Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

Version 2026-07-30 · Stand: 30. Juli 2026

zwischen

dem im Annahmenachweis bezeichneten Kunden – nachfolgend „Verantwortlicher“ –

und

Tom Trögler, handelnd unter RechneX, Schutterstr. 36/5, 77743 Neuried, Deutschland, E-Mail: datenschutz@rechnex.de – nachfolgend „Auftragsverarbeiter“ –

gemeinsam die „Parteien“.

1. Abschluss, Geltungsbereich und Rangfolge

1. Dieser Auftragsverarbeitungsvertrag („AVV“) wird für den Standarddienst RechneX in elektronischer Form geschlossen. Der Verantwortliche nimmt ihn durch eine gesonderte, nicht vorangekreuzte Erklärung im Nutzerkonto an. RechneX protokolliert Vertragspartei, Konto, E-Mail-Adresse, AVV-Version, Vertrags-Hash, Erklärungswortlaut, Zeitpunkt, Sprache und Abschlussweg. Eine handschriftliche Unterschrift ist nicht erforderlich.
2. Der AVV gilt nur, soweit RechneX personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Verarbeitungen, für die RechneX selbst Verantwortlicher ist – insbesondere Kontoführung, Vertragsverwaltung, Abrechnung, Zahlungsabwicklung, Missbrauchs- und Sicherheitsprävention, allgemeiner Support und Vertrieb – fallen nicht unter diesen AVV und sind in der Datenschutzerklärung beschrieben.
3. Individuelle Enterprise- oder API-Leistungen sind nur erfasst, wenn dies im jeweiligen Angebot oder Einzel-AVV ausdrücklich vereinbart ist. Für freigeschaltete Enterprise-Verarbeitungen gilt vorrangig der individuelle AVV.
4. Bei Widersprüchen gelten zwingendes Datenschutzrecht, danach dieser AVV einschließlich seiner Anlagen und anschließend Hauptvertrag und AGB. Haftungsregelungen der AGB gelten ergänzend, soweit zwingendes Datenschutzrecht und Ziffer 12 dieses AVV nicht entgegenstehen.

2. Gegenstand und Dauer

1. Gegenstand ist die technische Bereitstellung der vereinbarten RechneX-Standardfunktionen zur Konvertierung, Generierung, Anzeige und Validierung elektronischer Rechnungen sowie der hierfür erforderlichen temporären Verarbeitung.
2. Die Verarbeitung beginnt mit der Nutzung einer erfassten Funktion und dauert für die Laufzeit des Hauptvertrags beziehungsweise bis zum Abschluss der jeweiligen Einzelverarbeitung. Gesetzliche Nachweis- und Aufbewahrungspflichten bleiben unberührt.

3. Art und Zweck der Verarbeitung

RechneX verarbeitet Daten ausschließlich zur Erbringung der vom Verantwortlichen gewählten Standardfunktion:

- Entgegennahme von PDF-, XML- oder eingebetteten Rechnungsdateien;
- OCR- und KI-gestützte Extraktion von Rechnungsfeldern;
- vorübergehende Darstellung und Bearbeitung im Editor oder Viewer;
- Erzeugung von XRechnung oder ZUGFeRD;
- technische Prüfung mit KoSIT- und Mustang-Regeln;
- Bereitstellung von Ergebnisdateien und Prüfberichten;
- technisch notwendige Job-, Sicherheits- und Nutzungsmetadaten ohne planmäßige Speicherung von Rechnungsinhalten.

Eine Nutzung von Kundendaten für Werbung oder zum Training eigener oder fremder allgemeiner KI-Modelle ist nicht Gegenstand des Auftrags.

