

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

1. Parteien und Anwendungsbereich

Dieser Auftragsverarbeitungsvertrag ("AVV") ist Bestandteil der Vereinbarung zwischen dem Kunden ("Verantwortlicher") und der TECHARENABG EOOD ("Auftragsverarbeiter", "wir", "InboxDoc") und regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Zusammenhang mit dem Rechnungsverarbeitungsdienst InboxDoc.

2. Gegenstand und Dauer

Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen zur Erbringung des InboxDoc-Dienstes: Durchsuchen der verbundenen E-Mail-Konten des Verantwortlichen nach Nachrichten mit Rechnungsanhängen, Extraktion strukturierter Rechnungsdaten und Bereitstellung dieser Daten im Dashboard des Verantwortlichen.

Dieser AVV gilt für die Dauer der Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen und endet automatisch mit Beendigung der zugrunde liegenden Dienstvereinbarung und nach Löschung oder Rückgabe aller personenbezogenen Daten gemäß Ziffer 12.

3. Art und Zweck der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich, um: sich mit den vom Verantwortlichen benannten E-Mail-Konten (Gmail, Outlook oder IMAP) über die vom Verantwortlichen erteilte Zugriffsberechtigung zu verbinden; E-Mail-Nachrichten zu identifizieren, die Rechnungs- oder Gutschriftsanhänge enthalten oder wahrscheinlich enthalten; strukturierte Rechnungsdaten aus diesen Anhängen zu extrahieren (deterministisch aus strukturierten E-Rechnungs-XML-Dateien, soweit verfügbar, andernfalls KI-gestützt aus der PDF-Datei); sowie die extrahierten strukturierten Daten zu speichern, im Dashboard des Verantwortlichen anzuzeigen und zu exportieren.

4. Kategorien personenbezogener Daten

- Kontodaten der Nutzer des Verantwortlichen (Name, E-Mail-Adresse)
- Metadaten gescannter E-Mails (Absender, Betreff, Datum)
- Aus Rechnungen/Gutschriften extrahierte Daten (Lieferantenname, Rechnungsnummer, Datum, Beträge, Währung) – kann personenbezogene Daten enthalten, soweit eine Rechnung eine natürliche Person als Lieferant oder Kunde benennt
- OAuth-Zugriffs-/Refresh-Token bzw. ein verschlüsseltes IMAP-App-Passwort, ausschließlich zur Aufrechterhaltung der E-Mail-Verbindung
- Näherungsweise Herkunftsland, einmalig bei Registrierung aus der IP-Adresse abgeleitet; die IP-Adresse selbst wird nicht gespeichert

5. Kategorien betroffener Personen

Die eigenen Nutzer des Verantwortlichen (z. B. Mitarbeiter mit Dashboard-Zugriff) sowie Dritte, die auf über den Dienst verarbeiteten Rechnungen genannt werden (z. B. Ansprechpartner von Lieferanten, Einzelunternehmer, die dem Verantwortlichen Rechnungen stellen).

6. Rechte und Pflichten des Verantwortlichen

Der Verantwortliche bleibt allein verantwortlich für die Rechtmäßigkeit der zur Verarbeitung übermittelten personenbezogenen Daten (einschließlich der verbundenen E-Mail-Konten) sowie für die Beantwortung von Anfragen betroffener Personen, soweit der Auftragsverarbeiter nicht gemäß Ziffer 10 zur Unterstützung verpflichtet ist. Der Verantwortliche ist für die Erteilung dokumentierter Weisungen an den Auftragsverarbeiter verantwortlich; dieser AVV sowie die bestimmungsgemäße Nutzung der dokumentierten Funktionen des

Dienstes durch den Verantwortlichen stellen eine solche Weisung dar.

7. Pflichten des Auftragsverarbeiters

- Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, auch hinsichtlich internationaler Datenübermittlungen, sofern er nicht durch Unionsrecht oder das Recht der Mitgliedstaaten zu einer anderen Verarbeitung verpflichtet ist.
- Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet haben.
- Der Auftragsverarbeiter speichert keine Quelldateien (PDF-Anhänge oder E-Rechnungs-XML-Dateien) – gespeichert werden ausschließlich die daraus extrahierten strukturierten Datenfelder.
- Der Auftragsverarbeiter setzt die in Ziffer 8 beschriebenen technischen und organisatorischen Maßnahmen um.
- Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter (Unterauftragsverarbeiter) in Anspruch ohne vorherige allgemeine Genehmigung des Verantwortlichen; diese Genehmigung erteilt der Verantwortliche hiermit für die in Ziffer 9 genannten Unterauftragsverarbeiter. Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern und gibt dem Verantwortlichen die Möglichkeit, Einspruch zu erheben.

