Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO für belege.ai

Stand: 15. Juni 2026

Dieser Auftragsverarbeitungsvertrag („AVV“) konkretisiert die Verarbeitung personenbezogener Daten durch die digitally induced GmbH im Auftrag des Kunden bei Nutzung von belege.ai. Er gilt zusammen mit der Nutzungsvereinbarung und einer etwaigen Bestellung oder Individualvereinbarung als Hauptvertrag.

Parteien

Dieser AVV wird geschlossen zwischen dem Kunden, der belege.ai im eigenen Namen oder im Namen einer Organisation nutzt (nachfolgend „Auftraggeber“oder „Verantwortlicher“), und

digitally induced GmbH
Schanzenstraße 96
40549 Düsseldorf
Deutschland

als Auftragsverarbeiter (nachfolgend „Auftragnehmer“oder „Auftragsverarbeiter“). Auftraggeber und Auftragnehmer werden gemeinsam die „Parteien“genannt.

1. Gegenstand und Rangfolge

1. Der Auftragnehmer stellt dem Auftraggeber die Software belege.ai bereit. Der Dienst sammelt, verarbeitet und ordnet Belege, Rechnungen, Quittungen und verwandte Dokumente aus Banktransaktionen, E-Mail-Postfächern, Telegram-Nachrichten, Uploads, Portalen und angebundenen Drittservices. Dazu gehören insbesondere Belegsuche, Belegzuordnung, KI-gestützte Extraktion, Browser-Automatisierung, Bewirtungsbelege, Eigenbelege, Reisekostenabrechnungen und Exporte für Buchhaltung oder Steuerberatung.
2. Soweit der Auftragnehmer dabei personenbezogene Daten verarbeitet, für die der Auftraggeber Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist, erfolgt diese Verarbeitung ausschließlich im Auftrag und nach Weisung des Auftraggebers nach Maßgabe dieses AVV.
3. Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV für datenschutzrechtliche Fragen der Auftragsverarbeitung vor.

2. Art, Zweck und Dauer der Verarbeitung

1. Art, Zweck, Umfang, Kategorien personenbezogener Daten und Kategorien betroffener Personen ergeben sich aus Anlage 1.
2. Die Verarbeitung dient der vertragsgemäßen Bereitstellung von belege.ai, insbesondere der automatisierten Suche, Extraktion, Zuordnung, Erzeugung, Verwaltung und Ausgabe von Belegen und buchhaltungsnahen Unterlagen.
3. Die Dauer der Verarbeitung richtet sich nach der Laufzeit des Hauptvertrags. Nach Ende des Hauptvertrags werden Auftraggeber-Daten nach Ziffer 10 gelöscht oder herausgegeben, soweit keine gesetzlichen Aufbewahrungspflichten oder berechtigten Nachweiszwecke entgegenstehen.

3. Weisungen des Auftraggebers

1. Die Weisungen des Auftraggebers ergeben sich anfänglich aus diesem AVV, dem Hauptvertrag, den Einstellungen im Produkt, verbundenen Integrationen sowie den vom Auftraggeber oder seinen Nutzern erteilten Anweisungen über Weboberfläche, Telegram, E-Mail oder API.
2. Einzelweisungen können in Textform erteilt werden. Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, werden als Antrag auf Leistungs- oder Vertragsänderung behandelt.
3. Der Auftragnehmer verarbeitet Auftraggeber-Daten nur auf dokumentierte Weisung des Auftraggebers, sofern er nicht nach Unionsrecht oder deutschem Recht zu einer anderen Verarbeitung verpflichtet ist. In diesem Fall informiert der Auftragnehmer den Auftraggeber vorab, soweit das betreffende Recht dies nicht untersagt.
4. Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen Datenschutzrecht verstößt, weist er den Auftraggeber darauf hin und darf die Durchführung der Weisung bis zur Bestätigung oder Änderung aussetzen.