4. Datenarten und betroffene Personen

4.1 Datenarten

- Rechnungs-, Liefer- und Leistungsdaten;
- Namen, Anschriften und geschäftliche Kontaktdaten;
- Kunden-, Lieferanten-, Bestell-, Vertrags- und Rechnungsnummern;
- Steuer-, Zahlungs- und Bankverbindungsdaten;
- Freitext und Anlagen, soweit sie vom Verantwortlichen bereitgestellt werden;
- technische Job-, Format-, Prüf-, Sicherheits- und Nutzungsmetadaten.

4.2 Betroffene Personen

- Kunden, Lieferanten und Geschäftspartner des Verantwortlichen;
- Beschäftigte, Ansprechpartner und Erfüllungsgehilfen dieser Stellen;
- sonstige Personen, deren Daten der Verantwortliche in einer Rechnung oder Anlage bereitstellt.

4.3 Ausgeschlossene Daten

Der Standarddienst ist nicht für besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO oder Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO bestimmt. Der Verantwortliche darf solche Daten nicht in den Standarddienst eingeben oder hochladen. Eine Verarbeitung kommt nur nach vorheriger ausdrücklicher schriftlicher Vereinbarung im Enterprise-Bereich und mit dafür festgelegten zusätzlichen Schutzmaßnahmen in Betracht.

5. Weisungen und Pflichten des Verantwortlichen

1. RechneX verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen. Der Hauptvertrag, dieser AVV, die gewählte Produktfunktion und dokumentierte Einstellungen bilden die anfängliche Weisung.
2. Zusätzliche Weisungen bedürfen mindestens der Textform und müssen rechtmäßig, zumutbar und vom vereinbarten Leistungsumfang gedeckt sein. Mehraufwand außerhalb des Leistungsumfangs darf nach vorheriger Abstimmung berechnet werden.
3. Hält RechneX eine Weisung für rechtswidrig, informiert RechneX den Verantwortlichen unverzüglich und darf ihre Ausführung bis zur Klärung aussetzen.
4. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung, die Information der betroffenen Personen, die Datenrichtigkeit, die Wahrung der Betroffenenrechte und die Zulässigkeit seiner Weisungen verantwortlich.
5. Der Verantwortliche lädt nur erforderliche Daten hoch, prüft KI-extrahierte und erzeugte Ergebnisse vor ihrer Verwendung und sichert benötigte Ergebnisdateien rechtzeitig in seinem eigenen System.

6. Pflichten des Auftragsverarbeiters

RechneX verpflichtet sich,

- Daten nur im Rahmen dokumentierter Weisungen zu verarbeiten, soweit keine bindende gesetzliche Pflicht eine andere Verarbeitung verlangt; in diesem Fall wird der Verantwortliche vorab informiert, sofern dies rechtlich zulässig ist;
- nur Personen einzusetzen, die auf Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterworfen sind;
- angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO aufrechtzuerhalten;
- den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen angemessen bei Betroffenenanfragen, Datenschutz-Folgenabschätzungen, vorherigen Konsultationen und der Erfüllung der Pflichten aus Art. 32 bis 36 DSGVO zu unterstützen;
- Anfragen betroffener Personen, soweit sie den Auftrag betreffen, unverzüglich an den Verantwortlichen weiterzuleiten und nicht ohne dessen Weisung zu beantworten, sofern keine gesetzliche Pflicht besteht;

- dem Verantwortlichen Verletzungen des Schutzes auftragsverarbeiteter personenbezogener Daten unverzüglich nach Bekanntwerden mitzuteilen und die verfügbaren, für Art. 33 und 34 DSGVO erforderlichen Informationen schrittweise bereitzustellen;
- die Einhaltung dieses AVV nach Maßgabe von Ziffer 11 nachweisbar zu machen.

7. Technische und organisatorische Maßnahmen

Die bei Vertragsschluss maßgeblichen Maßnahmen sind in Anlage 2 beschrieben. RechneX darf sie dem technischen Fortschritt entsprechend ändern, wenn das vereinbarte Schutzniveau nicht unterschritten wird. Maßnahmen werden risikobasiert überprüft und erforderlichenfalls angepasst.

