Data Processing Agreement (Auftragsverarbeitungsvertrag / AVV)

pursuant to Art. 28(3) GDPR

in connection with the use of the Shopify App

“Revoq – EU Withdrawal-Button”

between

Jonas Busch (Sole Proprietor / Einzelunternehmer)
Hofstraße 2-4, 51061 Cologne, Germany
VAT ID: DE449524313
Email: hello@buschbytes.com
– hereinafter the “Processor” –

and

The Merchant,
who installs and uses the App via the Shopify App Store
– hereinafter the “Controller” –

– collectively the “Parties”, individually a “Party” –

Version: November 2026 (v2.4)

Note: In the event of any discrepancy between the German and English versions, the German version shall prevail.

Preamble

The Processor operates the Shopify App “Revoq – EU Withdrawal-Button” (hereinafter the “App”). The App supports the Controller in the technical implementation of the electronic withdrawal function pursuant to § 356a of the German Civil Code (BGB) (effective 19 June 2026) and EU Directive (EU) 2023/2673.

In the course of using the App, the Processor processes personal data of the Controller’s end customers (consumers who submit a withdrawal via the App) on behalf of and under the instructions of the Controller.

This Data Processing Agreement (hereinafter “DPA”) specifies the data protection obligations of the Parties pursuant to Art. 28(3) GDPR and supplements the terms of use (Terms of Service) agreed between the Parties.

Note: This DPA takes effect upon active confirmation by the Controller (see Annex 3). Use of the App requires acceptance of this DPA.

Section 1 – Subject Matter and Duration

(1) Subject Matter

This DPA governs the processing of personal data by the Processor in connection with the provision and operation of the App. Processing shall be carried out exclusively on behalf of and pursuant to the documented instructions of the Controller.

(2) Duration

This DPA shall remain in effect for the entire duration of the Controller’s use of the App. It shall terminate automatically upon uninstallation of the App or termination of the usage relationship, subject to the deletion obligations set out in Section 10.

(3) Nature and Purpose of Processing

The processing serves the following purposes:

- Receiving and processing electronic withdrawal declarations from the Controller’s end customers;
- Sending the legally required confirmation of receipt to the end customer by email;
- Providing an administrative interface (Merchant Admin) for the Controller to manage and document withdrawal cases;
- Optionally: order verification, deadline check, order tagging, audit trail, export functions (depending on the selected plan).

(4) Types of Personal Data

The following categories of personal data are processed:

Data Category	Description	Source
Name	First and/or last name of the end customer	Withdrawal form (entered by end customer)
Email address	For identification and delivery of the	Withdrawal form

	confirmation of receipt	
Order number	To identify the contract being withdrawn	Withdrawal form
Timestamps	Date and time of the withdrawal declaration and confirmation	System-generated
Withdrawal status	Processing status (new / in_progress / completed / rejected)	System-generated / Controller
Language preference	Locale for automatic form language selection (from URL parameter, Shopify session, or browser setting navigator.language)	URL / Shopify session / end customer browser
Email metadata	Delivery status, timestamps of the confirmation email	Email service provider (Resend)
Selected items	Items selected by the customer, incl. title, quantity, and product image reference; where no order can be matched, an optional free-text description of the affected products instead	Withdrawal form / Shopify API
Withdrawal reason (optional)	Optional entry by the customer (selection from predefined reasons); not a mandatory field	Withdrawal form (voluntary input)
Customer comment (optional)	Optional free-text message from the customer	Withdrawal form (voluntary input)
Shopify Order ID / Customer ID	Technical identifiers to associate the withdrawal with the Shopify order	Shopify API
Verification data	Result of matching order number and email (order match, email match)	System-generated
IP address (transient)	Solely for spam and abuse prevention (rate limiting, 60-second window); NOT permanently stored in the database	Request header (transient)

(4a) Write-back to Shopify

Depending on the features enabled and the selected plan, the App writes data back into the Controller's Shopify environment on the Controller's behalf: order tags (e.g., "Withdrawal declared"), Shopify return requests (incl. items, reason, customer comment), order edits / fulfillment holds, and configuration metafields (form settings and texts). This write-back takes place exclusively within the Shopify environment controlled by the Controller.

(5) Categories of Data Subjects

Data subjects are end customers (consumers) of the Controller who submit a withdrawal via the App.

Section 2 – Controller's Right to Issue Instructions

(1) The Processor shall process personal data solely on the basis of documented instructions from the Controller, unless processing is required by Union or Member State law to which the Processor is subject

(Art. 28(3)(a) GDPR). In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits such information on grounds of an important public interest.

