

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Stand: 12.10.2026

Vertragsparteien

Verantwortlicher (Auftraggeber): der Kunde von E-Rechnung leicht, wie in seinem Kundenkonto angegeben (im Folgenden „Kunde“)

Auftragsverarbeiter (Auftragnehmer): IDO GmbH, Anderslebener Straße 40, 39387 Oschersleben, vertreten durch den Geschäftsführer Martin Leue, E-Mail info@erechnung-leicht.de (im Folgenden „wir“)

Dieser Vertrag ist Bestandteil der Allgemeinen Geschäftsbedingungen von E-Rechnung leicht (§ 7 AGB) und gilt für jedes Kundenkonto, ohne dass er gesondert unterschrieben werden muss. Er wird in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO). Die aktuelle Fassung steht unter <https://erechnung-leicht.de/avv>; im Kundenkonto steht sie unter „Einstellungen“ als PDF mit den Firmendaten des Kunden bereit.

§ 1 Gegenstand und Dauer

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch uns im Auftrag des Kunden, wenn er E-Rechnung leicht (erechnung-leicht.de) mit einem Kundenkonto nutzt. Den Umfang der Leistungen beschreiben die AGB und die Preisseite. Dazu gehören, je nach Plan:

- Erstellen, Speichern und erneutes Abrufen von E-Rechnungen (XRechnung, ZUGFeRD) im Konto, auch mit eigenem Rechnungslayout und als Vorlage für neue Rechnungen,
- der Kundenstamm mit den Rechnungsempfängern des Kunden,
- der Rechnungseingang: PDF-Rechnungen, die der Kunde an seine persönliche Eingangsadresse weiterleitet oder im Konto hochlädt, werden ausgelesen und als Entwurf bereitgestellt; auf Wunsch betten wir die Rechnungsdaten in das Original-PDF des Kunden ein,
- der Versand von Rechnungen und Zahlungserinnerungen per E-Mail an die Rechnungsempfänger des Kunden sowie regelmäßige Rechnungen, auf Weisung des Kunden auch automatisch zu den von ihm eingestellten Terminen.

(2) Nicht Gegenstand dieses Vertrags sind Daten, die wir als eigener Verantwortlicher verarbeiten, zum Beispiel die Zugangs- und Abrechnungsdaten des Kundenkontos, Server-Protokolle, die Reichweitenmessung, Anfragen über das Kontaktformular und das kostenlose Anzeigen und Prüfen ohne Konto. Dafür gilt unsere Datenschutzerklärung.

(3) Der Vertrag gilt, solange das Kundenkonto besteht. Pflichten, die ihrer Natur nach über das Vertragsende hinaus gelten, insbesondere zur Löschung und zur Vertraulichkeit, bleiben bestehen.

§ 2 Art und Zweck der Verarbeitung, Art der Daten, betroffene Personen

(1) **Art der Verarbeitung:** Erheben (Eingabe im Formular, Upload, Eingang per Mail), Auslesen, Speichern, Ordnen, Abfragen, Verwenden zum Erzeugen von Rechnungsdateien, Übermitteln per E-Mail an die vom Kunden bestimmten Empfänger und Löschen.

(2) **Zweck:** Erstellen, Aufbewahren im Konto und Versenden der elektronischen Rechnungen des Kunden.

(3) **Art der Daten:**

- Angaben zu Rechnungsempfängern und ihren Ansprechpartnern: Name oder Firma, Ansprechpartner, Anschrift, Land, E-Mail-Adresse, USt-IdNr., Steuernummer, Leitweg-ID, abweichende Lieferanschrift sowie Notizen des Kunden im Kundenstamm,
- Rechnungsdaten: Rechnungsnummer, Datum, Leistungen und Positionen, Beträge, Zahlungsbedingungen, Bestell- und Referenznummern, Zahlungsstand,
- Inhalte des Rechnungseingangs: weitergeleitete oder hochgeladene Rechnungsdateien, Absender und Betreff der Mail sowie deren Text (etwa eine Signatur),
- Versanddaten: Empfängeradresse, Betreff und Text der Mail, Zeitpunkt und Ergebnis des Versands,
- Angaben des Kunden auf seinen Rechnungen, soweit sie Personen betreffen (zum Beispiel Name der Geschäftsführung oder eines Ansprechpartners, Bankverbindung).

(4) **Betroffene Personen:** Kunden und Auftraggeber des Kunden (Rechnungsempfänger) und deren Ansprechpartner sowie Beschäftigte und Vertreter des Kunden, soweit sie in Rechnungen, Mails oder Signaturen genannt sind.