8. Unterauftragsverarbeiter

1. Der Verantwortliche erteilt RechneX die allgemeine Genehmigung, die in Anlage 1 genannten und weitere Unterauftragsverarbeiter einzusetzen, soweit dies für die vereinbarte Leistung erforderlich ist.
2. RechneX informiert den Verantwortlichen grundsätzlich mindestens 14 Tage vor dem geplanten Einsatz oder Austausch eines Unterauftragsverarbeiters per E-Mail oder im Nutzerkonto. In begründeten Not- oder Sicherheitsfällen darf die Änderung kurzfristiger erfolgen; RechneX informiert dann ohne schuldhaftes Zögern.
3. Der Verantwortliche kann innerhalb der mitgeteilten Frist aus objektiv nachvollziehbaren Datenschutzgründen widersprechen. Die Parteien suchen eine angemessene Lösung. Ist eine Lösung nicht möglich, darf RechneX die betroffene Funktion einstellen oder jede Partei den davon betroffenen Leistungsteil kündigen.
4. RechneX verpflichtet Unterauftragsverarbeiter vertraglich zu im Wesentlichen gleichwertigen Datenschutzpflichten und bleibt gegenüber dem Verantwortlichen für die Erfüllung der Pflichten des Unterauftragsverarbeiters verantwortlich.

9. Verarbeitung in Drittländern

Soweit personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums verarbeitet werden, stellt RechneX ein nach Kapitel V DSGVO zulässiges Übermittlungsinstrument sicher, insbesondere einen Angemessenheitsbeschluss, eine wirksame Zertifizierung nach dem EU-US Data Privacy Framework oder EU-Standardvertragsklauseln einschließlich erforderlicher ergänzender Maßnahmen. Primäre Inhaltsverarbeitungen in Oracle Cloud Infrastructure und Supabase sind für den Standarddienst auf die dokumentierten Regionen Frankfurt ausgerichtet; technische Rand-, Support- oder Sicherheitsverarbeitungen einzelner Anbieter können in weiteren Ländern stattfinden.

10. Rückgabe und Löschung

1. Original-PDFs werden von RechneX nicht planmäßig dauerhaft gespeichert. Die KI-Verarbeitung erfolgt über für Zero Data Retention freigeschaltete zustandslose Mistral-Endpunkte. Hochgeladene Dateien in Validator und Viewer werden nach Abschluss der Anfrage verworfen.
2. Soweit Ergebnisdateien oder Prüfberichte in einem Downloadspeicher bereitgestellt werden, endet der Zugriff spätestens 24 Stunden nach ihrer Erzeugung. Die technische Bereinigung erfolgt anschließend in kurzen, regelmäßig ausgeführten Löschläufen.
3. Freiwillig gespeicherte Konto- oder Vorlagendaten bleiben bis zur Änderung, Löschung oder Beendigung des Kontos gespeichert, soweit keine gesetzlichen Pflichten oder berechtigten Nachweisinteressen entgegenstehen. Diese Verarbeitungen fallen nur insoweit unter diesen AVV, wie sie im Auftrag erfolgen.
4. Nach Ende der Auftragsverarbeitung löscht oder gibt RechneX die auftragsverarbeiteten Daten nach Wahl des Verantwortlichen zurück, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Sicherungskopien werden im Rahmen der regelmäßigen, technisch vorgesehenen Rotation überschrieben. Werden Sicherungen zur Wiederherstellung benötigt, werden zwischenzeitlich fällige Löschungen erneut angewendet.
5. Der Verantwortliche kann benötigte Ergebnisdateien während der Bereitstellungsfrist selbst herunterladen. Eine besondere Datenrückgabe, Wiederherstellung oder Migration außerhalb der Standardfunktion kann nach Aufwand vergütet werden.

