Auftragsverarbeitungsvertrag

(Data Processing Agreement)

gemäß Art. 28 Abs. 3 DSGVO
(pursuant to Art. 28(3) GDPR)

im Rahmen der Nutzung der Shopify-App

„EasyWiderruf"

zwischen

Maik Gossen (Einzelunternehmer)

Emanuel-Geibel-Straße 3, 65185 Wiesbaden

E-Mail: info@dd-gossen.com

– nachfolgend „Auftragsverarbeiter" oder „AV" –

und

Der Händler (Merchant),

der die App über den Shopify App Store installiert und nutzt

– nachfolgend „Verantwortlicher" oder „Auftraggeber" –

– gemeinsam „Parteien", einzeln „Partei" –

Stand / Version: Juni 2026 (v1.0)

Präambel

Der Auftragsverarbeiter betreibt die Shopify-App „EasyWiderruf" (nachfolgend „App"). Die App unterstützt den Verantwortlichen bei der technischen Umsetzung der elektronischen Widerrufsfunktion gemäß § 356a BGB (ab 19.06.2026) bzw. der EU-Richtlinie (EU) 2023/2673.

Im Rahmen der Nutzung der App verarbeitet der Auftragsverarbeiter personenbezogene Daten von Endkunden des Verantwortlichen (Verbrauchern, die über die App einen Widerruf erklären) im Auftrag und auf Weisung des Verantwortlichen.

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV") konkretisiert die datenschutzrechtlichen Pflichten der Parteien gemäß Art. 28 Abs. 3 DSGVO und ergänzt die zwischen den Parteien bestehende Nutzungsvereinbarung (Terms of Service der App).

Hinweis: Dieser AVV tritt mit aktiver Bestätigung durch den Verantwortlichen in Kraft (vgl. Anlage 3). Die Nutzung der App setzt die Zustimmung zu diesem AVV voraus.

§ 1 – Gegenstand und Dauer der Verarbeitung

(1) Gegenstand

Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Bereitstellung und des Betriebs der App. Die Verarbeitung erfolgt ausschließlich im Auftrag und nach dokumentierter Weisung des Verantwortlichen.

(2) Dauer

Dieser AVV gilt für die gesamte Dauer der Nutzung der App durch den Verantwortlichen. Er endet automatisch mit der Deinstallation der App oder der Beendigung des Nutzungsverhältnisses, vorbehaltlich der in § 10 geregelten Löschpflichten.

(3) Art und Zweck der Verarbeitung

Die Verarbeitung dient folgenden Zwecken:

- Entgegennahme und Verarbeitung elektronischer Widerrufserklärungen von Endkunden des Verantwortlichen;
- Übermittlung der gesetzlich vorgeschriebenen Eingangsbestätigung per E-Mail an den Endkunden;
- Bereitstellung einer Verwaltungsoberfläche (Merchant Admin) für den Verantwortlichen zur Bearbeitung und Dokumentation von Widerrufsvorgängen;
- Optional: Order-Verifizierung, Frist-Check, Order-Tagging, automatische Shopify-Rückgaben, Export-Funktionen (je nach gewähltem Funktionsumfang/Plan).

(4) Art der personenbezogenen Daten

Folgende Kategorien personenbezogener Daten werden verarbeitet:

