Auftragsverarbeitungsvertrag (AVV)

Version 1.0 · Stand: 14. Juli 2026

Vereinbarung über die Auftragsverarbeitung gemäß Art. 28 DSGVO zwischen dem Händler (Betreiber des Shopify-Shops, der die App „Extra Carts“ installiert) — **„Verantwortlicher“** — und der Q4 Reach Labs GmbH, Berthold-Litzmann-Str. 12a, 80995 München, Deutschland — **„Auftragsverarbeiter“**.

§ 1 Gegenstand und Dauer

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen der ereignisbasierten Produktempfehlung per E-Mail an Bestandskunden des Verantwortlichen sowie die zugehörige Attribution und Abrechnung („Leistung“), näher beschrieben in **Anlage 1** in ihrer jeweils aktivierten Fassung. (2) Die Vereinbarung wird mit Installation der App wirksam und endet mit Deinstallation; § 9 (Löschung) und § 11 (Nachweise) gelten fort.

§ 2 Art, Zweck, Datenkategorien, betroffene Personen

Abschließend beschrieben in **Anlage 1**, gegliedert nach Verarbeitungsstufen (Stufe 1 aktiv ab Installation; weitere Stufen nur nach dem Verfahren in § 12). Zusammengefasst: Endkunden-Stammdaten (E-Mail, Name, Anrede/Sprache), Einwilligungs-/Werbestatus, Bestell- und Produktdaten, E-Mail-Versand- und Interaktionsereignisse, Klick-/Attributionsdaten, E-Mail-Antworten von Endkunden (Weiterleitung an den Händler-Support). **Keine besonderen Kategorien** nach Art. 9 DSGVO; der Verantwortliche stellt sicher, dass solche Daten nicht übermittelt werden.

§ 3 Weisungsgebundenheit

(1) Verarbeitung ausschließlich auf dokumentierte Weisung des Verantwortlichen; die App-Konfiguration und diese Vereinbarung gelten als dokumentierte Weisung. (2) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich und darf die Ausführung aussetzen. (3) **Konservativer Grundsatz:** Bei unklarer Rechtsgrundlage einer einzelnen Zusendung unterbleibt der Versand (Suppression); dies gilt als weisungskonform vereinbart.

§ 4 Vertraulichkeit

Alle zur Verarbeitung befugten Personen sind zur Vertraulichkeit verpflichtet (Art. 28 Abs. 3 lit. b DSGVO).

§ 5 Sicherheit der Verarbeitung

Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO nach **Anlage 2**, mindestens: Verschlüsselung personenbezogener Daten im Ruhezustand (AES-256 oder gleichwertig) und bei Übertragung (TLS 1.2+), Least-Privilege-Zugriffskontrolle, Pseudonymisierung von Empfänger-Kennungen in Analysetabellen, keine personenbezogenen Daten in Anwendungs-Logs oder Fehler-Monitoring, Secrets-Management, tägliche Backups mit 30-Tage-Aufbewahrung, RTO < 4 h / RPO < 15 min, vierteljährlicher Restore-Test, Penetrationstest vor öffentlichem Launch.

§ 6 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt die **allgemeine Genehmigung** zum Einsatz der in **Anlage 3** gelisteten Unterauftragsverarbeiter. (2) Änderungen werden mindestens **30 Tage** vorab mitgeteilt; der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen; bei nicht ausräumbarem Widerspruch besteht ein Sonderkündigungsrecht (Deinstallation). (3) Pflichten werden Unterauftragsverarbeitern vertraglich in gleichwertiger Weise auferlegt.

(4) Drittlandübermittlungen erfolgen nur mit geeigneten Garantien (Art. 44 ff. DSGVO).

§ 7 Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Betroffenenrechten (Art. 12–23) und den Pflichten aus Art. 32–36. Technisch umgesetzt u. a. über die Shopify-Privacy-Webhooks: Auskunftsanfragen (customers/data_request) und Löschanfragen (customers/redact) werden **innerhalb von 48 Stunden** ab Webhook-Eingang erfüllt.

§ 8 Meldung von Verletzungen

Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten **unverzüglich**, spätestens innerhalb von 48 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, und dokumentiert Verlauf und Abhilfemaßnahmen.

