Art. 28 DSGVO konform · Version v2.2_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
E-Mail: support@argyron-automation.de

Der Auftraggeber schließt diesen Vertrag im Rahmen der Inanspruchnahme der kostenpflichtigen oder im Rahmen von Testkontingenten autorisierten B2B-Dienstleistungen von Argyron Automation ab. Die Vereinbarung erfasst alle Verarbeitungen, bei denen Systeme des Auftragnehmers mit personenbezogenen Daten des Auftraggebers in Berührung kommen.

2. Gegenstand, Art und Zweck der Verarbeitung

(1) **Verarbeitungszweck:** Der Auftragnehmer verarbeitet personenbezogene Daten aus vom Auftraggeber übermittelten Dokumenten ausschließlich zum Zweck der automatisierten optischen Zeichenerkennung (OCR), der semantischen Datenextraktion aus Belegen (PDF-Rechnungen, Lieferscheine), der Ausführung des algorithmischen 2-Wege-Positionsabgleichs sowie der Bereitstellung der Ergebnisse im Web-Interface und via Tabellenexport (.xlsx).

(2) **Zustandslosigkeit & Ephemere RAM-Inferenz:**

- Die Verarbeitung aller übermittelten Belegdokumente erfolgt zustandslos und flüchtig. Sämtliche Belegdateien und die daraus extrahierten Datensätze werden ausschließlich während der aktiven Workflow-Laufzeit im flüchtigen Arbeitsspeicher (RAM) der Verarbeitungsumgebung gehalten.
- In der relationalen Datenbank des Auftragnehmers (PostgreSQL) werden zu keinem Zeitpunkt Beleginhalte, Dokumententexte, Rechnungsposten oder Adressdaten persistent gespeichert. Die Datenbank erfasst ausschließlich Abrechnungs- und

Authentifizierungsmetadaten (Kundenkennung, Zähler über verbrauchte Prüfvorgänge zur Autorisierungsprüfung, Kontostatus).

- Sämtliche flüchtigen Prozessdaten, temporären Dateipuffer und Ausführungsprotokolle werden nach Abschluss der Datenübermittlung, spätestens jedoch **nach Ablauf von maximal 24 Stunden, automatisiert und unwiderruflich von den operativen Servern gelöscht**.
- Der Auftragnehmer stellt ausdrücklich kein GoBD-konformes Archivierungssystem dar. Dem Auftraggeber obliegt die eigenverantwortliche Archivierung der Originalbelege sowie die Speicherung der browserseitig generierten Exportdateien (.xlsx).

3. Kategorien betroffener Personen und Datenarten

- **Kategorien betroffener Personen:** Kunden, Lieferanten, Spediteure, 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, Positions-, Mengenangaben und Einzelpreise sowie handschriftliche Prüfvermerke auf Lieferscheinen.

4. Pflichten des Auftragnehmers (TOMs & Weisungsbindung)

- **Strikte Weisungsgebundenheit:** Der Auftragnehmer verarbeitet Daten ausschließlich zur Erfüllung des Hauptvertrages und auf dokumentierte Weisung des Auftraggebers. Eine Verarbeitung zu eigenen Zwecken ist ausgeschlossen.
- **Garantierter Ausschluss von Modelltraining (0 % Training):** Der Auftragnehmer gewährleistet, dass übermittelte Belege und Daten zu keinem Zeitpunkt zur Modelloptimierung, zum Training oder zur Feinabstimmung von Machine-Learning-Modellen Dritter oder eigener Systeme verwendet werden.
- **Vertraulichkeit & Datengeheimnis:** Alle zur Verarbeitung berechtigten Personen sind zur Vertraulichkeit und zur Einhaltung des Datengeheimnisses verpflichtet.
- **Technische und organisatorische Maßnahmen (TOMs):**
    - Ende-zu-Ende-Transportverschlüsselung via TLS 1.3 / HTTPS für alle Datenübertragungswege.
    - Isolierte Docker-Containerinfrastruktur auf ISO/IEC-27001-zertifizierten Servern innerhalb der Europäischen Union (Helsinki, Finnland).
    - Kryptografisch randomisierte API-Authentifizierung (Bearer-Token-Format `arg_...`) zur strikten Mandantentrennung auf Applikationsebene.

- Automatisierte Bereinigung flüchtiger Container-Zustände und vollständiger Verzicht auf Festplattenpersistenz für extrahierte Belegdaten.

5. Genehmigte Sub-Auftragsverarbeiter

Der Auftraggeber erteilt seine ausdrückliche Genehmigung zur Einbindung folgender Sub-Auftragsverarbeiter, die gemäß Art. 28 Abs. 2 und 4 DSGVO vertraglich verpflichtet wurden:

- **Hetzner Online GmbH (Deutschland):** Hosting der Serverinfrastruktur und Datenbanken im ISO-27001-zertifizierten Rechenzentrum in Helsinki (Finnland / EU).
- **Mistral AI SAS (Frankreich):** Bereitstellung von Cloud-Inferenzschnittstellen für:
  - Optische Zeichenerkennung (OCR) von Bilddateien und Scans über die Mistral OCR API (Serverstandort Frankfurt am Main / EU);
  - Semantische Extraktion, Postenstrukturierung und Abgleichsprüfung über Mistral Small Cloud-Modelle (Serverstandort Frankfurt am Main / EU).
  - Vertraglicher Ausschluss von Datenspeicherung und Modelltraining durch den Unterauftragnehmer.
- **Cloudflare Inc. (USA / EU-DPF):** Edge-Netzwerk, WAF, DDoS-Schutz und Reverse-Proxy unter dem EU-U.S. Data Privacy Framework.
- **Stripe Payments Europe Ltd. (Irland / EU):** Abwicklung von B2B-Zahlungen und Verwaltung des Kundenabrechnungsportals.
- **Sendinblue GmbH / Brevo (Deutschland / EU):** Versand von Transaktions-E-Mails zur Übermittlung von Authentifizierungsschlüsseln und Systembenachrichtigungen.

6. Rechte der Betroffenen und Vertragsbeendigung

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten im Rahmen des technisch Zumutbaren.

(2) Da auf den Systemen des Auftragnehmers keine Beleg- und Verarbeitungsdaten dauerhaft persistiert werden, verbleiben bei Beendigung des Hauptvertrages keine auftragsbezogenen Belegdaten auf den operativen Servern. Nach Vertragsbeendigung werden verbleibende Kundenmetadaten im Rahmen der gesetzlichen steuer- und handelsrechtlichen Aufbewahrungspflichten gesperrt und nach Fristablauf gelöscht.