

# Data Processing Agreement (DPA)

Version 1.2 · Last updated: July 28, 2026

*This is a convenience translation. The German Auftragsverarbeitungsvertrag (AVV) is the legally binding version.*

Agreement on processing on behalf of a controller (Art. 28 GDPR) between the merchant operating the Shopify store that installs the “Extra Carts” app – the **Controller** – and Q4 Reach Labs GmbH, Berthold-Litzmann-Str. 12a, 80995 Munich, Germany – the **Processor**.

## §1 Subject, duration

(1) The Processor provides event-based product-recommendation emails to the Controller’s existing customers plus the related attribution and billing (the “Service”), as described in **Annex 1** in its activated version. (2) Effective on app installation; ends on uninstall; §9 (deletion) and §11 (records) survive.

## §2 Nature, purpose, data categories, data subjects

Exhaustively described in **Annex 1**, structured by processing stages (Stage 1 active from installation; later stages only per §12). Summary: end-customer master data (email, name, salutation/locale), consent/marketing status, order and product data, email send and interaction events, click/attribution data, email replies (forwarded to the Controller’s support). **No special categories** (Art. 9 GDPR); the Controller ensures none are transmitted.

## §3 Instructions

(1) Processing only on documented instructions; the app configuration and this agreement constitute the documented instructions. (2) If an instruction appears unlawful, the Processor informs the Controller and may suspend. (3) **Conservative**

**principle:** where the legal basis of an individual send is unclear, the send is suppressed – agreed as instruction-compliant.

## §4 Confidentiality

All authorized persons are bound to confidentiality (Art. 28(3)(b) GDPR).

## §5 Security

Technical and organizational measures per **Annex 2**, at minimum: encryption at rest (AES-256 or equivalent) and in transit (TLS 1.2+), least-privilege access control, pseudonymized recipient identifiers in analytics, no personal data in application logs or error monitoring, secrets management, daily backups (30-day retention), RTO < 4 h / RPO < 15 min, quarterly restore test, pre-launch penetration test.

## §6 Sub-processors

(1) General authorization for the sub-processors listed in **Annex 3**. (2) Changes announced at least **30 days** in advance; objection for good data-protection cause; unresolved objection → special termination right (uninstall). (3) Equivalent obligations imposed on sub-processors. (4) Third-country transfers only with appropriate safeguards (Art. 44 et seq. GDPR).

## §7 Assistance

The Processor supports the Controller regarding data-subject rights (Art. 12–23) and Art. 32–36 duties; access requests (customers/data\_request) and deletion requests (customers/redact) are fulfilled **within 48 hours** of webhook receipt.

## §8 Breach notification

Without undue delay, at the latest within 48 hours of awareness, with the Art. 33(3) GDPR particulars, documented.

## §9 Deletion and return

(1) On uninstall: immediate send stop; complete deletion of all shop data at the latest with the shop/redact webhook (48 hours). (2) Ongoing deletion periods per **Annex 1**. (3) Exception: pseudonymized billing evidence without personal reference is retained 7 years for commercial/tax purposes (Art. 28(3)(g), last clause). (4) The suppression list is kept indefinitely as hashed email – legal basis: safeguarding the marketing objection.

## §10 Audit rights

The Processor provides all information necessary to demonstrate Art. 28 GDPR compliance and enables audits: annually and for cause, with reasonable notice, during business hours, without disrupting operations; primarily via current audit reports/certifications where sufficient.

## §11 Anonymized statistics

(1) The Processor may create and use **anonymized, aggregated statistics** from service delivery (counters and rates per subject-line variant – no order values, no catalog data, no personal data) to improve service quality for all merchants; this is a purpose specified by the Controller. (1a) These aggregates are **not** used to create, train, or improve machine-learning or AI systems except with Shopify's prior written consent (cf. Shopify API Terms §2.3(24)). (2) Aggregates contain **no end-customer personal data and no merchant-identifying information**; minimum cohorts:  $\geq 10$  merchants and  $\geq 1,000$  sends per aggregate. (3) Re-identification is technically and organizationally excluded. (4) A plain-language summary of changes is kept in Annex 4.

## §12 Staged model, changes to Annex 1

(1) Annex 1 describes all planned processing stages; only **Stage 1** is active at signature. (2) Activation of a later stage is announced at least **30 days** in advance in text form and in the dashboard with a plain-language changelog (Annex 4). (3) On objection, the stage is not activated for that Controller where technically

separable; otherwise a special termination right exists. (4) Material purpose changes outside the pre-described stages require a new agreement.

