Data Processing Agreement

Auftragsverarbeitungsvertrag (AVV)

pursuant to Art. 28 GDPR

Template Version 1.0 — June 2026 | StartFill / Blumental Bayern GmbH

Parties

1.1 The Controller (Merchant Client)

The controller within the meaning of Art. 4 No. 7 GDPR is the merchant client who engages StartFill for fulfilment services:

Company name: ____

Legal form: ____

Registered address: ____

VAT-ID: ____

Authorised representative: ____

Data protection contact (name / e-mail): ____

1.2 The Processor (StartFill)

The processor within the meaning of Art. 4 No. 8 GDPR is:

Company: Blumental Bayern GmbH (trading as StartFill)

Address: Melanchthonplatz 4–6, 90443 Nuremberg, Germany

Managing Director: Dr. Jalal Solati

Data protection contact: info@startfill.com

Commercial Register: HRB 36602, Registration Court Nuremberg

The controller and the processor are hereinafter referred to individually as a "Party" and collectively as the "Parties".

---

§ 1 Subject Matter, Duration, and Purpose

1.1 Subject Matter

This Agreement governs the processing of personal data by StartFill on behalf of the Controller in connection with the provision of third-party logistics (3PL) services including warehousing, order picking and packing, shipping, and returns management (the "Fulfilment Services"), as agreed in the General Terms and Conditions (Allgemeine Geschäftsbedingungen, "AGB") of StartFill between the Parties.

1.2 Duration

This Agreement enters into force upon signature by both Parties and remains in effect for as long as StartFill processes personal data on behalf of the Controller. It terminates automatically upon expiry or termination of the General Terms and Conditions (Allgemeine Geschäftsbedingungen, "AGB") of StartFill, subject to the data deletion obligations in § 9.

1.3 Purposes of Processing

Personal data is processed exclusively for the following purposes:

- Receiving, processing, and dispatching orders submitted by the Controller or retrieved via API from the Controller's selling platforms
- Generating shipping labels and transmitting delivery information to carriers
- Updating order status, tracking numbers, and stock levels on the Controller's selling platforms via API
- Processing returns and recording inspection results
- Generating fulfilment activity reports for billing and client dashboards

Processing for any other purpose requires a separate prior written instruction from the Controller.

---

§ 2 Nature of Data and Categories of Data Subjects

2.1 Categories of Personal Data

The following categories of personal data are processed under this Agreement:

Category	Examples	Sensitivity
Order & delivery data	Recipient name, delivery address (street, city, postcode, country), order reference	Standard
Contact for notifications	E-mail address and/or phone number (if provided by Controller for carrier notification or returns)	Standard
Return data	Return reason, inspection notes linked to order reference	Standard
Platform API data	Orders, line items, product data, fulfilment status retrieved via Controller's API credentials	Standard

No special category data (Art. 9 GDPR) is processed under this Agreement unless the Controller explicitly instructs StartFill to do so in writing.

2.2 Categories of Data Subjects

- End customers of the Controller who have placed orders via the Controller's selling channels
- Persons submitting returns

---

§ 3 Instructions

3.1 StartFill processes personal data solely on documented instructions from the Controller. This Agreement, together with the General Terms and Conditions (Allgemeine Geschäftsbedingungen, "AGB") of StartFill and any written addenda, constitutes the Controller's documented instructions.

3.2 The Controller may issue further instructions at any time by written notice (including e-mail to info@startfill.com). StartFill will confirm receipt and, where applicable, the feasibility of such instructions within five business days.

3.3 If StartFill considers that an instruction infringes the GDPR or other applicable data protection law, it shall immediately inform the Controller in writing and may suspend compliance with that instruction until it receives written confirmation from the Controller.

3.4 StartFill shall not use personal data processed under this Agreement for its own purposes, for profiling, for marketing, or for any purpose other than those specified in § 1.3.

---

§ 4 Confidentiality

4.1 StartFill ensures that all persons authorised to process personal data under this Agreement are subject to a binding obligation of confidentiality, either by contract or by statute.

