Data Processing Agreement (DPA)

pursuant to Art. 28(3) GDPR

in connection with the use of the Shopify app

"EasyWiderruf"

between

Maik Gossen (Sole Proprietor)

Emanuel-Geibel-Straße 3, 65185 Wiesbaden, Germany

Email: info@dd-gossen.com

hereinafter referred to as the "Data Processor" or "Processor"

and

The Merchant (Data Controller),

who installs and uses the app via the Shopify App Store

hereinafter referred to as the "Data Controller" or "Controller"

collectively the "Parties", individually a "Party"

Version: June 2026 (v1.0)

The German version of this DPA is legally binding. This English translation is provided for convenience only.

Preamble

The Data Processor operates the Shopify app "EasyWiderruf" (hereinafter referred to as the "App"). The App assists the Data Controller in the technical implementation of the electronic withdrawal function pursuant to Section 356a of the German Civil Code (BGB) (effective 19 June 2026) and EU Directive (EU) 2023/2673.

In connection with the use of the App, the Data Processor processes personal data of end customers of the Data Controller (consumers who submit a withdrawal via the App) on behalf of and under the instructions of the Data Controller.

This Data Processing Agreement (hereinafter referred to as "DPA") specifies the data protection obligations of the Parties pursuant to Art. 28(3) GDPR and supplements the terms of service agreement between the Parties (Terms of Service of the App).

Note: This DPA enters into force upon active confirmation by the Data Controller (see Annex 3). The use of the App requires acceptance of this DPA.

§ 1 Subject Matter and Duration of Processing

(1) Subject Matter

The subject matter of this DPA is the processing of personal data by the Data Processor in connection with the provision and operation of the App. Processing is carried out exclusively on behalf of and pursuant to documented instructions from the Data Controller.

(2) Duration

This DPA applies for the entire duration of the Data Controller's use of the App. It terminates automatically upon uninstallation of the App or termination of the usage relationship, subject to the deletion obligations set forth in Section 10.

(3) Nature and Purpose of Processing

The processing serves the following purposes:

- Receipt and processing of electronic withdrawal declarations from end customers of the Data Controller;
- Transmission of the legally required receipt confirmation via email to the end customer;
- Provision of a management interface (Merchant Admin) for the Data Controller to process and document withdrawal cases;
- Optional: order verification, deadline check, order tagging, automatic Shopify returns, export functions (depending on the selected feature scope/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 (input by end customer)
Email address	For identification and delivery of the receipt confirmation	Withdrawal form
Order number	For identification of the contract subject to withdrawal	Withdrawal form
Timestamp	Date and time of the withdrawal declaration and confirmation	System generated
Withdrawal status	Processing status (new / in_progress / completed / rejected)	System generated / Data Controller
Language preference	Locale for automatic language selection of the form	URL / Shopify session / end customer's browser
Email metadata	Delivery status, timestamp of the confirmation email	Email service provider (Mailjet)
Selected items	For partial withdrawal: items selected by the customer including title, quantity, and product image reference	Withdrawal form / Shopify API
Withdrawal reason (optional)	Optional statement by the customer; 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 for associating 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)	Exclusively for spam and abuse prevention (rate limiting, 60 second window); NO permanent storage in the database	Request header (transient)

(4a) Data Return to Shopify

Depending on activated features and the selected plan, the App writes data back to the Data Controller's Shopify environment on behalf of the Data Controller: order tags (e.g., "Withdrawal declared"), Shopify Return Requests (including items, reason, customer comment), configuration metafields (form settings and texts). This data return occurs exclusively within the Shopify environment controlled by the Data Controller.

(5) Categories of Data Subjects

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

§ 2 Instructions of the Data Controller

(1) The Data Processor shall process personal data exclusively on the basis of documented instructions from the Data Controller, unless required to do so by Union or Member State law to which the Data Processor is subject (Art. 28(3)(a) GDPR). In such a case, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest.