4. Verantwortung des Auftraggebers

1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, die Rechtmäßigkeit der Übermittlung an den Auftragnehmer, die Richtigkeit der bereitgestellten Daten und die Wahrung der Rechte betroffener Personen verantwortlich.
2. Der Auftraggeber stellt sicher, dass nur berechtigte Nutzer Zugriff auf seinen Account, seine Organisation, verbundene Postfächer, Bankdaten, Portale und Exporte erhalten.
3. Der Auftraggeber ist dafür verantwortlich, Belege, Auswertungen, steuerliche Einordnungen, KI-Ausgaben und Exporte vor Verwendung zu prüfen. belege.ai ersetzt keine Rechts-, Steuer- oder Buchhaltungsberatung.

5. Vertraulichkeit und Personal

1. Der Auftragnehmer verpflichtet alle Personen, die Auftraggeber-Daten verarbeiten können, zur Vertraulichkeit, soweit sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
2. Der Zugriff auf Auftraggeber-Daten wird auf Personen beschränkt, die ihn zur Leistungserbringung, Wartung, Sicherheit, Support oder Fehleranalyse benötigen.

6. Sicherheit der Verarbeitung

1. Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Die zum Stand dieses AVV getroffenen Maßnahmen sind in Anlage 3 beschrieben.
2. Der Auftragnehmer darf technische und organisatorische Maßnahmen weiterentwickeln und ersetzen, sofern das vertraglich vereinbarte Schutzniveau nicht wesentlich unterschritten wird.
3. Kundendaten werden nicht zum Training eigener oder fremder KI-Modelle verwendet. Soweit KI-Modell-Anbieter eingesetzt werden, erfolgt dies im Rahmen der in Anlage 2 beschriebenen Unterauftragsverarbeitung und Transfermechanismen.

7. Weitere Auftragsverarbeiter

1. Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung, weitere Auftragsverarbeiter einzusetzen. Die bei Vertragsschluss genehmigten weiteren Auftragsverarbeiter sind in Anlage 2 aufgeführt.
2. Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen durch Hinzufügung oder Ersetzung weiterer Auftragsverarbeiter über die Trust-Seite, per E-Mail oder auf anderem geeigneten Weg. Der Auftraggeber kann aus wichtigem Grund innerhalb von 14 Tagen nach Information widersprechen.

3. Erhebt der Auftraggeber einen begründeten Widerspruch und ist dem Auftragnehmer die Leistungserbringung ohne den betroffenen weiteren Auftragsverarbeiter nicht zumutbar, kann der Auftragnehmer den Hauptvertrag und diesen AVV mit einer Frist von 30 Tagen kündigen.
4. Der Auftragnehmer verpflichtet weitere Auftragsverarbeiter vertraglich auf Datenschutzpflichten, die den Pflichten dieses AVV im Wesentlichen entsprechen.

8. Drittlandübermittlungen

1. Eine Verarbeitung findet grundsätzlich innerhalb der EU oder des EWR statt. Einzelne weitere Auftragsverarbeiter können Daten in Drittländern verarbeiten, insbesondere in den USA.
2. Drittlandübermittlungen erfolgen nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere durch Angemessenheitsbeschluss, EU-Standardvertragsklauseln, das EU-US Data Privacy Framework oder einen anderen zulässigen Transfermechanismus.

9. Unterstützungspflichten

1. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren durch geeignete technische und organisatorische Maßnahmen bei der Beantwortung von Anträgen betroffener Personen nach Kapitel III DSGVO.
2. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei dessen Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und Konsultationen mit Aufsichtsbehörden.
3. Soweit der Auftragnehmer durch Unterstützungsleistungen einen Aufwand hat, der über die übliche Leistungserbringung hinausgeht, kann er eine angemessene Vergütung verlangen, sofern gesetzlich nichts anderes zwingend vorgeschrieben ist.

10. Datenschutzverletzungen

1. Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Auftraggeber-Daten bekannt wird.
2. Die Information enthält, soweit verfügbar, die Art der Verletzung, betroffene Daten- und Personenkategorien, wahrscheinliche Folgen sowie ergriffene oder vorgeschlagene Maßnahmen zur Behebung und Abmilderung.
3. Der Auftragnehmer trifft unverzüglich angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen.