(2) The Controller's instructions are primarily documented through the configuration and use of the App (e.g., enabling/disabling features, setting retention periods, configuring email settings), without prejudice to the Controller's right to issue additional documented instructions where necessary to ensure compliance with applicable data protection law or internal compliance requirements. Such additional instructions require text form (email suffices) and shall be directed to hello@buschbytes.com.

(3) The Processor shall immediately inform the Controller if, in its opinion, an instruction violates data protection law. The Processor shall be entitled to suspend the execution of such an instruction until the Controller confirms or amends it.

Section 3 – Obligations of the Processor

The Processor undertakes in particular to:

- process personal data only within the scope of the Controller's documented instructions (Section 2);
- ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR);
- take the technical and organisational measures required under Art. 32 GDPR (see Section 5);
- comply with the conditions for engaging sub-processors set out in Section 6;
- assist the Controller, insofar as possible, in fulfilling the Controller's obligation to respond to requests for exercising data subjects' rights (Art. 15–22 GDPR) (Section 7);
- assist the Controller in ensuring compliance with its obligations under Art. 32–36 GDPR;
- delete or return all personal data after the end of the provision of services in accordance with Section 10;
- make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and allow for and contribute to audits, including inspections (Section 9);
- not process personal data in a manner that would cause the Controller to breach applicable data protection laws; not copy, export, or extract personal data except as strictly necessary to provide the App; and maintain records and information necessary to demonstrate compliance with this DPA and applicable data protection laws;
- not use, input, upload, train, fine-tune, or otherwise improve any artificial intelligence system or machine-learning model using the Controller's personal data or end-customer data without the Controller's prior express written consent. For the avoidance of doubt, no personal data processed under this DPA shall be used to develop, enhance, or benchmark any AI/ML product or service.

Section 4 – Obligations of the Controller

The Controller is in particular obliged to:

- ensure the lawfulness of data processing and bear sole responsibility for the permissibility of processing within the meaning of Art. 6 GDPR;
- inform data subjects (end customers) in accordance with Art. 13 and 14 GDPR about the data processing, including processing by the Processor and its sub-processors;
- accurately and completely reflect the data processing in its own privacy policy;

- ensure that the use of the App and the associated data processing comply with applicable data protection law;
- issue instructions to the Processor in documented form.

Section 5 – Technical and Organisational Measures (TOMs)

(1) The Processor shall implement appropriate technical and organisational measures pursuant to Art. 32 GDPR to ensure a level of security appropriate to the risk.

(2) The measures in place at the time of conclusion of this DPA are described in Annex 1. The Processor is entitled to adapt the measures during the term, provided the agreed level of protection is not reduced. The Controller shall be informed of material changes. The Processor shall not materially reduce the level of security without the Controller's prior written consent. The Processor shall, where technically feasible, comply with reasonable additional minimum security requirements notified by the Controller in writing.

Section 6 – Sub-Processors

(1) The Controller grants the Processor general written authorisation to engage further processors (sub-processors), subject to compliance with paragraphs (2) to (4).

(2) The sub-processors engaged at the time of conclusion of this DPA are listed in Annex 2. By agreeing to this DPA, the Controller approves the engagement of the sub-processors listed therein.

(3) The Processor shall inform the Controller of any intended changes concerning the addition or replacement of sub-processors at least 14 days in advance by email and/or in-app notification. If the Controller does not object within 14 days, approval shall be deemed granted.

(4) If the Controller raises a justified objection, the Processor shall use best efforts to offer an alternative. If no reasonable alternative is available, either Party may terminate this DPA and the usage relationship with 30 days' notice.

(5) The Processor shall ensure that each sub-processor is subject to at least the same data protection obligations as set out in this DPA.

(6) The Processor remains fully liable for the acts and omissions of any sub-processor as if they were the acts and omissions of the Processor. Upon request, the Processor shall disclose to the Controller the processing locations and data protection safeguards applicable to each sub-processor. Sub-processor agreements shall impose obligations no less protective than those in this DPA.

Section 7 – Assistance with Data Subject Rights

(1) The Processor shall assist the Controller in fulfilling the Controller's obligation to respond to requests for exercising data subjects' rights under Art. 15–22 GDPR.

(2) If a data subject contacts the Processor directly, the Processor shall promptly forward the request to the Controller and shall not act independently without the Controller's instruction.

(3) The Processor provides functions within the App's admin interface to view and delete the personal data processed.