§ 3 Weisungen

(1) Wir verarbeiten die Daten nur auf dokumentierte Weisung des Kunden. Die Weisungen ergeben sich aus diesem Vertrag und aus der Nutzung der Funktionen von E-Rechnung leicht: Was der Kunde im Konto eingibt, hochlädt, einstellt, versendet oder löscht, gilt als Weisung. Weitere Weisungen erteilt der Kunde in Textform, etwa per E-Mail an info@erechnung-leicht.de. Weisungsberechtigt ist, wer Zugang zum Kundenkonto hat oder den Kunden vertritt.

(2) Zahlungserinnerungen und regelmäßige Rechnungen, die der Kunde auf automatischen Versand gestellt hat, versenden wir auf seine Weisung an die Empfänger, mit den Inhalten und zu den Terminen, die er festgelegt hat.

(3) Verpflichtet uns das Recht der EU oder Deutschlands zu einer anderen Verarbeitung, teilen wir dem Kunden das vorher mit, sofern das Recht diese Mitteilung nicht verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(4) Halten wir eine Weisung für rechtswidrig, weisen wir den Kunden unverzüglich darauf hin (Art. 28 Abs. 3 Satz 3 DSGVO).

§ 4 Unsere Pflichten

(1) Wir verarbeiten die Daten ausschließlich, um die vereinbarten Leistungen zu erbringen, nicht für eigene Zwecke, nicht für Werbung und nicht zum Training von KI-Modellen.

(2) Personen, die bei uns Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht (Art. 28 Abs. 3 lit. b DSGVO).

(3) Wir treffen die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Wir dürfen sie an den Stand der Technik anpassen, solange das Schutzniveau nicht sinkt.

(4) Wir unterstützen den Kunden mit geeigneten Maßnahmen dabei, Anfragen betroffener Personen zu beantworten (Art. 12 bis 23 DSGVO). Vieles kann der Kunde selbst im Konto erledigen: Rechnungen herunterladen, Kunden im Kundenstamm ändern oder löschen, Eingänge löschen. Wenden sich Betroffene direkt an uns, leiten wir die Anfrage unverzüglich an den Kunden weiter.

(5) Wir unterstützen den Kunden bei seinen Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung) im Rahmen der Art der Verarbeitung und der

uns vorliegenden Informationen.

(6) Werden uns Verletzungen des Schutzes personenbezogener Daten des Kunden bekannt, melden wir sie dem Kunden unverzüglich per E-Mail an die Adresse seines Kundenkontos, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie uns vorliegen.

(7) Wir verarbeiten die Daten in Deutschland. Eine Übermittlung in ein Drittland findet nur nach § 7 statt.

§ 5 Pflichten des Kunden

(1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen verantwortlich. Er bestimmt, welche Daten er eingibt, an wen Rechnungen und Erinnerungen gehen und was darin steht.

(2) Er informiert uns unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

(3) Hinterlegt der Kunde einen eigenen Mailserver für den Versand, gehen seine Mails über diesen Server. Dessen Betreiber ist nicht unser Unterauftragsverarbeiter; das Verhältnis besteht allein zwischen dem Kunden und seinem Anbieter.

§ 6 Unterauftragsverarbeiter

(1) Der Kunde ist mit den in Anlage 2 genannten Unterauftragsverarbeitern einverstanden (allgemeine Genehmigung nach Art. 28 Abs. 2 DSGVO).

(2) Wollen wir einen Unterauftragsverarbeiter hinzunehmen oder ersetzen, informieren wir den Kunden mindestens vier Wochen vorher per E-Mail an die Adresse seines Kundenkontos. Der Kunde kann der Änderung bis zu ihrem Wirksamwerden in Textform widersprechen. Können wir den Einwand nicht ausräumen, kann der Kunde den Vertrag zum Wirksamwerden der Änderung kündigen.

(3) Wir verpflichten jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieses Vertrags entsprechen (Art. 28 Abs. 4 DSGVO).

(4) Keine Unterauftragsverarbeiter im Sinne dieses Vertrags sind der Zahlungsdienstleister Stripe, der nur die Daten des Abos verarbeitet (dafür sind wir selbst Verantwortlicher), die Mailserver der Empfänger und ein vom Kunden hinterlegter eigener Mailserver.

§ 7 Übermittlung in Drittländer

(1) Die Verarbeitung findet auf unseren Servern in Deutschland statt. Das gilt auch für das Erstellen der Rechnungsdateien, das Einbetten der Rechnungsdaten in das Original-PDF und den Mailversand.