4.2 Access to personal data is strictly limited to personnel who require such access to perform the Fulfilment Services. StartFill maintains a current register of authorised personnel.

4.3 The confidentiality obligations of this clause survive the termination of this Agreement.

---

§ 5 Technical and Organisational Measures (TOMs)

5.1 StartFill implements and maintains appropriate technical and organisational measures in accordance with Art. 32 GDPR to ensure a level of security appropriate to the risk. The current TOMs are set out in Annex A to this Agreement.

5.2 StartFill may update or improve the TOMs at any time, provided that the level of protection is not reduced below the standard set out in Annex A without prior written agreement from the Controller.

5.3 The Controller acknowledges that the TOMs described in Annex A are appropriate having regard to the nature of the personal data processed and the risks involved.

---

§ 6 Sub-Processors

6.1 The Controller hereby grants general authorisation to StartFill to engage the sub-processors listed in Annex B. StartFill will inform the Controller of any intended addition or replacement at least 30 days in advance by e-mail.

6.2 The Controller may object to a new sub-processor on reasonable data protection grounds within 14 days of notification. If no solution can be agreed, either Party may terminate the affected part of the Fulfilment Services with 30 days' notice.

6.3 StartFill shall impose on each sub-processor data protection obligations equivalent to those in this Agreement and remains liable to the Controller for sub-processor compliance.

6.4 Sub-processors outside the EU/EEA are engaged only on the basis of EU Standard Contractual Clauses (SCCs) or another recognised transfer mechanism under Chapter V GDPR, as noted in Annex B.

---

§ 7 Assistance Obligations

7.1 Data Subject Rights

Taking into account the nature of the processing, StartFill shall assist the Controller in fulfilling its obligations to respond to data subject requests under Chapter III GDPR (access, rectification, erasure, restriction, portability, objection). Where a data subject contacts StartFill directly, StartFill shall forward the request to the Controller within three business days.

7.2 Breach Notification

StartFill shall notify the Controller without undue delay — and in any event within 24 hours — after becoming aware of a personal data breach affecting data processed under this Agreement. The notification shall include:

- Nature of the breach and categories / approximate number of data subjects and records affected
- Name and contact details of the data protection contact at StartFill
- Likely consequences of the breach
- Measures taken or proposed to address the breach and mitigate its effects

StartFill shall cooperate with the Controller in any investigation and in making notifications to supervisory authorities and individuals under Arts. 33–34 GDPR.

7.3 Data Protection Impact Assessments

StartFill shall provide reasonable assistance to the Controller in conducting DPIAs under Art. 35 GDPR and prior consultations with supervisory authorities under Art. 36 GDPR, to the extent such assessments require information only available to StartFill.

---

§ 8 Audits and Inspections

8.1 StartFill shall make available to the Controller all information reasonably necessary to demonstrate compliance with Art. 28 GDPR.

8.2 The Controller or a mandated auditor may conduct audits of StartFill's processing activities, subject to: (a) at least 14 days' prior written notice; (b) limitation to business hours and one audit per calendar year absent a data breach; (c) a confidentiality undertaking by the Controller and its auditors; and (d) the Controller bearing all costs.

8.3 As an alternative to an on-site audit, StartFill may produce up-to-date third-party certifications or audit reports that provide equivalent assurance. An on-site audit may only be requested if such reports do not reasonably address the concern.

---

§ 9 Return and Deletion of Data

9.1 Upon termination or expiry of the General Terms and Conditions (Allgemeine Geschäftsbedingungen, "AGB") of StartFill, StartFill shall, at the Controller's written election: (a) return all personal data processed under this Agreement in a structured, commonly used machine-readable format; or (b) securely delete all such personal data and provide written confirmation of deletion.

9.2 The Controller must specify its election within 30 days of the effective date of termination. In the absence of an election, StartFill will securely delete all personal data within 60 days.

9.3 Notwithstanding the above, StartFill may retain personal data to the extent required by applicable law (in particular § 257 HGB and § 147 AO — up to 10 years). Data retained under this clause is kept securely with restricted access and used solely to fulfil the applicable retention obligation.