## **§13 Liability, final provisions**

Liability per Art. 82 GDPR and statutory rules. German law; venue is Munich. Severability. In conflicts with the Terms of Service, this agreement prevails on data protection. **The German AVV is the authoritative text; this translation is for convenience.**

## **Annex 1 – Processing description (staged model)**

**Stage 1 – active from installation.** Purpose: event-based product recommendations by email to existing customers (post-purchase, similar goods within the meaning of §7(3) UWG), click attribution, percentage billing of the attributed order value on the Fair plan (6% of the gross merchandise value incl. taxes, excl. shipping, at the cycle-end snapshot; on the Free plan, sending pauses after the first 100 recommendations of each billing cycle and no billing occurs), subject-line rotation for quality measurement (variant-level aggregate evaluation per §11).

Data categories:

- order data of the last 60 days (line items, refund, payment and fulfillment state, customer-journey data)
- end-customer master data: email, first and last name, salutation/locale, marketing-consent status
- product and variant data (title, image, URL, price, availability, product type, collection membership)
- email send and interaction events, click/attribution data
- end-customer email replies (forwarded to the merchant's support)

Data subjects: the merchant's end customers.

Deletion periods:

| Data category                                             | Period                                                                                                |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| End-customer master data<br>(email, name)                 | deleted on the customers/redact signal or 24 months<br>after last interaction – whichever comes first |
| Click logs                                                | 24 months                                                                                             |
| Audit logs                                                | 24 months                                                                                             |
| Pseudonymized billing evidence<br>(no personal reference) | 7 years (commercial/tax law)                                                                          |
| Suppression list (hashed email)                           | indefinite (safeguarding the marketing objection)                                                     |

Otherwise, personal data is deleted as soon as it is no longer required for the purposes named in this annex. Place of processing: EU.

**Stage 2 – pre-described, not active.** Abandoned-checkout trigger (including checkout data); control-group (holdout) assignment to measure added value and automatic credits (performance credit). Activation per §12.

**Stage 3 – pre-described, not active.** Further triggers per the product roadmap (repurchase/winback, replenishment reminder, back-in-stock notification on the customer's explicit request); possibly further markets. Activation per §12.

## Annex 2 – Technical and organizational measures (Art. 32 GDPR)

**Confidentiality and access control:** encryption of personal data at rest (AES-256 or equivalent); transport encryption TLS 1.2+ for all access; least-privilege access control; separation of PII storage from behavioral/analytics storage where practical; pseudonymization (hashing) of recipient identifiers in analytics tables.

**Data minimization in operations:** no personal data in application logs; no personal data in error-monitoring payloads.

**Integrity:** HMAC verification of all Shopify webhook signatures; HMAC-signed, time-bounded click-redirect tokens; secrets in a managed secrets store (no secrets in container environment variables).

**Availability and resilience:** daily backups with 30-day retention; recovery objectives RTO < 4 h / RPO < 15 min; quarterly restore test; queues retain events on processing failure.

**Regular review procedures:** quarterly dependency audit; penetration test before public launch; continuous system monitoring.

## Annex 3 – Sub-processors

| Company                                                                        | Service          | Location / place of processing | Safeguard |
|--------------------------------------------------------------------------------|------------------|--------------------------------|-----------|
| Brevo                                                                          | email delivery   | EU                             | DPA       |
| Hosting provider – named in this list before the first send                    | hosting/database | EU region                      | DPA       |
| Error monitoring (no personal data) – named in this list before the first send | error monitoring | EU region intended             | DPA/SCC   |

Changes to this list are announced at least 30 days in advance per §6.

## Annex 4 – Change log (plain language)

| Date       | Version | Stage/change                    | What changes for you                                                                                                                              | Your options                                  |
|------------|---------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| 2026-07-14 | 1.0     | Stage 1 active                  | –                                                                                                                                                 | –                                             |
| 2026-07-28 | 1.1     | Fees adjusted (Annex 1, §3 ToS) | Fee now 6% of gross merchandise value instead of 9% net; first 100 recommendations free; billing at cycle end                                     | Terminate any time (uninstall)                |
| 2026-07-28 | 1.2     | Two plans: Free/Fair (Annex 1)  | Only recommendations sent on the Fair plan are billed; on the Free plan sending pauses after 100 recommendations per cycle – with no billing ever | Choose your plan any time; uninstall any time |

## Versions

- [Version 1.2 · current version](#)
- [Version 1.1 · PDF](#)
- [Version 1.0 · PDF](#)