11. Nachweise und Kontrollen

1. RechneX stellt auf Anfrage die für den Nachweis nach Art. 28 DSGVO erforderlichen Informationen zur Verfügung. Kontrollen erfolgen vorrangig durch aktuelle Dokumentationen, geeignete Prüfberichte, Fragebögen und Videokonferenzen.
2. Vor-Ort-Kontrollen sind zulässig, wenn Remote-Nachweise nicht ausreichen. Sie sind grundsätzlich einmal pro Kalenderjahr, mit mindestens 14 Tagen Vorlauf, während üblicher Geschäftszeiten und durch fachkundige, unabhängige und nicht konkurrierende Prüfer durchzuführen. Anlassbezogene Kontrollen nach einem erheblichen Sicherheitsvorfall oder auf verbindliche Anordnung einer Aufsichtsbehörde bleiben unberührt.
3. Kontrollen dürfen den Betrieb und die Sicherheit nicht unangemessen beeinträchtigen und keine Daten anderer Kunden, Geschäftsgeheimnisse oder Schwachstellen offenlegen. Prüfer sind zur Vertraulichkeit zu verpflichten.
4. Der Verantwortliche trägt seine Kontrollkosten und angemessenen Zusatzaufwand von RechneX, soweit die Kontrolle nicht eine wesentliche, von RechneX zu vertretende Vertragsverletzung bestätigt oder behördlich wegen eines von RechneX zu vertretenden Umstands angeordnet wurde.

12. Haftung und Zusammenarbeit bei Ansprüchen

1. Die zwingenden Rechte betroffener Personen und die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleiben unberührt.
2. Im Innenverhältnis tragen die Parteien Schäden und Aufwendungen entsprechend ihrem jeweiligen Verantwortungs- und Verursachungsanteil; Art. 82 Abs. 5 DSGVO bleibt maßgeblich.
3. Die Parteien informieren sich unverzüglich über gegen sie gerichtete Ansprüche, arbeiten bei der Abwehr angemessen zusammen und geben ohne vorherige Abstimmung keine den anderen Teil belastenden Anerkenntnisse oder Vergleiche ab; eine Zustimmung darf nicht unbillig verweigert werden. Beide Parteien sind zur angemessenen Schadensminderung verpflichtet.
4. Im Übrigen gelten die Haftungsbeschränkungen des Hauptvertrags beziehungsweise der AGB, soweit gesetzlich zulässig. Eine verschuldensunabhängige Freistellung oder Haftung für Umstände außerhalb des jeweiligen Verantwortungsbereichs wird nicht begründet.

13. Vertraulichkeit und Schlussbestimmungen

1. Beide Parteien behandeln nicht öffentliche Informationen aus der Auftragsverarbeitung vertraulich.
2. Änderungen und Ergänzungen dieses AVV bedürfen mindestens der Textform. RechneX überschreibt abgeschlossene Fassungen nicht. Eine neue AVV-Version wird nur durch erneute ausdrückliche Annahme Vertragsbestandteil, sofern nicht lediglich für den Verantwortlichen ausschließlich vorteilhafte, rein redaktionelle oder gesetzlich zwingende Anpassungen ohne nachteilige Auswirkung erfolgen.
3. Sollte eine Bestimmung unwirksam sein, bleibt der übrige AVV wirksam. Anstelle der unwirksamen Regelung gilt die gesetzlich zulässige Regelung, die dem Zweck am nächsten kommt.
4. Es gilt deutsches Recht, soweit gesetzlich zulässig. Die deutsche Fassung ist verbindlich; Übersetzungen dienen der Information.