9.4 All API credentials (access tokens, keys, secrets) provided by the Controller are deleted immediately upon contract termination. The Controller is separately responsible for revoking those tokens at the source (Shopify, Amazon Seller Central, eBay, etc.).

---

§ 10 Liability

10.1 Each Party is liable for damages caused to data subjects by its own GDPR infringement in accordance with Art. 82 GDPR.

10.2 Where both Parties are responsible for the same damage, they shall be jointly and severally liable to the data subject, subject to the right of recourse between them in proportion to their respective responsibility.

10.3 StartFill shall be exempt from liability to the extent it demonstrates it is not responsible for the damaging event, including where it processed data in compliance with the Controller's documented instructions.

10.4 Any limitation of liability agreed in the General Terms and Conditions (Allgemeine Geschäftsbedingungen, "AGB") of StartFill applies equally to claims under this Agreement, unless excluded by Art. 82 GDPR or other mandatory law.

---

§ 11 Governing Law and Jurisdiction

This Agreement is governed by the law of the Federal Republic of Germany, excluding the UN Convention on Contracts for the International Sale of Goods (CISG). The exclusive place of jurisdiction is Nuremberg, Germany, provided the Controller is a commercial entity (Kaufmann), a legal person under public law, or a special fund under public law.

---

§ 12 General Provisions

12.1 In the event of a conflict between this Agreement and the General Terms and Conditions (Allgemeine Geschäftsbedingungen, "AGB") of StartFill on data protection matters, this Agreement prevails.

12.2 Amendments require written form signed by both Parties. E-mail satisfies the written requirement.

12.3 Should any provision be or become invalid, the remaining provisions shall not be affected. The invalid provision shall be replaced by one that most closely reflects its economic purpose.

12.4 In the event of inconsistency between translations, the English text prevails.

Signatures

This Agreement is entered into by the authorised representatives of the Parties as of the date last signed below.

For the Controller:		For StartFill (Processor):
Signature **Name:** ____________________ **Title:** ____________________ **Date:** ____________________		Signature **Name:** Dr. Jalal Solati **Title:** Managing Director, Blumental Bayern GmbH **Date:** ____________________

Annex A — Technical and Organisational Measures (TOMs)

Pursuant to Art. 32 GDPR | StartFill / Blumental Bayern GmbH | Version June 2026

A.1 Physical Access Control

- Warehouse access controlled by key/fob entry; visitor log maintained
- WMS server PC accessible only to authorised operators
- UPS on server PC and router; LTE broadband fallback for internet outages

A.2 System Access Control

- All accounts protected by strong passwords (16+ chars) in Bitwarden Teams encrypted vault
- Hardware security keys (YubiKey) required for Bitwarden and all critical platform logins
- Multi-factor authentication (MFA) enforced on all cloud services
- Automatic screen lock after 5 minutes of inactivity on WMS PC
- Windows Defender Antivirus and regular malware scans

A.3 Data Access Control

- Role-based access in JTL-Wawi: operational staff have pick/pack/putaway permissions only; client data accessible only to authorised managers
- Merchant data segregated by 3-letter client code; operators cannot access another merchant's records
- Monday.com dashboards accessible to each merchant as read-only guest only for their own data
- API credentials stored exclusively in Bitwarden; never stored in plain text
- TLS 1.2+ encryption for all data in transit

A.4 Transmission Control

- All API connections to selling platforms use TLS-encrypted HTTPS
- Sendcloud carrier API connections are TLS encrypted
- Google Workspace enforces TLS transport encryption for all e-mail

A.5 Input and Audit Logging

- All pick, pack, and putaway operations in JTL-Wawi are attributed to operator login ID with timestamp
- Order status changes and label generations are logged in JTL and Sendcloud
- N8N automation workflows log all data transfer events with timestamps