The Data Controller's instructions are primarily documented through the configuration and use of the App (e.g., activation/deactivation of features, setting of retention periods, configuration of email settings). This does not affect the Data Controller's right to issue additional documented instructions insofar as this is necessary to comply with applicable data protection regulations or internal compliance requirements. Such additional instructions must be in text form (email is sufficient) and shall be addressed to info@dd-gossen.com.

(3) The Data Processor shall immediately inform the Data Controller if, in the Data Processor's opinion, an instruction infringes data protection regulations. The Data Processor shall be entitled to suspend the execution of such an instruction until the Data Controller confirms or amends it.

§ 3 Obligations of the Data Processor

The Data Processor undertakes in particular:

- to process personal data exclusively within the scope of the documented instructions of the Data Controller (Section 2);
- to ensure that persons authorized to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR);
- to take the technical and organizational measures required under Art. 32 GDPR (see Section 5 of this DPA);
- to comply with the conditions set out in Section 6 for engaging sub-processors;
- to assist the Data Controller, where possible, by appropriate technical and organizational measures in fulfilling the Data Controller's obligation to respond to requests for exercising the data subject's rights (Art. 15 to 22 GDPR) (Section 7);
- to assist the Data Controller in ensuring compliance with obligations pursuant to Art. 32 to 36 GDPR (security, notification of personal data breaches, data protection impact assessment, prior consultation);

• to delete or return all personal data after the end of the processing in accordance with Section 10;

• to make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and to allow for and contribute to audits, including inspections (Section 9).

§ 4 Obligations of the Data Controller

The Data Controller is obligated in particular:

• to ensure the lawfulness of data processing and to bear sole responsibility for the permissibility of processing within the meaning of Art. 6 GDPR;

• to inform the data subjects (end customers) pursuant to Art. 13 and 14 GDPR about the data processing, including processing by the Data Processor and its sub-processors;

• to accurately and completely reflect the data processing in the Data Controller's own privacy policy;

• to ensure that the use of the App and the associated data processing comply with applicable data protection regulations;

• to issue instructions to the Data Processor in documented form.

§ 5 Technical and Organizational Measures (TOMs)

(1) The Data Processor shall, pursuant to Art. 32 GDPR, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

(2) The measures in place at the time of conclusion of this agreement are described in Annex 1 (Technical and Organizational Measures). The Data Processor is entitled to adapt these measures during the term of the agreement, provided that the agreed level of protection is not reduced. The Data Controller shall be informed of any material changes.

§ 6 Sub-Processors

(1) The Data Controller grants the Data Processor general written authorization to engage additional processors (sub-processors), provided that the conditions set out in paragraphs (2) to (4) are met.

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

therein.

(3) The Data Processor shall inform the Data Controller of any intended changes regarding the addition or replacement of sub-processors, thereby giving the Data Controller the opportunity to object to such changes. Notification shall be provided via email and/or in-app notification. If the Data Controller does not raise an objection within 14 days of receipt of the notification, the authorization shall be deemed granted.

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

(5) The Data Processor shall ensure that each sub-processor is subject to at least the same data protection obligations as set out in this DPA, in particular with regard to technical and organizational measures and compliance with instructions.

§ 7 Assistance with Data Subject Rights

(1) The Data Processor shall assist the Data Controller, where possible, by appropriate technical and organizational measures in fulfilling the Data Controller's obligation to respond to requests for exercising the rights of data subjects set forth in Art. 15 to 22 GDPR.

(2) If a data subject (end customer) contacts the Data Processor directly to exercise their rights, the Data Processor shall forward such request to the Data Controller without undue delay and shall not act independently towards the data subject without instructions from the Data Controller.

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

§ 8 Notification of Personal Data Breaches

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

(2) The notification shall contain at least the following information, insofar as 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 to address the breach.

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

§ 9 Demonstration of Compliance and Audit Rights

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

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

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

§ 10 Deletion and Return of Data

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

(2) Deletion shall be carried out within 30 days of termination of the usage relationship, unless the Data Controller has previously requested the return of the data (e.g., via CSV export).

(3) During the term of the agreement, the retention periods configured by the Data Controller or prescribed by the respective feature scope (plan) shall apply:

- Free Plan: automatic deletion after 90 days (fixed);
- Pro Plan: configurable retention period by the Data Controller.