(2) Einzige Ausnahme ist das Auslesen normaler PDF-Rechnungen ohne eingebettete E-Rechnung, die per Mail oder Upload in den Rechnungseingang kommen: Dafür übermitteln wir das PDF und gegebenenfalls den Text der weitergeleiteten Mail an Anthropic, PBC in den USA (Anlage 2). Grundlage sind Standardvertragsklauseln der EU-Kommission (Art. 46 Abs. 2 lit. c DSGVO) im Rahmen des Vertrags zur Auftragsverarbeitung mit Anthropic. E-Rechnungen (XRechnung, ZUGFeRD) lesen wir ohne KI; ist das monatliche KI-Kontingent des Plans aufgebraucht, lesen wir per Texterkennung auf unserem eigenen Server.

(3) Wer keine Übermittlung in die USA möchte, erstellt seine Rechnungen über das Formular; dabei wird nichts an Anthropic übermittelt.

§ 8 Nachweise und Kontrollen

(1) Wir weisen die Einhaltung unserer Pflichten in erster Linie durch Auskünfte und Unterlagen nach, etwa die Beschreibung der Maßnahmen in Anlage 1 und Nachweise unserer Unterauftragsverarbeiter (zum Beispiel das ISO/IEC-27001-Zertifikat der Hetzner Online GmbH für ihre Rechenzentren).

(2) Reicht das nicht aus, kann der Kunde sich nach Anmeldung mit angemessener Frist während der üblichen Geschäftszeiten selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer von der Einhaltung überzeugen (Art. 28 Abs. 3 lit. h DSGVO). Die Kontrolle darf den Betrieb nicht unverhältnismäßig stören und muss die Vertraulichkeit der Daten anderer Kunden wahren. Prüfer, die mit uns im Wettbewerb stehen, dürfen wir ablehnen.

§ 9 Löschung und Rückgabe

(1) Der Kunde kann seine Rechnungen jederzeit als ZUGFeRD-PDF oder XRechnung herunterladen. Kunden im Kundenstamm, Eingänge und das ganze Konto löscht er selbst im Konto.

(2) Löscht der Kunde sein Konto, löschen wir alle Daten, die wir in seinem Auftrag verarbeiten, sofort aus der Anwendung. Vorher sollte der Kunde die Rechnungen herunterladen, die er aufbewahren muss; nach der Löschung ist das nicht mehr möglich.

(3) Unabhängig davon löschen wir automatisch:

Daten	Löschung
Rechnungen, Kundenstamm, Firmendaten, Rechnungslayout mit Logo, regelmäßige Rechnungen und Einstellungen	mit dem Löschen des Kontos (Konto › Einstellungen); einzelne Kunden und Eingänge jederzeit selbst
Ersetztes Logo	sobald es auf keiner Rechnung des Kontos mehr steht
Weitergeleitete Mail im Abholpostfach	direkt nach der Abholung (jede Minute)
Original-Datei im Rechnungseingang (Mail-Anhang oder Upload)	sobald daraus eine E-Rechnung erstellt ist, sonst nach 60 Tagen
Eintrag im Rechnungseingang ohne Datei	nach 180 Tagen
Abgewiesene Mails (Absender nicht freigegeben) und nicht lesbare Eingänge, ohne Anhang	nach 14 Tagen
Protokoll automatisch versendeter Mails (Zeitpunkt, Empfängeradresse, Art, Ergebnis, ohne Inhalt)	nach 400 Tagen
Datenbanksicherungen vor Aktualisierungen der Anwendung	die letzten 14 Sicherungen bleiben, ältere werden gelöscht

(4) In Datenbanksicherungen bleiben gelöschte Daten enthalten, bis die jeweilige Sicherung gelöscht wird (siehe Tabelle); sie werden nur zur Wiederherstellung nach einem Fehler verwendet.

§ 10 Haftung und Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO; im Übrigen gelten die Haftungsregeln der AGB (§ 8).

(2) Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes den AGB vor.