A.6 Availability and Resilience

- Nightly automated SQL backup of JTL-Wawi database to encrypted local SSD and encrypted cloud (two locations)
- Recovery time objective (RTO): 4 hours using cold-standby PC with pre-installed JTL
- Recovery point objective (RPO): 24 hours (last nightly backup)

A.7 Client Data Separation

- Each merchant's goods, orders, stock records, and reports are segregated by unique 3-letter client code
- Billing data per client is generated and stored separately

– Returns processed in isolated per-client queues

A.8 Incident Response

– Personal data breach identification and escalation procedure documented in StartFill SOPs
– Controller notified within 24 hours of breach detection (§ 7.2 of this Agreement)
– Incident register maintained and reviewed monthly

Annex B — Authorised Sub-Processors

Pursuant to § 6 of this Agreement | Version June 2026

The following sub-processors are authorised to process personal data on StartFill's behalf. The Controller is notified at least 30 days before any addition or replacement.

Sub-Processor	Country	Purpose / Data Processed	Transfer Basis	Privacy Policy
JTL-Software GmbH	Germany (EU)	WMS; order, stock, operator data	EU — no transfer	jtl-software.de
Sendcloud B.V.	Netherlands (EU)	Carrier API, label generation; end-customer addresses	EU — no transfer	sendcloud.com/privacy
DHL Paket GmbH	Germany (EU)	Parcel delivery; name & address	EU — no transfer	dhl.de/datenschutz
DPD Deutschland GmbH	Germany (EU)	Parcel delivery; name & address	EU — no transfer	dpd.com/de/datenschutz
GLS Germany GmbH	Germany (EU)	Parcel delivery; name & address	EU — no transfer	gls-group.eu/datenschutz
lexoffice (Haufe-Lexware)	Germany (EU)	Invoicing & accounting; billing data	EU — no transfer	lexoffice.de/datenschutz
monday.com Ltd.	Israel	CRM, ops boards, client dashboards; contact & order summaries	EU SCCs + IL adequacy	monday.com/privacy
n8n GmbH	Germany (EU)	Workflow automation; all data in transit between systems	EU — no transfer	n8n.io/privacy
Bitwarden Inc.	USA	Encrypted credential vault; API token metadata	EU SCCs	bitwarden.com/privacy
Google LLC (Workspace)	USA	Email + Drive; client correspondence & documents	EU SCCs + DPF	policies.google.com/privacy
Meta (WhatsApp Business)	Ireland (EU)	Client communication; phone numbers & message metadata	EU — no transfer	whatsapp.com/legal/privacy-policy
Automattic (WordPress)	USA	Website & lead forms; prospect enquiry data, logs	EU SCCs + DPF	automattic.com/privacy

DPF = EU–US Data Privacy Framework adequacy decision (July 2023). SCCs = EU Standard Contractual Clauses (Commission Decision 2021/914). Carriers listed above act as independent data controllers for the delivery process.

Annex C — Processing Details (complete per merchant)

This annex customises the Agreement for the specific merchant client. Complete all fields before signing.

C.1 Selling Platforms — API Connections

Tick all platforms from which StartFill will retrieve order data via API:

	Platform	Data Retrieved	Credential Type
☐	WooCommerce	Orders, line items, shipping address, tracking updates	Consumer key / secret
☐	Shopify	Orders, customer address, products, tracking	Private app API key + secret
☐	Amazon Seller Central	Orders, shipping addresses, return requests (SP-API)	SP-API access token + refresh token
☐	eBay	Orders, delivery addresses	OAuth token
☐	Kaufland	Orders, delivery addresses	API key
☐	Otto	Orders, delivery addresses	API key
☐	Other: ________________		___________________

C.2 Data Volume and Product Type

Approximate monthly order volume: ____

Estimated unique end-customer records per month:

____

Age-restricted goods? (Yes / No): ____

Cosmetics, supplements, or food products? (Yes / No):

____

Temperature-controlled storage required? (Yes / No):

____

C.3 Special Processing Instructions

Any instructions that deviate from the defaults in this Agreement (e.g. carrier restrictions, label content, data deletion timelines):