Anlage 1 – Genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Ort	Aufgabe im Auftrag	Vorgesehene Verarbeitung / Schutzrahmen
Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA	globale Edge-Standorte	Auslieferung, Routing, DDoS-Schutz, WAF und technische Anfrageverarbeitung	Inhalts- und technische Metadaten soweit für Transport und Schutz erforderlich; DPA, EU-Standardvertragsklauseln und weitere Garantien nach Kapitel V DSGVO
Mistral AI SAS, 15 rue des Halles, 75001 Paris, Frankreich	Europäische Union	OCR und KI-gestützte Extraktion	Scale Plan API mit aktiviertem Zero Data Retention über zustandslose Endpunkte; keine Nutzung von API-Inhalten zum Modelltraining; Mistral-DPA
ORACLE Deutschland B.V. & Co. KG, Riesstraße 25, 80992 München, Deutschland	Oracle Cloud Region eu-frankfurt-1	Betrieb der KoSIT- und Mustang-Validator-Dienste	temporäre Verarbeitung von XML-/PDF-Inhalten und technischen Metadaten; Oracle-Datenschutzvereinbarungen und EU-Region
Supabase Pte. Ltd., 65 Chulia Street #38-02/03, OCBC Centre, Singapur 049513	primäre Projektregion Frankfurt (eu-central-1); weitere Support-/Unterauftragsstandorte möglich	Authentifizierungs-, Datenbank-, Speicher- und Jobfunktionen	DPA, dokumentierte Projektregion und Garantien nach Kapitel V DSGVO

Zahlungsdienste, optionale externe Anmeldung, allgemeiner Support und transaktionale Vertrags-E-Mails werden von RechneX für eigene Vertrags- und Geschäftszwecke eingesetzt und sind deshalb nicht als Unterauftragsverarbeiter dieses engen Verarbeitungsauftrags aufgeführt.

Anlage 2 – Technische und organisatorische Maßnahmen

1. Vertraulichkeit

- verschlüsselte Übertragung über TLS;
- rollen- und aufgabenbezogene Zugriffe nach dem Prinzip der geringsten Berechtigung;
- serverseitige Verwaltung von Zugangsdaten und API-Schlüsseln;
- logische Mandantentrennung, Datenbankregeln auf Zeilenebene und getrennte Speicherpfade;
- Vertraulichkeitsverpflichtung für zugriffsberechtigte Personen;
- administrative Mehrfaktor-Authentifizierung, soweit vom jeweiligen System unterstützt und eingerichtet.

2. Integrität

- Eingabeprüfung, Größen- und Formatgrenzen sowie technische Validierung;
- kontrollierte Softwarebereitstellung und Versionsverwaltung;
- Schutz vor unbefugter Veränderung durch Authentifizierung und Berechtigungsprüfungen;
- protokollierte Vertragsversionen und unveränderliche Annahmenachweise mit SHA-256-Dokumenthash.

3. Verfügbarkeit und Belastbarkeit

- Edge-Schutz, Rate-Limits, DDoS-Schutz und Web Application Firewall;
- verwaltete Cloud-Infrastruktur mit Überwachung und Fehlerprotokollierung;
- Sicherungs- und Wiederherstellungsverfahren des Datenbankanbieters im Umfang des gebuchten Dienstes;
- dokumentierte Reaktion auf Sicherheits- und Betriebsstörungen.

4. Trennung, Datenminimierung und Löschung

- getrennte Produktfunktionen und zweckbezogene Datenflüsse;
- keine planmäßige dauerhafte Speicherung hochgeladener Original-PDFs;

- Zero Data Retention für die eingesetzten zustandslosen Mistral-API-Endpunkte;
- Validator-Dienste in Oracle Cloud Infrastructure, Region Frankfurt;
- primäre Supabase-Projektregion Frankfurt;
- zeitlich begrenzte Downloadbereitstellung und regelmäßige technische Bereinigung;
- keine planmäßige Aufnahme von Rechnungsinhalten in reguläre Anwendungsprotokolle.

5. Wirksamkeitskontrolle

- regelmäßige Überprüfung relevanter Berechtigungen, Abhängigkeiten und Schutzkonfigurationen;
- Fehler- und Sicherheitsanalyse sowie risikobasierte Korrekturmaßnahmen;
- Anpassung der Maßnahmen bei wesentlichen Änderungen der Verarbeitung oder erkannten Risiken.