Vertrag zur Auftragsverarbeitung (AVV)

Aura UG (haftungsbeschränkt) · Stand 8. November 2026

Fassung vom 8. November 2026. Vertrag über die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 Abs. 3 DSGVO zwischen Ihnen als Verantwortlichem („Auftraggeber“) und der Aura UG (haftungsbeschränkt), Ludwig-Erhard-Straße 18, 20459 Hamburg, Deutschland, Amtsgericht Hamburg, HRB 192077 („Auftragnehmer“ oder „wir“).

1. Geltung und Abschluss

Dieser Vertrag gilt für jede Nutzung des Dienstes E-Rechnungslotse (erechnungslotse.de), bei der Sie als Unternehmen oder sonst als Verantwortlicher Dateien mit personenbezogenen Daten hochladen oder solche Daten in eine Rechnung eingeben, auch bei kostenloser Nutzung ohne Konto. Er wird mit dem Hochladen einer Datei oder mit dem Erstellen einer Rechnung Bestandteil des Nutzungsvertrags nach unseren Allgemeinen Geschäftsbedingungen und geht diesen in Fragen des Datenschutzes vor.

Der Vertrag liegt in elektronischer Form vor (Art. 28 Abs. 9 DSGVO). Sie können ihn auf dieser Seite abrufen, speichern und ausdrucken. Wer den Dienst ausschließlich für persönliche oder familiäre Zwecke nutzt, fällt nicht unter die DSGVO (Art. 2 Abs. 2 lit. c DSGVO); für diese Nutzung ist der Vertrag gegenstandslos.

2. Gegenstand und Dauer

Gegenstand ist die Prüfung und Anzeige elektronischer Rechnungen, die der Auftraggeber hochlädt, das Umwandeln hochgeladener Rechnungen (PDF, Word, Excel) in E-Rechnungen und das Erstellen von E-Rechnungen aus Formulardaten. Die Verarbeitung einer Datei beginnt mit dem Hochladen und endet mit der Löschung ihrer Inhalte, spätestens 24 Stunden nach dem Hochladen. Der Vertrag endet, wenn die letzte Datei des Auftraggebers gelöscht ist.

3. Art und Zweck der Verarbeitung

Wir verarbeiten die Daten ausschließlich, um die vom Auftraggeber angeforderte Leistung zu erbringen:

- Empfang der Datei über das Netz von Cloudflare und Speicherung im Dateispeicher
- automatische Prüfung mit dem KoSIT-Validator (XRechnung) bzw. Mustang (ZUGFeRD, Factur-X) und Speicherung des Prüfberichts in unserer Datenbank
- lesbare Darstellung der Rechnung und Erzeugung von Ansicht und Prüfbericht als PDF
- Bereitstellung des Ergebnisses über einen zufällig erzeugten Link
- beim Umwandeln: Umwandlung von Word- und Excel-Dateien in PDF, Auslesen des Textes, Auslesen der Rechnungsfelder aus dem Text durch ein Sprachmodell oder feste Regeln, Speicherung der Felder zur Bearbeitung durch den Auftraggeber
- beim Umwandeln und Erstellen: Erzeugung einer XRechnung (XML) oder eines ZUGFeRD-PDFs aus den Feldern und Prüfung der erzeugten Datei vor dem Download
- Löschung nach 24 Stunden oder sofort auf Anforderung („Jetzt löschen“)

Wir verarbeiten die Daten nicht für eigene Zwecke. Wir sehen sie nicht ein, werten sie nicht aus und verwenden sie nicht zum Training von KI-Modellen.

4. Art der Daten

Verarbeitet werden die Daten, die in den hochgeladenen Rechnungen enthalten sind, insbesondere:

- Namen, Firmen und Anschriften von Verkäufer, Käufer, Zahlungsempfänger und Lieferanschrift
- Kontaktdaten von Ansprechpartnern, etwa Name, E-Mail-Adresse und Telefonnummer
- Bankverbindungen, etwa IBAN, BIC und Kontoinhaber
- Steuer- und Registerangaben, etwa Umsatzsteuer-Identifikationsnummer, Steuernummer und Handelsregisternummer
- Rechnungs- und Vertragsdaten, etwa Positionen, Beträge, Leistungszeitraum, Bestell- und Vertragsnummern und Leitweg-ID
- Freitexte und Anhänge der Rechnung sowie der Dateiname

Der Dienst ist nicht für besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) bestimmt. Laden Sie Rechnungen mit solchen Daten nur hoch, wenn Sie das nach eigener Prüfung verantworten können.

