) Der Auftragsverarbeiter kann diesen AVV ändern, soweit dies aufgrund geänderter Rechtslage, neuer Funktionen oder geänderter Unterauftragsverarbeiter erforderlich ist und den Schutz der Daten nicht verringert. Er kündigt Änderungen mindestens 30 Tage vorher per E-Mail oder in KontoBee an. Widerspricht der Verantwortliche innerhalb dieser Frist in Textform, kann er den Hauptvertrag zum Zeitpunkt der Änderung außerordentlich kündigen; im Voraus gezahlte Entgelte werden anteilig erstattet. Ohne Widerspruch gilt die Änderung als angenommen; darauf weist der Auftragsverarbeiter in der Ankündigung hin.

(2) Es gilt deutsches Recht. Der Gerichtsstand richtet sich nach dem Hauptvertrag.

(3) Ist eine Bestimmung unwirksam, bleiben die übrigen wirksam. An ihre Stelle tritt eine Regelung, die dem Zweck am nächsten kommt und Art. 28 DSGVO entspricht.

Anlage 1: Technische und organisatorische Maßnahmen

Vertraulichkeit

- **Zutritt:** Betrieb ausschließlich in Rechenzentren der Unterauftragsverarbeiter mit Zutrittskontrolle, Videoüberwachung und Zertifizierung (z. B. ISO 27001); keine Kundendaten auf Servern in Büroräumen.
- **Zugang:** Individuelle Konten; Passwörter nach Stand der Technik, gespeichert nur als Hash; Zwei-Faktor-Authentifizierung für alle administrativen Zugänge, für Nutzer von KontoBee wählbar und je Firma verpflichtend einstellbar; administrative Oberflächen nur über verschlüsselte Tunnel erreichbar.
- **Zugriff:** Rollen- und Rechtekonzept nach dem Prinzip der minimalen Rechte; Zugriff des Personals auf Kundendaten nur, soweit für Betrieb oder Support nötig; Protokollierung administrativer Änderungen.
- **Trennung:** Logische Mandantentrennung; jeder Datensatz ist einer Firma zugeordnet und nur für sie abrufbar; getrennte Produktions-, Test- und Entwicklungsumgebungen; Tests ohne echte Kundendaten.

Integrität

- **Übertragung:** Verschlüsselung aller Verbindungen per TLS nach Stand der Technik; E-Mail-Versand mit SPF, DKIM und DMARC.
- **Speicherung:** Verschlüsselung der Hauptdatenbank und des Dateispeichers einschließlich ihrer Sicherungen im Ruhezustand.
- **Eingabekontrolle:** Änderungsprotokoll für Buchungsdaten (manipulationsgesicherte Kette) und sicherheitsrelevante Ereignisse.

Verfügbarkeit und Belastbarkeit

- **Speicherung und Sicherung:** Dateien werden bei Amazon Web Services innerhalb der EU gespeichert; die Datenbank wird von MongoDB Atlas automatisiert und verschlüsselt gesichert; Ausbau um zusätzliche Sicherungen bei einem externen Anbieter (Anlage 2) vorbehalten;
- Überwachung der Systeme mit Alarmierung, Schutz vor Überlast (Ratenbegrenzung), regelmäßige Sicherheitsupdates und Prüfung der Container-Images auf bekannte Schwachstellen;
- Server-Logs werden in der Regel nach 30 Tagen gelöscht.

Verfahren zur regelmäßigen Überprüfung

- Automatisierte Tests vor jeder Auslieferung, Code-Reviews, Sicherheitsprüfungen;
- Prozess zur Behandlung von Sicherheitsvorfällen und Meldungen von Sicherheitslücken;
- Sorgfältige Auswahl und regelmäßige Überprüfung der Unterauftragsverarbeiter;
- Datenschutzfreundliche Voreinstellungen: Funktionen mit zusätzlicher Datenverarbeitung (z. B. Bankanbindung, WhatsApp, Postfach-Abruf) sind nur aktiv, wenn der Verantwortliche sie einschaltet.

Anlage 2: Unterauftragsverarbeiter

Teil A: Genehmigte Unterauftragsverarbeiter

Nr.	Unternehmen	Leistung	Ort
1	Hetzner Online GmbH, Gunzenhausen, Deutschland	Server-Hosting von KontoBee (Anwendung, Suchindex, Support-System), E-Mail-Postfach des Supports, Datensicherung (verschlüsselte Backups, soweit eingesetzt)	EU
2	Amazon Web Services EMEA SARL, Luxemburg	Dateispeicher, E-Mail-Versand und -Empfang, Hosting von Eagle Doc (Texterkennung) und von KI-Modellen	EU
3	MongoDB Ltd., Dublin, Irland	Datenbank (MongoDB Atlas)	EU
4	Microsoft Ireland Operations Ltd., Dublin, Irland	KI-Modelle (Azure OpenAI), E-Mail der S2Tec GmbH (Kopien von Support-Anfragen)	EU
5	Google Cloud EMEA Ltd., Dublin, Irland	KI-Modelle (Vertex AI) und Texterkennung	EU
6	finAPI GmbH, München, Deutschland	Abruf von Bankkonten und -umsätzen; nur bei Nutzung der Bankanbindung	EU
7	Meta Platforms Ireland Ltd., Dublin, Irland	Empfang und Versand von WhatsApp-Nachrichten; nur bei Nutzung des WhatsApp-Kanals	EU und USA
8	IONOS SE, Montabaur, Deutschland	Datensicherung (verschlüsselte Backups, soweit eingesetzt)	EU

Garantien für Drittlandzugriffe richten sich nach Ziffer 8 des AVV.

Teil B: Keine Unterauftragsverarbeitung

- **Eagle Doc:** eigener Dienst der S2Tec GmbH; dessen Dienstleister sind in Teil A enthalten.
- **Stripe Payments Europe Ltd., Dublin, Irland:** Abrechnung des KontoBee-Abonnements (eigene Verantwortung der S2Tec GmbH). Bindet der Verantwortliche sein eigenes Stripe-Konto an, ruft KontoBee Daten aus diesem Konto in seinem Auftrag ab; Stripe ist dabei Vertragspartner des Verantwortlichen.
- **DATEV eG und Steuerberater:** Übermittlung nur auf Veranlassung des Verantwortlichen an dessen eigene Vertragspartner.
- **Postfächer des Verantwortlichen:** Abruf über IMAP nur mit den vom Verantwortlichen hinterlegten Zugangsdaten.
- **Europäische Kommission (VIES):** Prüfung von USt-IdNrn. bei der amtlichen Schnittstelle.