Art. 28 DSGVO konform · Version v2.3_2026-10

Auftragsverarbeitungsvertrag (AVV)

Vereinbarung über die Datenverarbeitung im Auftrag gemäß Art. 28 DSGVO für die B2B-Plattform Argyron Automation · Stand: Oktober 2026

1. Vertragsparteien & Geltungsbereich

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten bei der Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Kunden (nachfolgend **„Auftraggeber“**):

Auftragnehmer:
Simon Gollas, handelnd unter **Argyron Automation**
Raiffeisenstraße 25, 63939 Wörth am Main, Deutschland
E-Mail: support@argyron-automation.de

Der Auftraggeber schließt diesen Vertrag im Rahmen der Inanspruchnahme der B2B-SaaS-Dienstleistungen von Argyron Automation ab. Die Vereinbarung erfasst alle Verarbeitungstätigkeiten, bei denen Systeme des Auftragnehmers mit personenbezogenen Daten des Auftraggebers in Berührung kommen, die in hochgeladenen Belegdokumenten enthalten sind.

2. Gegenstand, Art und Zweck der Verarbeitung

(1) **Verarbeitungszweck:** Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zur Erbringung der vertraglich vereinbarten SaaS-Dienstleistung. Dies umfasst die optische Zeichenerkennung (Mistral OCR), die semantische Datenextraktion aus digitalen PDF-Belegen (Rechnungen, Lieferscheine), die Ausführung des algorithmischen 2-Wege-Positionsabgleichs sowie die Bereitstellung der Ergebnisse über das Web-Portal und via Tabellenexport (.xlsx).

(2) **Verarbeitungsarchitektur & Speicherungszyklus:**

- **Flüchtige Inferenz im Arbeitsspeicher (RAM):** Die optische Zeichenerkennung und die semantische Modellinferenz erfolgen flüchtig im Arbeitsspeicher der Serverumgebung. PDF-Rohdateien und Bildextrakte werden in diesem Verarbeitungsschritt nicht persistent auf Festplatten gespeichert.

- **Asynchrones Polling-Caching (PostgreSQL):** Zur Ermöglichung des asynchronen Abrufs der Analyseergebnisse über die Status-Polling-Schnittstellen (`/job-status` bzw. `/demo-status`) wird das aggregierte JSON-Ergebnisdatenset (enthält Belegmetadaten, Posten, Beträge und den berechneten Abgleichsstatus) temporär in der relationalen Datenbank (`document_jobs`) auf Servern des Auftragnehmers zwischengespeichert.
- **Verbindliche 24-Stunden-Löschroutine:** Sämtliche in der PostgreSQL-Datenbank hinterlegten Ergebnisdatensätze (`document_jobs.result`) sowie temporäre Ausführungsprotokolle werden automatisiert **nach Ablauf von maximal 24 Stunden vollständig und unwiderruflich von den Servern gelöscht**.
- **Ausschluss von Modelltraining (0 % Training):** Der Auftragnehmer gewährleistet, dass die übermittelten Belege und Daten zu keinem Zeitpunkt für das Training, die Optimierung oder die Validierung von Machine-Learning-Modellen des Auftragnehmers oder Dritter verwendet werden.
- **Keine Archivierungsfunktion:** Der Auftragnehmer stellt kein GoBD-konformes Revisionsarchiv dar. Dem Auftraggeber obliegt die eigenverantwortliche Archivierung der Originalbelege sowie die Sicherung der clientseitig erzeugten Tabellenexporte (.xlsx).

3. Kategorien betroffener Personen und Datenarten

- **Kategorien betroffener Personen:** Kunden, Lieferanten, Frachtführer, Spediteure, kaufmännische Ansprechpartner sowie Beschäftigte des Auftraggebers oder Dritter, deren Daten auf den verarbeiteten Belegen aufgeführt sind.
- **Kategorien personenbezogener Daten:** Namen, geschäftliche Anschriften, E-Mail-Adressen, Telefonnummern, Steuernummern, USt-IdNrn., Bankverbindungen (IBAN/BIC), Belegnummern, Bestelldaten, Lieferdaten, Positionsbeschreibungen, Mengenangaben, Einzel- und Gesamtpreise sowie handschriftliche Prüfvermerke.

4. Pflichten des Auftragnehmers (Weisungsbindung & TOMs)

- **Strikte Weisungsgebundenheit (Art. 28 Abs. 3 lit. a DSGVO):** Der Auftragnehmer verarbeitet Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Die über die Webschnittstelle oder API initiierten Verarbeitungsaufträge gelten als abschließende dokumentierte Weisungen.
- **Hinweispflicht bei rechtswidrigen Weisungen:** Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er den Auftraggeber hierüber unverzüglich. Er ist berechtigt, die Durchführung der Weisung auszusetzen, bis diese bestätigt oder geändert wird.

- **Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO):** Alle Personen, die zur Verarbeitung personenbezogener Daten befugt sind, sind zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht.
- **Technische und organisatorische Maßnahmen (Art. 28 Abs. 3 lit. c, Art. 32 DSGVO):**
  - Verschlüsselung nach aktuellem Stand der Technik: Vollständige Transportverschlüsselung via TLS 1.3 / HTTPS;
  - Serverstandorte innerhalb der Europäischen Union auf ISO/IEC-27001-zertifizierter Infrastruktur;
  - Kryptografisch generierte API-Tokens (Format `arg_...`) zur logischen Mandantentrennung auf Applikationsebene;
  - Automatisierte Löschroutinen persistierter Ergebnisdaten nach maximal 24 Stunden.