Section 8 – Data Breach Notification

(1) The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach (Art. 33(2) GDPR). The notification shall be sent by email to the email address stored in the Controller's Shopify account.

(2) The notification shall contain at least the following, to the extent known at the time of notification: description of the nature of the breach; categories and approximate number of data subjects and data records affected; description of the likely consequences; description of the measures taken or proposed.

(3) The Processor shall assist the Controller in fulfilling its notification obligations under Art. 33 and 34 GDPR.

Section 9 – Accountability and Audit Rights

(1) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in this DPA and Art. 28 GDPR.

(2) The Controller shall have the right to conduct audits, or to have them conducted by a mandated auditor. Audits shall be carried out with reasonable consideration for the Processor's business operations and with a notice period of at least 30 days. In the event of a substantiated suspicion of a personal data breach, a shorter notice period of 7 business days shall apply.

(3) The Processor may alternatively satisfy the audit requirement by providing a suitable and current attestation (e.g., certification, audit report by an independent third party, or self-assessment).

Section 10 – Deletion and Return of Data

(1) Upon termination of the usage relationship (uninstallation of the App), the Processor shall delete all personal data processed on behalf of the Controller, unless statutory retention obligations apply.

(2) Deletion shall take place within 30 days of termination, unless the Controller has previously requested the return of data (e.g., via CSV export).

(3) During the term, the retention periods configured by the Controller or defined by the selected plan shall apply:

- Starter plan: automatic deletion after 90 days (fixed);
- Essential / Professional plan: configurable retention (6 / 12 / 18 / 24 months), adjustable by the Controller.

(4) The Processor shall confirm deletion upon request by the Controller.

(5) Where deleted data are still contained in database backups, these backups are overwritten automatically within 7 days of the respective deletion. This applies equally to deletions under paragraphs 1 to 3.

Section 11 – International Data Transfers

(1) Processing of personal data shall take place primarily within the EU/EEA. The primary data infrastructure is located in Germany (Frankfurt) and the Netherlands (Amsterdam).

(2) Where individual sub-processors process personal data outside the EU/EEA (see Annex 2), the Processor shall ensure an adequate level of data protection through appropriate safeguards, in particular:

- Adequacy decision of the European Commission (Art. 45 GDPR);
- EU Standard Contractual Clauses (SCCs, Art. 46(2)(c) GDPR);
- Certification under the EU-US Data Privacy Framework;
- Other appropriate safeguards pursuant to Art. 46 GDPR.

(3) The Processor shall not commence any new third-country transfer of the Controller's personal data without the Controller's prior written authorisation and disclosure of the recipient country, transfer mechanism, and relevant sub-processor.

(4) Upon request, the Processor shall provide copies of applicable SCCs/transfer safeguards and conduct/document a transfer impact assessment and supplementary measures where required.

(5) The Processor shall promptly notify the Controller if it becomes aware that it cannot comply with the transfer safeguards or that the law/practice of a third country undermines protection. The Controller may suspend affected transfers or terminate affected services if equivalent protection cannot be ensured.

(6) Annex 2 sets out any third-country transfers and the safeguards applied in each case.

Section 12 – Liability

(1) The liability of the Parties shall be governed by the provisions of the GDPR, in particular Art. 82 GDPR, as well as applicable statutory provisions.

(2) The Processor shall only be liable to data subjects to the extent that it has not fulfilled its obligations under the GDPR or has acted contrary to the lawful instructions of the Controller.

(3) Where a Party is required to pay compensation to data subjects, it shall have a right of recourse against the other Party to the extent that the other Party has caused the damage.

(4) Each party shall, at its own cost, maintain throughout the term of this DPA insurance coverage appropriate to the nature and scope of its contractual obligations, including professional liability insurance and cyber liability insurance, in each case with reputable insurers and coverage limits that are commercially reasonable for its business and the risks associated with its performance.

Section 13 – Final Provisions

(1) This DPA shall be governed by the laws of the Federal Republic of Germany, unless mandatory data protection provisions of the Controller's EU Member State take precedence.

(2) Amendments and additions to this DPA require text form. This also applies to any waiver of this text form requirement.

(3) Should any provision be or become invalid, the remaining provisions shall continue in full force. The Parties shall replace the invalid provision with one most closely approximating its intent.

(4) In the event of conflicts between this DPA and other agreements, this DPA shall prevail with respect to data protection matters.