11. Löschung und Herausgabe

1. Nach Abschluss der Verarbeitungsleistungen löscht der Auftragnehmer Auftraggeber-Daten oder gibt sie heraus, soweit der Auftraggeber dies verlangt und keine gesetzlichen Aufbewahrungspflichten oder berechtigten Nachweiszwecke entgegenstehen.
2. Produktfunktionen können dem Auftraggeber Exporte bereitstellen, etwa Monats-ZIP, CSV, PDF-Dossiers oder Steuerberater-Links. Gesetzliche Aufbewahrungspflichten des Auftraggebers bleiben unberührt.
3. Dokumentationen, Protokolle und Nachweise, die der Auftragnehmer zur Erfüllung rechtlicher Pflichten, zur Sicherheit, zur Abrechnung oder zur Verteidigung gegen Ansprüche benötigt, dürfen nach Vertragsende aufbewahrt werden, soweit erforderlich.

12. Nachweise und Überprüfungen

1. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO und diesem AVV zur Verfügung.
2. Der Auftraggeber ist berechtigt, die Einhaltung dieses AVV zu überprüfen. Inspektionen vor Ort bedürfen einer angemessenen Vorankündigung, dürfen den Betriebsablauf nicht unverhältnismäßig stören und sind auf die für den Nachweis erforderlichen Informationen beschränkt.
3. Der Auftragnehmer darf vertrauliche Informationen, Informationen zu anderen Kunden, Geschäftsgeheimnisse und sicherheitskritische Details schützen oder nur in angemessen geschwärzter Form bereitstellen.
4. Der Auftragnehmer kann den Nachweis auch durch geeignete Dokumentationen, Zertifizierungen, Sicherheitskonzepte, Prüfberichte oder gleichwertige Nachweise erbringen.

13. Haftung

Für die Haftung der Parteien gelten die Regelungen des Hauptvertrags. Zwingende gesetzliche Ansprüche nach Datenschutzrecht bleiben unberührt.

14. Laufzeit und Schlussbestimmungen

1. Dieser AVV gilt ab Annahme der Nutzungsvereinbarung oder ab sonstigem Abschluss des Hauptvertrags und endet mit dem Hauptvertrag, soweit sich aus diesem AVV oder gesetzlichen Pflichten nichts Abweichendes ergibt.
2. Änderungen dieses AVV bedürfen der Textform, soweit nicht eine strengere Form gesetzlich vorgeschrieben ist.
3. Es gilt deutsches Recht. Ausschließlicher Gerichtsstand für Kaufleute ist, soweit zulässig, Düsseldorf.

Ort, Datum	Ort, Datum
Auftraggeber	digitally induced GmbH

Anlage 1: Verarbeitungstätigkeiten

Gegenstand	Bereitstellung von belege.ai als SaaS-Plattform für Belegsammlung, Belegsuche, Belegzuordnung, Spesen- und Reisekostenprozesse, Eigenbelege, Exporte und buchhaltungsnahe Automatisierung.
Zwecke	Betrieb des Accounts, Authentifizierung, Support, Abruf und Verarbeitung von Banktransaktionen, Suche in E-Mails und Portalen, Verarbeitung von hochgeladenen Belegen, KI-gestützte Extraktion und Klassifikation, Telegram-Kommunikation, Erstellung von Bewirtungsbelegen, Eigenbelegen, Reisekostenabrechnungen, Steuerberater-Exporten und Nachweisen.
Art der Verarbeitung	Erheben, Empfangen, Speichern, Ordnen, Auslesen, Abfragen, Analysieren, Extrahieren, Klassifizieren, Verknüpfen, Anzeigen, Übermitteln, Exportieren, Einschränken, Löschen und Archivieren.
Dauer	Laufzeit des Hauptvertrags zuzüglich gesetzlicher Aufbewahrungs- und Nachweisfristen.