Datenkategorie	Beschreibung	Quelle
Name	Vor- und/oder Nachname des Endkunden	Widerrufsformular (Eingabe durch Endkunden)
E-Mail-Adresse	Zur Identifikation und Zustellung der Eingangsbestätigung	Widerrufsformular
Bestellnummer	Zur Identifikation des widerrufenen Vertrags	Widerrufsformular
Zeitstempel	Datum und Uhrzeit der Widerrufserklärung und -bestätigung	Systemgeneriert
Widerrufsstatus	Bearbeitungsstatus (new / in_progress / completed / rejected)	Systemgeneriert / Verantwortlicher
Sprachpräferenz	Locale zur automatischen Sprachauswahl des Formulars	URL / Shopify-Session / Browser des Endkunden
E-Mail-Metadaten	Zustellstatus, Zeitstempel der Bestätigungsmail	E-Mail-Dienstleister (Mailjet)
Ausgewählte Artikel	Bei Teilwiderruf: vom Kunden ausgewählte Artikel inkl. Titel, Menge und Produktbild-Referenz	Widerrufsformular / Shopify API
Widerrufsgrund (optional)	Optionale Angabe des Kunden; keine Pflichtangabe	Widerrufsformular (freiwillige Eingabe)
Kundenkommentar (optional)	Optionale Freitextnachricht des Kunden	Widerrufsformular (freiwillige Eingabe)
Shopify Order-ID / Customer-ID	Technische Kennungen zur Zuordnung des Widerrufs zur Shopify-Bestellung	Shopify API
Verifikationsdaten	Ergebnis des Abgleichs von Bestellnummer und E-Mail (Order-Match, E-Mail-Match)	Systemgeneriert
IP-Adresse (transient)	Ausschließlich zur Spam- und Missbrauchsabwehr (Rate-Limiting, 60-Sekunden-Fenster); KEINE dauerhafte Speicherung in der Datenbank	Request-Header (flüchtig)

(4a) Rückübermittlung an Shopify

Je nach aktivierten Funktionen und gewähltem Plan schreibt die App im Auftrag des Verantwortlichen Daten in die Shopify-Umgebung des Verantwortlichen zurück: Order-Tags (z. B. „Withdrawal declared"), Shopify Return Requests (inkl. Artikel, Grund, Kundenkommentar),

Konfigurations-Metafelder (Formulareinstellungen und -texte). Diese Rückübermittlung erfolgt ausschließlich innerhalb der vom Verantwortlichen kontrollierten Shopify-Umgebung.

(5) Kategorien betroffener Personen

Betroffene Personen sind Endkunden (Verbraucher) des Verantwortlichen, die über die App einen Widerruf erklären.

§ 2 – Weisungsbefugnis des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist durch Unionsrecht oder das Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet (Art. 28 Abs. 3 lit. a DSGVO). In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtliche Anforderung vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Die Weisungen des Verantwortlichen werden in erster Linie durch die Konfiguration und Nutzung der App dokumentiert (z. B. Aktivierung/Deaktivierung von Funktionen, Einstellung von Aufbewahrungsfristen, Konfiguration von E-Mail-Einstellungen). Dies lässt das Recht des Verantwortlichen unberührt, zusätzliche dokumentierte Weisungen zu erteilen, soweit dies zur Einhaltung geltender datenschutzrechtlicher Vorschriften oder interner Compliance-Anforderungen erforderlich ist. Solche zusätzlichen Weisungen bedürfen der Textform (E-Mail genügt) und sind an info@dd-gossen.com zu richten.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung einer solchen Weisung auszusetzen, bis der Verantwortliche sie bestätigt oder abändert.

§ 3 – Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich insbesondere:

- die personenbezogenen Daten ausschließlich im Rahmen der dokumentierten Weisungen des Verantwortlichen zu verarbeiten (§ 2);
- sicherzustellen, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO);
- die gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen (vgl. § 5 dieses AVV);
- die in § 6 genannten Bedingungen für die Inanspruchnahme von Unterauftragsverarbeitern einzuhalten;

• den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte betroffener Personen (Art. 15–22 DSGVO) nachzukommen (§ 7);

• den Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32–36 DSGVO zu unterstützen (Sicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation);

• nach Beendigung der Auftragsverarbeitung alle personenbezogenen Daten gemäß § 10 zu löschen oder zurückzugeben;

• dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung zu stellen und Überprüfungen einschließlich Inspektionen zu ermöglichen (§ 9).