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

§ 11 Data Transfers to Third Countries

(1) The processing of personal data takes place in principle within the European Union / European Economic Area (EU/EEA). The primary data infrastructure is located in Germany (Frankfurt).

(2) Insofar as individual sub-processors process personal data outside the EU/EEA (see Annex 2), the Data Processor shall ensure that an adequate level of data protection is guaranteed through appropriate safeguards. This may be achieved in particular through:

- 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 Data Processor provides information in Annex 2 regarding any third country transfers and the respective safeguards applied.

§ 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 general statutory provisions.

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

(3) Where a Party is obligated to pay damages to data subjects, it shall be entitled to claim recourse against the other Party to the extent that the other Party caused the damage.

§ 13 Final Provisions

(1) This DPA is governed by German law, unless mandatory data protection provisions of the EU Member State of the Data Controller take precedence.

(2) Amendments and supplements to this DPA must be made in text form. This also applies to the waiver of this text form requirement.

(3) Should any provision of this DPA be or become invalid or unenforceable, this shall not affect the validity of the remaining provisions. The Parties undertake to replace the invalid provision with a valid provision that most closely achieves the economic and data protection purpose of the invalid provision.

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

(5) The Data Processor is entitled to amend this DPA in the event of changes in the legal framework or technical infrastructure. The following distinction applies:

• Editorial amendments (e.g., correction of typographical errors, updating of contact details) as well as changes mandated by legal requirements shall be communicated to the Data Controller at least 30 days before taking effect via email and/or in-app notification. If the Data Controller does not object within 30 days, the amendment shall be deemed approved.

• Material substantive amendments, in particular those affecting the scope of processing, the mandatory contents pursuant to Art. 28(3) GDPR, the list of sub-processors, the technical and organizational measures, or third country transfers, shall require the express consent of the Data Controller in text form (email is sufficient).

Annex 1 Technical and Organizational Measures (TOMs)

The following measures describe the status at the time of conclusion of the agreement and are continuously adapted to the state of the art.

Measure	Description
Encryption in transit	TLS 1.2+ for all connections (storefront, API, admin, email transmission)
Encryption at rest	SQLite database on encrypted Fly.io volume; encrypted backups
Access control	Principle of least privilege; access to production data limited to the operator only; multi-factor authentication for infrastructure access
Tenant separation	Logical separation of merchant data at the database level (shop-based isolation)
Input validation	Server-side input validation; anti-spam measures (honeypot, rate limiting)
Availability control	Hosting on Fly.io (EU region: Frankfurt) with automatic health check and restart
Processing control	Processing exclusively in accordance with documented instructions; no disclosure to third parties except to approved sub-processors
Separation control	Strict purpose limitation of data processing; separate processing of merchant and end customer data
Deletion concept	Automatic deletion according to configured retention period (90 days on Free Plan); deletion after uninstallation within 30 days
Data minimization	Collection of only the data strictly necessary for the withdrawal process; no permanent storage of IP addresses

Annex 2 Approved Sub-Processors

As of: June 2026. Changes will be communicated in accordance with Section 6(3).

Provider	Purpose	Location / Region	Third Country Transfer / Safeguard	Contractual Basis
Fly.io Inc.	Application hosting / server	Frankfurt, Germany (EU)	EU, no third country transfer	DPA with Fly.io (incl. SCCs)
Mailjet SAS	Email delivery (receipt confirmation)	France (EU)	EU, no third country transfer	DPA with Mailjet
Shopify Inc.	E-commerce platform; API access to order data for order verification	Canada / Global	Adequacy decision (Canada); additionally SCCs	Shopify Partner Agreement; Shopify DPA

Note: The Data Processor endeavors to keep data processing within the EU/EEA as far as possible. A Data Processing Agreement (DPA) has been concluded with each sub-processor. For sub-processors located in third countries, an adequate level of protection is ensured through contractual measures (in particular SCCs) and/or certification under the EU-US Data Privacy Framework.