Kategorien personenbezogener Daten:

- Konto- und Organisationsdaten: Name, E-Mail-Adresse, Firma, Rolle, Einstellungen, Login-Daten in gehashter Form, Passkey-Metadaten, Referral-Daten.
- Bank- und Transaktionsdaten: Betrag, Datum, Empfänger, Verwendungszweck, IBAN-/Konto-Metadaten, Buchungsstatus, Zuordnungen und Notizen.
- E-Mail-Daten: Absender, Empfänger, Betreff, Datum, Text, Anhänge, Suchergebnisse und Metadaten aus verbundenen Gmail-, Outlook- oder IMAP-Postfächern.
- Beleg- und Dokumentdaten: Rechnungen, Quittungen, Bewirtungsbelege, Reisekostenunterlagen, PDF-/Bild-Dateien, OCR-Daten und Extraktionsergebnisse.
- Telegram- und Kommunikationsdaten: Telegram-User-ID, Chat-ID, Nachrichten, Fotos, Dateien, Sprachnachrichten, Transkripte, Button-Bestätigungen und Support-Kommunikation.
- Integrationsdaten: OAuth-Tokens, API-Antworten und Fachdaten aus angebundenen Diensten wie Stripe, Shopify, Mollie, Moco, Lexware, Qonto, Tesla, YAXI/Open Banking und Portalen.
- Zugangsdaten und Sitzungen: vom Auftraggeber bereitgestellte Portal-Login-Daten, Session-Kontexte, Zwei-Faktor-Hinweise und verschlüsselt gespeicherte Credentials.
- Stammdaten und Beziehungsdaten: Kunden, Lieferanten, Ansprechpartner, Restaurantteilnehmer, Reisende, Steuerberater und sonstige Kontakte.
- Optionale Signaturdaten: faksimilierte Unterschriften für Bewirtungsbelege oder Reisekostenabrechnungen.
- Protokoll-, Diagnose- und Sicherheitsdaten: Zeitstempel, IP-Adressen, Browser-/Gerätedaten, Fehlerlogs, Agent-Aktivitäten und Audit-/Genehmigungsnachweise.

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Ziel der Verarbeitung. Sie können jedoch in vom Auftraggeber bereitgestellten Dokumenten, Nachrichten oder Belegen enthalten sein; der Auftraggeber bleibt für die Rechtmäßigkeit dieser Bereitstellung verantwortlich.

Kategorien betroffener Personen:

- Nutzer, Mitarbeiter, Geschäftsführer und Administratoren des Auftraggebers.
- Kunden, Lieferanten, Dienstleister, Zahlungs- oder Geschäftspartner des Auftraggebers.
- Teilnehmer von Bewirtungen, Reisende, Mitreisende, Fahrer und Ansprechpartner.
- Absender und Empfänger von E-Mails oder Telegram-Nachrichten, soweit deren Daten zur Belegsuche verarbeitet werden.
- Personen, die in Rechnungen, Quittungen, Verträgen, Buchungen, Portalen oder sonstigen Dokumenten des Auftraggebers genannt sind.

Anlage 2: Genehmigte weitere Auftragsverarbeiter

Anbieter	Zweck	Datenarten	Ort / Transfer
Netcup	Hosting und Infrastruktur	Auftraggeber-Daten, Anwendungsdaten, Datenbankdaten	Deutschland
Amazon Web Services (SES)	E-Mail-Versand und Zustellung	E-Mail-Adressen, technische Versanddaten, Inhalte aus System-E-Mails	EU, insbesondere Irland
Stripe	Zahlungsabwicklung, Rechnungs- und Zahlungsinformationen	Abrechnungsdaten, Zahlungsstatus, Rechnungsdaten	EU/USA, geeignete Garantien wie SCCs oder DPF
OpenAI	KI-Modelle für Belegextraktion, Vision, Transkription und Agentenantworten	Relevante Eingaben und Dokumentauszüge, keine Nutzung zum Training	EU/USA, geeignete Garantien wie SCCs oder DPF
Google (Gemini)	KI-Modelle für Vision und Extraktion; Google-APIs bei vom Nutzer verbundenen Diensten	Relevante Eingaben, Dokumentauszüge und API-Daten	EU/USA, geeignete Garantien wie SCCs oder DPF
Browserbase	Browser-Automatisierung zum Abruf fehlender Belege aus Portalen	Portal-URLs, Sitzungskontexte, Browserdaten, Belegdokumente	USA, geeignete Garantien wie SCCs oder DPF
YAXI	Open-Banking-Anbindung und Abruf von Banktransaktionen nach Einwilligung	Bank- und Transaktionsdaten, Bankverbindungsmetadaten	EU
PostHog	Produktanalyse, Fehleranalyse und Nutzungsstatistiken	Nutzungs- und Diagnosedaten, pseudonymisierte Nutzerkennungen soweit möglich	EU/USA, geeignete Garantien wie SCCs oder DPF
Datakant	Webanalyse und Consent-Management	Webanalyse- und Consent-Daten	Deutschland / EU