§ 4 – Pflichten des Verantwortlichen

Der Verantwortliche ist insbesondere verpflichtet:

• die Rechtmäßigkeit der Datenverarbeitung sicherzustellen und die alleinige Verantwortung für die Zulässigkeit der Verarbeitung im Sinne des Art. 6 DSGVO zu tragen;

• die betroffenen Personen (Endkunden) gemäß Art. 13 und 14 DSGVO über die Datenverarbeitung zu informieren, einschließlich der Verarbeitung durch den Auftragsverarbeiter und dessen Unterauftragsverarbeiter;

• die Datenverarbeitung in seiner eigenen Datenschutzerklärung korrekt und vollständig abzubilden;

• sicherzustellen, dass die Nutzung der App und die damit verbundene Datenverarbeitung den geltenden datenschutzrechtlichen Vorschriften entspricht;

• Weisungen an den Auftragsverarbeiter in dokumentierter Form zu erteilen.

§ 5 – Technische und organisatorische Maßnahmen (TOMs)

(1) Der Auftragsverarbeiter trifft gemäß Art. 32 DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die zum Zeitpunkt des Vertragsschlusses getroffenen Maßnahmen sind in Anlage 1 (Technische und organisatorische Maßnahmen) beschrieben. Der Auftragsverarbeiter ist berechtigt, die Maßnahmen während der Vertragslaufzeit anzupassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Über wesentliche Änderungen ist der Verantwortliche zu informieren.

§ 6 – Unterauftragsverarbeiter (Sub-Processors)

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine schriftliche Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen, sofern die Bedingungen der Absätze (2) bis (4) eingehalten werden.

(2) Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 2 aufgeführt. Durch die Zustimmung zu diesem AVV genehmigt der Verantwortliche den Einsatz der dort genannten Unterauftragsverarbeiter.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern, wobei er dem Verantwortlichen die Möglichkeit gibt, gegen derartige Änderungen Einspruch zu erheben. Die Information erfolgt per E-Mail und/oder In-App-Benachrichtigung. Erhebt der Verantwortliche nicht innerhalb von 14 Tagen nach Zugang der Information Einspruch, gilt die Genehmigung als erteilt.

(4) Erhebt der Verantwortliche berechtigten Einspruch, bemüht sich der Auftragsverarbeiter nach besten Kräften, dem Verantwortlichen eine alternative Lösung anzubieten. Ist keine zumutbare Alternative verfügbar, steht beiden Parteien das Recht zu, den AVV und das Nutzungsverhältnis mit einer Frist von 30 Tagen zu kündigen.

(5) Der Auftragsverarbeiter stellt sicher, dass jedem Unterauftragsverarbeiter mindestens die gleichen datenschutzrechtlichen Pflichten auferlegt werden, wie sie in diesem AVV festgelegt sind, insbesondere hinsichtlich der technischen und organisatorischen Maßnahmen und der Weisungsbindung.

§ 7 – Unterstützung bei Betroffenenrechten

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung seiner Pflicht, Anträge auf Wahrnehmung der in Art. 15–22 DSGVO genannten Rechte betroffener Personen zu beantworten.

(2) Wendet sich eine betroffene Person (Endkunde) direkt an den Auftragsverarbeiter, um ihre Rechte geltend zu machen, leitet der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiter und wird ohne Weisung des Verantwortlichen nicht eigenständig gegenüber der betroffenen Person tätig.

(3) Der Auftragsverarbeiter stellt dem Verantwortlichen über die Admin-Oberfläche der App Funktionen zur Einsicht und Löschung der verarbeiteten personenbezogenen Daten bereit.

§ 8 – Meldung von Datenschutzverletzungen

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird (Art. 33 Abs. 2 DSGVO). Die Benachrichtigung erfolgt per E-Mail an die im Shopify-Konto des Verantwortlichen hinterlegte

E-Mail-Adresse.

(2) Die Benachrichtigung enthält mindestens folgende Informationen, soweit zum Zeitpunkt der Meldung bekannt:

- Beschreibung der Art der Verletzung;
- Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze;
- Beschreibung der wahrscheinlichen Folgen;
- Beschreibung der ergriffenen oder vorgeschlagenen Abhilfemaßnahmen.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Meldepflichten nach Art. 33 und 34 DSGVO.

§ 9 – Nachweispflichten und Kontrollrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zur Verfügung, die zur Überprüfung der Einhaltung der in diesem AVV und in Art. 28 DSGVO niedergelegten Pflichten erforderlich sind.