5. Genehmigte Unterauftragsverarbeiter & Änderungsverfahren

(1) **Genehmigte Sub-Prozessoren:** Der Auftraggeber erteilt seine allgemeine Genehmigung zur Einbindung folgender Unterauftragsverarbeiter:

- **Hetzner Online GmbH (Deutschland):** Hosting der Serverinfrastruktur und der relationalen Datenbank im ISO-27001-zertifizierten Rechenzentrum in Helsinki (Finnland / EU).
- **Mistral AI SAS (Frankreich):** Bereitstellung von Cloud-Inferenzschnittstellen für optische Zeichenerkennung (Mistral OCR) und semantischen Postenabgleich (Mistral Small) im Rechenzentrum Frankfurt am Main (Deutschland / EU) unter vertraglichem Ausschluss von Datenspeicherung und Modelltraining.
- **Cloudflare Inc. (USA):** DDoS-Schutz, WAF und Reverse-Proxy auf Grundlage der Zertifizierung unter dem EU-U.S. Data Privacy Framework (DPF).
- **Stripe Payments Europe Ltd. (Irland / EU):** Zahlungsabwicklung und Bereitstellung des Abrechnungsportals.
- **Sendinblue GmbH / Brevo (Deutschland / EU):** Versand transaktionaler E-Mails zur Übermittlung von Authentifizierungs-Tokens.

(2) **Verfahren bei Änderungen von Unterauftragsverarbeitern (Art. 28 Abs. 2 Satz 2 DSGVO):** Beabsichtigt der Auftragnehmer, weitere Unterauftragsverarbeiter hinzuzuziehen oder bestehende zu ersetzen, informiert er den Auftraggeber mindestens **14 Tage vor dem beabsichtigten Inkrafttreten in Textform** (z. B. per E-Mail). Der Auftraggeber ist berechtigt, der beabsichtigten Änderung innerhalb von 14 Tagen nach Zugang der Mitteilung aus wichtigem datenschutzrechtlichem Grund in Textform zu widersprechen.

(3) **Rechtsfolgen des Widerspruchs:** Erhebt der Auftraggeber innerhalb der Frist Widerspruch, bemühen sich die Parteien um eine einvernehmliche Lösung. Kann keine Einigung erzielt werden und ist dem Auftragnehmer das Festhalten am bisherigen Zustand unzumutbar, steht beiden Parteien ein Sonderkündigungsrecht des Hauptvertrages mit einer Frist von 14 Tagen zum Monatsende zu. Erfolgt innerhalb der Frist kein Widerspruch, gilt die Änderung als genehmigt.

6. Kontroll- und Auditrechte (Art. 28 Abs. 3 lit. h DSGVO)

(1) Der Auftragnehmer stellt dem Auftraggeber auf schriftliche Anforderung alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO zur Verfügung.

(2) Der Auftragnehmer ermöglicht dem Auftraggeber oder einem von diesem beauftragten, zur Verschwiegenheit verpflichteten Prüfer (der kein Mitbewerber des Auftragnehmers sein darf) die Durchführung von Inspektionen und Audits. Vor-Ort-Inspektionen sind mit einer Frist von mindestens zwei Wochen anzukündigen, finden während der regulären Geschäftszeiten statt und dürfen den Geschäftsbetrieb des Auftragnehmers nicht unverhältnismäßig beeinträchtigen.

(3) Der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen kann vorrangig durch Vorlage aktueller Testate, Zertifizierungen (z. B. ISO/IEC 27001) oder anerkannter Prüfberichte erbracht werden.

7. Unterstützungspflichten & Incident-Meldung

(1) **Betroffenenrechte:** Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen Maßnahmen bei der Beantwortung von Anfragen betroffener Personen nach Kapitel III der DSGVO. Richtet sich eine betroffene Person direkt an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter.

(2) **Meldung von Datenschutzverletzungen (Art. 33 Abs. 2 DSGVO):** Wird dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt, informiert er den Auftraggeber hierüber **unverzüglich, spätestens innerhalb von 36 Stunden** nach Kenntniserlangung, in Textform unter Mitteilung der nach Art. 33 Abs. 3 DSGVO relevanten Umstände.

8. Beendigung und Löschung

(1) Nach Beendigung der Leistungsvereinbarung löscht der Auftragnehmer alle in seinen Besitz gelangten auftragsbezogenen Verarbeitungsdaten, sofern nicht nach Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine gesetzliche Aufbewahrungspflicht besteht.

(2) Da Beleginhalte im operativen Betrieb automatisiert nach Ablauf von 24 Stunden gelöscht werden, verbleiben bei Beendigung des Hauptvertrages keine auftragsbezogenen Belegdaten auf den operativen Servern. Administrative Metadaten werden nach Ablauf der gesetzlichen handels- und steuerrechtlichen Aufbewahrungsfristen (§ 147 AO, § 257 HGB) automatisiert gesperrt und gelöscht.

9. Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform.

(2) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist der Geschäftssitz des Auftragnehmers.