Die jeweils aktuelle öffentliche Anbieterübersicht ist auf der Trust-Seite von belege.ai abrufbar. Verbundene Dienste des Auftraggebers wie Banken, Telegram, Gmail, IMAP-Provider, Tesla, Shopify, Lexware, Moco, Mollie, Stripe oder Qonto werden nur nach Einrichtung oder Einwilligung des Auftraggebers genutzt.

Anlage 3: Technische und organisatorische Maßnahmen

Die nachfolgenden Maßnahmen beschreiben den Stand zum Stand dieses AVV. Sie werden entsprechend Risiko, Stand der Technik und Produktentwicklung fortlaufend angepasst.

1. Vertraulichkeit

Zugangskontrolle	Betrieb auf kontrollierter Serverinfrastruktur; Administrationszugriff nur für berechtigte Personen; Zugriff auf Produktionssysteme über geschützte Admin-Zugänge.
Zugriffskontrolle	Rollen- und Rechtekonzept, individuelle Nutzerkonten, Passwörter gehasht, optionale Passkeys, Adminzugriff auf das erforderliche Minimum beschränkt.
Mandantentrennung	Mandantenspezifische Datenbankzugriffe, Row-Level-Security und anwendungsseitige Berechtigungsprüfungen.
Verschlüsselung	TLS für Transportwege; verschlüsselte Speicherung sensibler Tokens und Zugangsdaten; Trennung von Secrets und Quellcode.

2. Integrität

Weitergabekontrolle	Übermittlungen an Unterauftragsverarbeiter nur für definierte Zwecke; bevorzugt verschlüsselte Schnittstellen; Zugriff auf verbundene Dienste nur nach Einrichtung oder Einwilligung.
Eingabekontrolle	Protokollierung relevanter System- und Agentenaktivitäten; Nachvollziehbarkeit von Telegram-Genehmigungen, Belegzuordnungen und Exporten.
Änderungskontrolle	Versionierte Quellcodeverwaltung, Reviews nach Risiko, migrationsbasierte Schemaänderungen und automatisierbare Deployments.

3. Verfügbarkeit und Belastbarkeit

Backups	Regelmäßige Sicherungen von Datenbank und relevanten Systemdaten; Wiederherstellungsprozesse für technische Zwischenfälle.
Monitoring	Systemd-Services, Logs, Fehlerbenachrichtigungen, Job- und Deploy-Überwachung.
Wiederherstellung	Automatisierte Deployments, reproduzierbare Infrastruktur, dokumentierte Betriebsabläufe und Möglichkeit zur Wiederherstellung aus Backups.

4. Regelmäßige Überprüfung

Sicherheitsprüfung	Laufende Pflege von Abhängigkeiten, Fehleranalyse, Zugriffskontrollen und technische Plausibilitätsprüfungen.
Datenschutzfreundliche Voreinstellungen	Datenabruf nur nach Einrichtung oder Einwilligung, kein KI-Training mit Kundendaten, gezielte E-Mail-Suche statt pauschalem Dauer-Scan.
Unterauftragskontrolle	Auswahl geeigneter Dienstleister, vertragliche Datenschutzpflichten, Transfermechanismen und öffentliche Transparenz über wesentliche Anbieter.