5. Betroffene Personen

- Inhaber, Mitarbeiter und Ansprechpartner des Auftraggebers
- Kunden und Lieferanten des Auftraggebers sowie deren Inhaber, Mitarbeiter und Ansprechpartner
- Kontoinhaber und sonstige Personen, die in den Rechnungen genannt sind

6. Weisungen

Wir verarbeiten die Daten nur auf dokumentierte Weisung des Auftraggebers, auch bei einer Übermittlung in ein Drittland, es sei denn, das Recht der Union oder eines Mitgliedstaats verpflichtet uns zu einer Verarbeitung. In diesem Fall teilen wir dem Auftraggeber diese rechtlichen Anforderungen vorher mit, sofern das Recht eine solche Mitteilung nicht verbietet (Art. 28 Abs. 3 lit. a DSGVO).

Die Weisungen sind durch diesen Vertrag und durch die Bedienung des Dienstes festgelegt: Hochladen, Wahl von Prüfung, Ansicht oder PDF, Bearbeiten und Erzeugen einer Rechnung, und Löschen. Weitere Weisungen erteilt der Auftraggeber in Textform an hello@erechnungslotse.de. Halten wir eine Weisung für rechtswidrig, teilen wir das dem Auftraggeber unverzüglich mit (Art. 28 Abs. 3 Unterabs. 2 DSGVO).

7. Vertraulichkeit

Zugang zu den Systemen, auf denen die Daten verarbeitet werden, haben nur Personen, die wir zur Vertraulichkeit verpflichtet haben oder die einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Verpflichtung gilt auch nach dem Ende ihrer Tätigkeit.

8. Sicherheit der Verarbeitung

Wir treffen die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in der Anlage beschrieben sind. Wir passen sie an den Stand der Technik an. Das Schutzniveau darf dabei nicht sinken.

9. Unterauftragsverarbeiter

Der Auftraggeber erlaubt uns, die folgenden Unterauftragsverarbeiter einzusetzen (Art. 28 Abs. 2 DSGVO):

Unternehmen	Leistung	Ort der Verarbeitung
Hosting-Anbieter in der EU, Rechenzentrum in Polen. Den Namen nennen wir Auftraggebern auf Anfrage.	Dedizierter Server für Webseite, Datenbank und Prüfwerkzeuge	Polen
Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA	Verbindung zu unserem Server und Schutz vor Angriffen (Cloudflare Tunnel). Speicherung hochgeladener Dateien (R2)	Dateien: Europäische Union. Übertragung: weltweites Netz, in der Regel ein Rechenzentrum in der Nähe des Nutzers. Übermittlung in die USA auf Grundlage des EU-US-Datenschutzrahmens (Art. 45 DSGVO) und der Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO)
Mistral AI SAS, Paris, Frankreich	Nur beim Umwandeln: Auslesen der Rechnungsfelder aus dem Text der hochgeladenen Rechnung mit einem Sprachmodell	Europäische Union
Cloudflare, Inc. (Anschrift oben), Dienst Email Routing	Nur wenn der Auftraggeber uns Rechnungsdaten per E-Mail schickt, etwa bei einer Supportanfrage: Empfang der E-Mail an unsere Kontaktadresse und Weiterleitung an unser Postfach	Weltweites Netz, auch USA. Übermittlung in die USA wie oben
Proton AG, Route de la Galaise 32, 1228 Plan-les-Ouates, Schweiz	Nur wenn der Auftraggeber uns Rechnungsdaten per E-Mail schickt: Speicherung der E-Mail in unserem Postfach	Schweiz, Deutschland oder Norwegen. Für die Schweiz gilt ein Angemessenheitsbeschluss (Art. 45 DSGVO, Entscheidung 2000/518/EG)

Word- und Excel-Dateien wandelt beim Umwandeln der Dienst switchfile in ein PDF um. switchfile betreibt der Auftragnehmer selbst (Aura UG). switchfile ist deshalb kein Unterauftragsverarbeiter, sondern Teil unserer eigenen Verarbeitung; es gelten dieser Vertrag und seine Anlage unmittelbar. switchfile nutzt dieselben Unterauftragsverarbeiter, den Hosting-Anbieter (Server in Polen) und Cloudflare (Dateispeicher R2 in der EU). Wir löschen die Datei bei switchfile direkt nach der Umwandlung, spätestens nach einem Tag. Betreibt künftig ein anderes Unternehmen switchfile, nehmen wir es nach dem folgenden Verfahren in die Liste auf.