(5) The Processor may adapt this DPA in response to changes in law or technical infrastructure, subject to the following distinction:

- Editorial adjustments (e.g., correction of typographical errors, updating of contact details) and changes required by mandatory legal provisions shall be communicated to the Controller at least 30 days before taking effect by email and/or in-app notification. If the Controller does not object within 30 days, the amendment shall be deemed approved.
- Material changes – in particular those affecting the scope of processing, the mandatory contents pursuant to Art. 28(3) GDPR, the list of sub-processors, technical and organisational measures, or international data transfers – require the Controller's express consent in text form (email suffices).

Annex 1 – Technical and Organisational Measures (TOMs)

Status at the time of conclusion of this DPA. Continuously adapted to the state of the art.

Measure	Description
Encryption in transit	TLS 1.2+ for all connections (storefront, API, admin, email delivery)
Encryption at rest	Database level (Supabase/PostgreSQL: AES-256); encrypted backups
Access control	Least-privilege principle; production data restricted to the operator; MFA for infrastructure access
Tenant separation	Logical separation of merchant data at database level (Row-Level Security via Supabase)
Input validation	Server-side input validation; anti-spam measures (honeypot, rate limiting)
Availability	Hosting on Fly.io (EU: Amsterdam, Frankfurt) with automatic failover; database on Supabase (Frankfurt) with automated backups
Processing control	Processing exclusively pursuant to documented instructions; no disclosure to third parties other than approved sub-processors
Purpose limitation	Strict purpose limitation; separate processing of merchant and end-customer data
Deletion concept	Automatic deletion per retention period (Starter: 90 days fixed; Essential/Professional: 6 to 24 months, configurable); deletion upon uninstallation within 30 days; database backups overwritten within 7 days of deletion
Monitoring & incident response	Error tracking via Sentry (EU region, data residency Frankfurt). End-customer personal data is masked before transmission to Sentry (sendDefaultPii=false, server-side and client-side PII scrubbing). Logging of security-relevant events; defined incident response process
Data minimisation	Collection only of data strictly necessary for the withdrawal process; withdrawal reason and customer comment are optional fields and never mandatory

Annex 2 – Approved Sub-Processors

As of: May 2026. Changes communicated pursuant to Section 6(3).

Provider	Purpose	Location / Region	Third-Country Transfer / Safeguard	Contractual Basis
Supabase Pte. Ltd	Database hosting (PostgreSQL)	Frankfurt, Germany (EU)	EU – no third-country transfer	DPA with Supabase (incl. SCCs)
Fly.io Inc.	Application hosting / server	Amsterdam (NL), Frankfurt (DE)	EU – no third-country transfer	DPA with Fly.io (incl. SCCs)
Resend Inc. (Plus Five Five, Inc.)	Email delivery (confirmation of receipt)	Ireland (eu-west-1)	Certified under EU-US Data Privacy Framework (since 20 Feb 2025). Data processing in EU region. Additionally: SCCs.	DPA with Resend (incl. SCCs)
Sentry (Functional Software Inc.)	Error tracking and performance monitoring (technical data only; no end-customer PII is transmitted)	Frankfurt, Germany (EU region)	EU – no third-country transfer with EU configuration. Certified under EU-US Data Privacy Framework. Additionally: SCCs.	DPA with Sentry (incl. SCCs)
Crisp IM SAS	In-app support chat for merchants (no end-customer data)	France (company); Netherlands / Germany (data)	EU – no third-country transfer	DPA with Crisp
Shopify Inc.	E-commerce platform; API access to order data for order verification	Canada / Global	Adequacy decision (Canada); supplemented by SCCs	Shopify Partner Agreement; Shopify DPA

Note: The Processor endeavours to keep data processing within the EU/EEA. Data Processing Agreements (DPAs) have been concluded with all sub-processors. For sub-processors based in third countries, an adequate level of protection is ensured through contractual measures (SCCs) and/or certification under the EU-US Data Privacy Framework.

Annex 3 – Conclusion of Agreement and Contact Details

Conclusion of Agreement

This DPA takes effect when the Controller actively confirms acceptance. Confirmation is provided via the App (Settings → "Data Processing Agreement" section → checkbox → "Accept DPA"). The date and time of acceptance are recorded electronically.

The full DPA is available at https://www.consumer-withdrawal.eu/dpa at all times and can be downloaded as a PDF.

Contact Details for Data Protection Enquiries

Processor	Jonas Busch (Sole Proprietor / Einzelunternehmer)
Address	Hofstraße 2-4, 51061 Cologne, Germany · VAT ID: DE449524313
Email (Data Protection)	hello@buschbytes.com
Website	https://www.consumer-withdrawal.eu
Data Protection Officer	Not appointed (no obligation pursuant to Art. 37 GDPR)