8. Technische und organisatorische Maßnahmen (TOM)

- Verschlüsselung von OAuth-Token und IMAP-App-Passwörtern im Ruhezustand; HTTPS/TLS für alle Datenübertragungen
- Row-Level-Security in der Datenbank, sodass jeder Kunde ausschließlich auf seine eigenen Daten zugreifen kann
- Keine Speicherung von Quell-PDF-/XML-Dateien – gespeichert werden nur die extrahierten strukturierten Felder (siehe Datenschutzerklärung)
- Zugriff auf Gmail/Outlook ausschließlich über OAuth-Scopes mit minimal notwendigen Berechtigungen; Passwörter für Gmail/Outlook werden zu keinem Zeitpunkt abgefragt oder gespeichert (IMAP-App-Passwörter werden verschlüsselt und niemals im Klartext gespeichert)
- Zwei-Faktor-Authentifizierung (MFA) für den Kontozugriff verfügbar
- Zugriffskontrolle: interner Zugriff auf Produktionsdaten ist auf Personen beschränkt, die ihn für Support/Betrieb benötigen
- Wo möglich deterministische, nicht KI-basierte Extraktion (strukturierte E-Rechnungs-XML); KI-gestützte Extraktion kommt nur als Rückfalllösung und ausschließlich auf das Dokument selbst zur Anwendung, niemals auf Zugangsdaten

9. Unterauftragsverarbeiter

Der Verantwortliche genehmigt die Einbindung folgender Unterauftragsverarbeiter:

- Supabase – Datenbank-Hosting, Authentifizierung – EU (Irland, eu-west-1)
- Vercel Inc. – Anwendungs-Hosting / Serverless-Funktionen – EU (Dublin, dub1; festgelegt)
- Cloudflare, Inc. – Netzwerk-Proxy/DNS
- Anthropic, PBC – KI-gestützte Rechnungsdatenextraktion (nur Rückfalllösung; nicht genutzt bei E-Rechnungen, die über strukturiertes XML verarbeitet werden) – USA; Übermittlungsgarantie: Standardvertragsklauseln (Art. 46 DSGVO)
- Lemon Squeezy, Inc. (ein Unternehmen von Stripe) – Zahlungsabwicklung als Merchant of Record
- Google LLC – Zugriff auf die Gmail-API (mit ausdrücklicher Einwilligung des Verantwortlichen); Google Analytics (GA4), nur nach Cookie-Einwilligung – USA
- Microsoft Corporation – Zugriff auf Outlook/Microsoft Graph API (mit ausdrücklicher Einwilligung des Verantwortlichen)

10. Unterstützung bei Anfragen betroffener Personen

Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen, soweit dies angemessen möglich ist, bei der Erfüllung von dessen Pflicht zur Beantwortung von Anträgen betroffener Personen zur Ausübung ihrer Rechte nach Kapitel III DSGVO. Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet dieser die Anfrage unverzüglich an den Verantwortlichen weiter, sofern nicht anders angewiesen.

11. Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter meldet dem Verantwortlichen unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten in Bezug auf dessen Daten bekannt geworden ist, und unterstützt ihn angemessen bei dessen eigenen Meldepflichten nach Art. 33/34 DSGVO.

12. Löschung oder Rückgabe von Daten nach Beendigung

Nach Beendigung der zugrunde liegenden Dienstvereinbarung löscht oder gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen sämtliche im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten zurück und löscht vorhandene Kopien, sofern nicht nach Unionsrecht oder dem Recht der Mitgliedstaaten eine fortdauernde Speicherpflicht besteht. Die vom Verantwortlichen über die Selbstbedienungsfunktion "Konto löschen" veranlasste Kontolöschung löscht sofort und unwiderruflich extrahierte Rechnungsdaten, widerruft OAuth-Token beim jeweiligen Anbieter und löscht Profil- und Benachrichtigungsdaten, wie in der Datenschutzerklärung beschrieben.

13. Kontrollrechte

Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in diesem AVV und in Art. 28 DSGVO niedergelegten Pflichten erforderlich sind, und ermöglicht Überprüfungen einschließlich Inspektionen, die vom Verantwortlichen oder einem von ihm beauftragten Prüfer durchgeführt werden, und wirkt an diesen mit, vorbehaltlich angemessener vorheriger Ankündigung und Vertraulichkeit.

14. Haftung

Die Haftung zwischen den Parteien im Zusammenhang mit diesem AVV richtet sich nach den Haftungsbestimmungen der zugrunde liegenden Nutzungsbedingungen.

15. Anwendbares Recht

Dieser AVV unterliegt dem Recht Bulgariens sowie der Datenschutz-Grundverordnung (EU) 2016/679.

TODO(legal-review): Dieses gesamte Dokument ist ein Entwurf auf Grundlage der uns beschriebenen tatsächlichen technischen Umsetzung; es wurde noch nicht von einem auf Datenschutzrecht spezialisierten Anwalt geprüft und sollte vor einer solchen Prüfung nicht als verbindliches Rechtsdokument verwendet, unterzeichnet oder an Kunden versendet werden.