§ 9 Löschung und Rückgabe

(1) Nach Deinstallation: sofortiger Versandstopp; vollständige Löschung aller Shop-Daten spätestens mit dem shop/redact-Webhook (48 Stunden nach Auslösung durch Shopify). (2) Regellöschfristen im laufenden Betrieb gemäß **Anlage 1**. (3) **Ausnahme:** pseudonymisierte Abrechnungsnachweise ohne Personenbezug werden zu handels-/steuerrechtlichen Zwecken 7 Jahre aufbewahrt (Art. 28 Abs. 3 lit. g, letzter Hs.). (4) Die Unterdrückungsliste (Suppression) wird als gehashte E-Mail unbefristet geführt — Rechtsgrundlage: Sicherstellung des Werbewiderspruchs.

§ 10 Nachweis- und Kontrollrechte

Der Auftragsverarbeiter stellt alle erforderlichen Informationen zum Nachweis der Pflichten nach Art. 28 DSGVO bereit und ermöglicht Überprüfungen. Audits: einmal jährlich sowie anlassbezogen, mit angemessener Vorankündigung,

während der Geschäftszeiten, ohne Störung des Betriebs; vorrangig durch Vorlage aktueller Prüfberichte/Zertifikate, soweit ausreichend.

§ 11 Anonymisierte Auswertungen

(1) Der Auftragsverarbeiter darf aus der Leistungserbringung **anonymisierte, aggregierte Statistiken** erstellen und nutzen (Zähler und Raten je Betreffzeilen-Variante — keine Bestellwerte, keine Katalogdaten, keine personenbezogenen Daten), um die Qualität der Leistung für alle Händler zu verbessern; dies ist ein vom Verantwortlichen festgelegter Zweck. (1a) Diese Aggregate werden **nicht** zum Erstellen, Trainieren oder Verbessern von Machine-Learning- oder KI-Systemen verwendet, es sei denn mit vorheriger schriftlicher Zustimmung von Shopify (vgl. Shopify API Terms § 2.3(24)). (2) Diese Aggregate enthalten **keine personenbezogenen Daten von Endkunden und keine händleridentifizierenden Angaben**; Mindestkohorten: ≥ 10 Händler und ≥ 1.000 Versendungen je Aggregat. (3) Eine Re-Identifizierung wird technisch und organisatorisch ausgeschlossen. (4) Eine Klartext-Zusammenfassung von Änderungen enthält Anlage 4.

§ 12 Stufenmodell und Änderungen der Anlage 1

(1) Anlage 1 beschreibt sämtliche geplanten Verarbeitungsstufen; bei Vertragsschluss ist ausschließlich **Stufe 1** aktiv. (2) Die Aktivierung einer weiteren Stufe wird dem Verantwortlichen mindestens **30 Tage** vorab in Textform und im Dashboard mit Klartext-Änderungsprotokoll (Anlage 4) angekündigt. (3) Widerspricht der Verantwortliche, wird die Stufe für ihn nicht aktiviert, soweit technisch trennbar; andernfalls besteht ein Sonderkündigungsrecht. (4) Wesentliche Zweckänderungen außerhalb der in Anlage 1 vorgezeichneten Stufen bedürfen einer neuen Vereinbarung.

§ 13 Haftung, Schlussbestimmungen

Haftung nach Art. 82 DSGVO und den gesetzlichen Regeln. Es gilt deutsches Recht; Gerichtsstand ist München. Salvatorische Klausel. Bei Widersprüchen zwischen dieser Vereinbarung und den AGB geht diese Vereinbarung hinsichtlich

des Datenschutzes vor. Bei Abweichungen zwischen Sprachfassungen ist die deutsche Fassung maßgeblich.

Anlage 1 — Verarbeitungsbeschreibung (Stufenmodell)

Stufe 1 — aktiv ab Installation. Zweck: ereignisbasierte Produktempfehlung per E-Mail an Bestandskunden (Post-Purchase, ähnliche Waren i. S. d. § 7 Abs. 3 UWG), Klick-Attribution, prozentuale Abrechnung des attribuierten Bestellwerts (9 %, fällig frühestens 14 Tage nach Zahlungseingang), Betreffzeilen-Rotation zur Qualitätsmessung (variantenbezogene aggregierte Auswertung nach § 11).