Wir verpflichten jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, wie sie dieser Vertrag vorsieht (Art. 28 Abs. 4 DSGVO). Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haften wir dem Auftraggeber gegenüber dafür.

Unterauftragsverarbeiter, die beim Hochladen einer Datei oder beim Erstellen einer Rechnung in dieser Liste stehen, genehmigt der Auftraggeber mit dem Abschluss dieses Vertrags. Wollen wir einen weiteren Unterauftragsverarbeiter einsetzen oder einen ersetzen, veröffentlichen wir die geänderte Liste mindestens 30 Tage vor dem Einsatz auf dieser Seite. Inhaber eines Kontos informieren wir zusätzlich per E-Mail an die Adresse des Kontos. Der Auftraggeber kann der Änderung bis zum Einsatz in Textform widersprechen. Nach einem Widerspruch verarbeiten wir seine Daten nicht mit dem neuen Unterauftragsverarbeiter. Kann der Dienst ohne ihn nicht erbracht werden, kann der Auftraggeber die betroffene Funktion nicht mehr nutzen.

10. Unterstützung des Auftraggebers

Wir unterstützen den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Kapitel III DSGVO zu beantworten (Art. 28 Abs. 3 lit. e DSGVO). Ohne Konto können wir eine Datei nur zuordnen, wenn der Auftraggeber uns den Link zum Ergebnis nennt; Umwandlungen ordnen wir dem Konto zu. Wendet sich eine betroffene Person direkt an uns, verweisen wir sie an den Auftraggeber, soweit wir ihn kennen.

Wir unterstützen den Auftraggeber bei seinen Pflichten aus Art. 32 bis 36 DSGVO (Art. 28 Abs. 3 lit. f DSGVO). Eine Verletzung des Schutzes personenbezogener Daten melden wir unverzüglich, nachdem sie uns bekannt geworden ist (Art. 33 Abs. 2 DSGVO), mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie uns vorliegen. Hat der Auftraggeber ein Konto, schreiben wir an die E-Mail-Adresse des Kontos. Ohne Konto haben wir keine Kontaktdaten des Auftraggebers. Dann veröffentlichen wir die Meldung auf der Webseite.

11. Löschung und Rückgabe

Wir löschen jede hochgeladene Datei und den zugehörigen Prüfbericht 24 Stunden nach dem Hochladen automatisch. Der Auftraggeber kann beides vorher mit „Jetzt löschen“ sofort löschen. Beim Umwandeln löschen wir die hochgeladene Datei direkt nach dem Auslesen und die ausgelesenen Felder 24 Stunden nach dem Hochladen. Mit dem Löschen des Kontos löschen wir alle Umwandlungen sofort. Von Dateien, Prüfberichten und Feldern legen wir keine Sicherungskopien an (Art. 28 Abs. 3 lit. g DSGVO).

Eine Rückgabe ist nicht vorgesehen: Die Originaldatei hat der Auftraggeber selbst, Ansicht und Prüfbericht kann er bis zur Löschung herunterladen.

12. Nachweise und Kontrollen

Wir stellen dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Pflichten aus Art. 28 DSGVO zur Verfügung und ermöglichen Überprüfungen, einschließlich Inspektionen, durch den Auftraggeber oder einen von ihm beauftragten Prüfer (Art. 28 Abs. 3 lit. h DSGVO). Anfragen richten Sie an hello@erechnungslotse.de.

Als Nachweis dienen in der Regel dieser Vertrag mit der Anlage und schriftliche Auskünfte. Inspektionen vereinbaren wir mit angemessener Vorankündigung. Sie dürfen den Betrieb nicht stören und die Vertraulichkeit der Daten anderer Auftraggeber nicht gefährden. Kontrollen bei Unterauftragsverarbeitern richten sich nach deren Verträgen, etwa über deren Prüfberichte.

13. Ort der Verarbeitung

Server, Dateispeicher und Sprachmodell-Anbieter liegen in der Europäischen Union. Über das Netz von Cloudflare können Daten bei der Übertragung auch außerhalb der EU verarbeitet werden. Schickt uns der Auftraggeber Rechnungsdaten per E-Mail, liegen sie in unserem Postfach bei Proton auch in der Schweiz oder in Norwegen. Dafür gelten die in Abschnitt 9 genannten Garantien.