(3) Es gilt deutsches Recht. Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- **Rechenzentrum:** Unsere Server stehen im Rechenzentrum der Hetzner Online GmbH in Nürnberg. Zutritt und physische Sicherheit regelt Hetzner; deren Informationssicherheits-Managementsystem ist nach ISO/IEC 27001 zertifiziert (ein Zertifikat von Hetzner, nicht der IDO GmbH). Wir selbst haben keinen physischen Zugang zu den Servern.
- **Zugang zu den Servern:** nur für beauftragte Administratoren der IDO GmbH, nur über verschlüsselte Verbindungen.
- **Anmeldung im Kundenkonto:** Passwort mit mindestens 10 Zeichen, gespeichert nur als Hash (Argon2id). Freiwillig Zwei-Faktor-Anmeldung mit einer Authenticator-App (TOTP) und 10 Notfallcodes, die nur als HMAC gespeichert werden; ein Code gilt nur einmal. Nach 10 Fehlversuchen in 15 Minuten (je Anschluss und je Konto) ist die Anmeldung gesperrt. Ändert sich das Passwort oder die Zwei-Faktor-Anmeldung, werden alle anderen Sitzungen ungültig.
- **Sitzung:** Sitzungs-Cookie nur über HTTPS, für Skripte nicht lesbar (HttpOnly), nicht an fremde Seiten mitgesendet (SameSite), ungültig nach 8 Stunden ohne Aktivität.
- **Trennung:** Jede Abfrage auf Kundendaten ist an das angemeldete Kundenkonto gebunden; ein Konto sieht nur seine eigenen Rechnungen, Kunden und Eingänge. Unsere Betreiber-Übersicht zeigt Kennzahlen und Kontodaten, keine Rechnungsinhalte.
- **Verschlüsselung:** Alle Verbindungen zur Anwendung laufen über HTTPS (TLS) mit HSTS. Zugangsdaten zu einem eigenen Mailserver des Kunden und das Geheimnis der Zwei-Faktor-Anmeldung speichern wir mit AES-256-GCM verschlüsselt.

Integrität

- **Schutz der Anwendung:** CSRF-Schutz für alle Formulare im Konto, strenge Content-Security-Policy, keine Skripte oder Schriften fremder Anbieter, Einbetten in fremde Seiten untersagt (X-Frame-Options DENY), Bot-Schutz ohne externen Dienst.
- **Rechnungseingang:** Mails werden nur von freigegebenen Absendern angenommen, Mails mit fehlgeschlagener DMARC-Prüfung abgewiesen, höchstens 100 Mails je Tag und Konto. Mails an unbekannte Eingangsadressen werden verworfen.
- **Nachvollziehbarkeit:** An jeder Rechnung steht, wann und an wen sie versendet wurde und wann zuletzt erinnert wurde. Automatisch versendete Mails werden mit Zeitpunkt, Empfänger und Ergebnis protokolliert.
- **Grenzen gegen Missbrauch:** Versand höchstens 60 Mails je Stunde und 300 je Tag und Konto; Ratenbegrenzung für Uploads und Anmeldung.

Verfügbarkeit und Belastbarkeit

- Vor jeder Aktualisierung der Anwendung wird der neue Stand automatisch geprüft und die Datenbank gesichert; die letzten 14 Sicherungen bleiben erhalten. Bei einem Fehler lässt sich der vorherige Stand wiederherstellen.
- Regelmäßige zusätzliche Sicherungen an einem getrennten Ort richten wir als Betreiber ein; diese Anlage wird ergänzt, sobald sie bestehen.

Regelmäßige Überprüfung

- Wir überprüfen die Maßnahmen bei jeder wesentlichen Änderung der Anwendung und passen sie an den Stand der Technik an. Unterauftragsverarbeiter setzen wir nur mit Vertrag zur Auftragsverarbeitung ein (Anlage 2).

Anlage 2: Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Deutschland	Rechenzentrum und Server (Hetzner Cloud), auf denen wir die Anwendung, die Datenbank und unsere Mailserver für Versand und Rechnungseingang betreiben	Deutschland (Rechenzentrum Nürnberg) kein Drittland
Anthropic, PBC 548 Market Street, San Francisco, CA 94104, USA	KI-Dienst „Claude“: liest normale PDF-Rechnungen ohne eingebettete E-Rechnung aus, die per Mail oder Upload in den Rechnungseingang kommen (PDF und gegebenenfalls Text der weitergeleiteten Mail)	USA Standardvertragsklauseln der EU-Kommission (Art. 46 Abs. 2 lit. c DSGVO)

Stand dieser Fassung: 12.10.2026

Dokument erstellt am 13.10.2026 aus <https://erechnung-leicht.de/avv>. Elektronisch geschlossen als Bestandteil der AGB, ohne Unterschrift gültig (Art. 28 Abs. 9 DSGVO). IDO GmbH · Anderslebener Straße 40 · 39387 Oschersleben · Amtsgericht Stendal, HRB 106935