Datenkategorien:

- Bestelldaten der letzten 60 Tage (Positionen, Erstattungs-, Zahlungs- und Versandstatus, Customer-Journey-Daten)
- Endkunden-Stammdaten: E-Mail, Vor- und Nachname, Anrede/Sprache, Werbe-Einwilligungsstatus
- Produkt- und Variantendaten (Titel, Bild, URL, Preis, Verfügbarkeit, Produkttyp, Kollektionszugehörigkeit)
- E-Mail-Versand- und Interaktionsereignisse, Klick-/Attributionsdaten
- E-Mail-Antworten von Endkunden (Weiterleitung an den Händler-Support)

Betroffene Personen: Endkunden des Händlers.

Löschfristen:

Datenkategorie	Frist
Endkunden-Stammdaten (E-Mail, Name)	Löschung auf customers/redact-Signal oder 24 Monate nach letzter Interaktion — je nachdem, was früher eintritt
Klick-Protokolle	24 Monate
Audit-Protokolle	24 Monate
Pseudonymisierte Abrechnungsnachweise (ohne Personenbezug)	7 Jahre (handels-/steuerrechtlich)
Unterdrückungsliste (gehashte E-Mail)	unbefristet (Sicherung des Werbewiderspruchs)

Im Übrigen werden personenbezogene Daten gelöscht, sobald sie für die in dieser Anlage genannten Zwecke nicht mehr erforderlich sind. Ort der Verarbeitung: EU.

Stufe 2 — vorgezeichnet, nicht aktiv. Warenkorbabbruch-Trigger (einschließlich Checkout-Daten); Kontrollgruppen-Zuordnung (Holdout) zur Messung des Mehrwerts und automatischer Gutschriften (Performance Credit). Aktivierung nach § 12.

Stufe 3 — vorgezeichnet, nicht aktiv. Weitere Trigger gemäß Produkt-Roadmap (Wiederkauf/Winback, Nachkauf-Erinnerung, Wieder-verfügbar-Benachrichtigung auf ausdrücklichen Kundenwunsch); gegebenenfalls weitere Märkte. Aktivierung nach § 12.

Anlage 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit und Zugriffskontrolle: Verschlüsselung personenbezogener Daten im Ruhezustand (AES-256 oder gleichwertig); Transportverschlüsselung TLS 1.2+ für sämtliche Zugriffe; Least-Privilege-Zugriffskontrolle; Trennung von PII-Speicher und Analyse-/Verhaltensdaten, soweit praktikabel; Pseudonymisierung (Hashing) von Empfänger-Kennungen in Analysetabellen.

Datenminimierung im Betrieb: keine personenbezogenen Daten in Anwendungs-Logs; keine personenbezogenen Daten in Fehlerüberwachungs-Daten.

Integrität: HMAC-Verifikation aller Shopify-Webhook-Signaturen; HMAC-signierte, zeitlich begrenzte Klick-Redirect-Tokens; Secrets in einem verwalteten Secrets-Store (keine Secrets in Umgebungsvariablen von Containern).

Verfügbarkeit und Belastbarkeit: tägliche Backups mit 30 Tagen Aufbewahrung; Wiederherstellungsziele RTO < 4 h / RPO < 15 min; vierteljährlicher Restore-Test; Warteschlangen halten Ereignisse bei Verarbeitungsfehlern vor.

Verfahren zur regelmäßigen Überprüfung: vierteljährliches Abhängigkeits-Audit; Penetrationstest vor dem öffentlichen Launch; laufende Überwachung der Systeme.

Anlage 3 — Unterauftragsverarbeiter

Unternehmen	Leistung	Sitz / Verarbeitungsort	Garantie
Brevo	E-Mail-Versand	EU	AVV
Hosting-Anbieter — wird vor dem ersten Versand in dieser Liste benannt	Hosting/Datenbank	EU-Region	AVV
Fehlerüberwachung (ohne personenbezogene Daten) — wird vor dem ersten Versand in dieser Liste benannt	Fehler-Monitoring	EU-Region angestrebt	AVV/SCC

Änderungen an dieser Liste werden gemäß § 6 mindestens 30 Tage vorab angekündigt.

Anlage 4 — Änderungsprotokoll (Klartext)

Datum	Version	Stufe/Änderung	Was sich für Sie ändert	Ihre Optionen
2026-07-14	1.0	Stufe 1 aktiv	—	—