14. Haftung und Schlussbestimmungen

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Verhältnis zwischen Auftraggeber und Auftragnehmer gilt im Übrigen die Haftungsregelung der AGB.

Für jede Nutzung gilt die Fassung dieses Vertrags, die beim Hochladen einer Datei oder beim Erstellen einer Rechnung auf dieser Seite steht. Es gilt deutsches Recht. Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam.

Anlage: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Verschlüsselung

- Verbindungen zwischen Browser und Cloudflare nur verschlüsselt (TLS).
- Verbindung zwischen Cloudflare und unserem Server über einen verschlüsselten Tunnel (Cloudflare Tunnel).
- Verbindung zwischen unserem Server und dem Dateispeicher nur verschlüsselt (HTTPS). Der Dateispeicher (Cloudflare R2) speichert alle Dateien verschlüsselt (AES-256).

Zugang und Zugriff

- Der Server ist aus dem Internet nur über Cloudflare Tunnel erreichbar. Datenbank und Prüfwerkzeuge sind nur im internen Netz des Servers erreichbar.
- Zugangsdaten für Datenbank und Dateispeicher liegen nur auf dem Server und werden nicht protokolliert.
- Administrativen Zugang zum Server hat nur der Geschäftsführer.
- Das Ergebnis einer Prüfung ist nur über einen zufällig erzeugten Link mit 128 Bit Zufall abrufbar. Es gibt keine Liste oder Suche hochgeladener Dateien.
- Der Server steht im Rechenzentrum des Hosters in Polen. Zutritt und physische Sicherung regelt der Hoster.

Trennung und Datenminimierung

- Prüfen, Anzeigen und Erstellen sind ohne Konto möglich. Für das Umwandeln ist ein Konto nötig; dafür speichern wir E-Mail-Adresse, Name und Passwort-Hashwert.
- Umwandlungen sind nur für das Konto abrufbar, das sie angelegt hat.
- An den Sprachmodell-Anbieter geht nur der Text der hochgeladenen Rechnung, keine Angaben zum Konto. Ohne konfigurierten Anbieter liest unser Server die Felder selbst mit festen Regeln aus.
- Jede Datei wird unter einem eigenen, zufälligen Schlüssel gespeichert und nur für die angeforderte Leistung verarbeitet.
- Die Prüfwerkzeuge laufen in einem eigenen Dienst ohne Verbindung ins Internet.

- Für die Begrenzung der Uploads speichern wir nur einen Hashwert der IP-Adresse, höchstens zwei Stunden lang.
- Protokolle enthalten keine Rechnungsinhalte und keine IP-Adressen.

Integrität und Schutz vor Angriffen

- XML-Parser lösen keine externen Entitäten auf (Schutz vor XXE). Transformationen greifen nicht auf das Netz zu.
- Grenzen für Dateigröße, Seitenzahl sowie Zahl und Größe eingebetteter Anhänge.
- Zeitlimits und Speichergrenzen für jede Prüfung.
- Die lesbare Ansicht wird in einem abgeschotteten Rahmen mit strikter Content Security Policy angezeigt.
- Begrenzung der Uploads je Besucher und Stunde. Schutz vor Angriffen durch Cloudflare.

Löschung

- Ein Hintergrunddienst löscht Dateien und Prüfberichte automatisch 24 Stunden nach dem Hochladen.
- Beim Umwandeln löschen wir die hochgeladene Datei direkt nach dem Auslesen. Ausgelesene Felder und Dateiname löschen wir 24 Stunden nach dem Hochladen; im Verlauf des Kontos bleiben nur Datum, Art der Vorlage, Status und Format.
- Erzeugte E-Rechnungen speichern wir nicht.
- Der Nutzer kann beides jederzeit sofort löschen („Jetzt löschen“).
- Von Dateien und Prüfberichten werden keine Sicherungskopien angelegt.

Verfügbarkeit und Überprüfung

- Sicherheitsupdates für Betriebssystem, Prüfwerkzeuge und Bibliotheken spielen wir zeitnah ein, Sicherheits-Releases der XRechnung-Visualisierung sofort.
- Wir überprüfen die Maßnahmen bei jeder wesentlichen Änderung des Dienstes und mindestens einmal im Jahr.