(2) Der Verantwortliche hat das Recht, Überprüfungen durchzuführen oder durch einen beauftragten Prüfer durchführen zu lassen. Überprüfungen werden unter angemessener Berücksichtigung des Geschäftsbetriebs des Auftragsverarbeiters durchgeführt und mit einer Vorlaufzeit von mindestens 30 Tagen angekündigt. Abweichend hiervon ist bei begründetem Verdacht auf eine Verletzung des Schutzes personenbezogener Daten eine kurzfristige Überprüfung mit einer Vorlaufzeit von 7 Werktagen zulässig.

(3) Der Auftragsverarbeiter kann die Überprüfung alternativ durch Vorlage eines geeigneten und aktuellen Nachweises (z. B. Zertifizierung, Audit-Bericht eines unabhängigen Dritten oder Selbstauskunft) erfüllen.

§ 10 – Löschung und Rückgabe von Daten

(1) Nach Beendigung des Nutzungsverhältnisses (Deinstallation der App) löscht der Auftragsverarbeiter sämtliche im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten, es sei denn, es bestehen gesetzliche Aufbewahrungspflichten.

(2) Die Löschung erfolgt innerhalb von 30 Tagen nach Beendigung des Nutzungsverhältnisses, sofern der Verantwortliche nicht zuvor die Rückgabe der Daten (z. B. per CSV-Export) verlangt.

(3) Während der Vertragslaufzeit gelten die vom Verantwortlichen konfigurierten oder die im jeweiligen Funktionsumfang (Plan) vorgegebenen Aufbewahrungsfristen:

- Free Plan: automatische Löschung nach 90 Tagen (fest);
- Pro Plan: konfigurierbare Aufbewahrungsfrist durch den Verantwortlichen.

(4) Der Auftragsverarbeiter bestätigt die Löschung auf Verlangen des Verantwortlichen.

§ 11 – Datenübermittlung in Drittländer

(1) Die Verarbeitung personenbezogener Daten findet grundsätzlich innerhalb der Europäischen Union / des Europäischen Wirtschaftsraums (EU/EWR) statt. Die primäre Dateninfrastruktur befindet sich in Deutschland (Frankfurt).

(2) Soweit einzelne Unterauftragsverarbeiter personenbezogene Daten außerhalb der EU/des EWR verarbeiten (vgl. Anlage 2), stellt der Auftragsverarbeiter sicher, dass ein angemessenes Datenschutzniveau durch geeignete Garantien gewährleistet wird. Dies kann insbesondere erfolgen durch:

- Angemessenheitsbeschluss der Europäischen Kommission (Art. 45 DSGVO);
- EU-Standardvertragsklauseln (Standard Contractual Clauses, Art. 46 Abs. 2 lit. c DSGVO);
- Zertifizierung unter dem EU-US Data Privacy Framework;
- sonstige geeignete Garantien gemäß Art. 46 DSGVO.

(3) Der Auftragsverarbeiter informiert in Anlage 2 über etwaige Drittlandtransfers und die jeweils angewandten Schutzmaßnahmen.

§ 12 – Haftung

(1) Die Haftung der Parteien richtet sich nach den Regelungen der DSGVO, insbesondere Art. 82 DSGVO, sowie den allgemeinen gesetzlichen Bestimmungen.

(2) Der Auftragsverarbeiter haftet gegenüber betroffenen Personen nur in dem Umfang, in dem er seinen in der DSGVO auferlegten Pflichten nicht nachgekommen ist oder gegen rechtmäßige Weisungen des Verantwortlichen verstoßen hat.

(3) Soweit eine Partei gegenüber betroffenen Personen zum Schadensersatz verpflichtet wird, steht ihr ein Regressanspruch gegen die andere Partei zu, soweit diese den Schaden verursacht hat.

§ 13 – Schlussbestimmungen

(1) Dieser AVV unterliegt dem Recht der Bundesrepublik Deutschland, sofern nicht zwingende datenschutzrechtliche Vorschriften des EU-Mitgliedstaats des Verantwortlichen Vorrang haben.

(2) Änderungen und Ergänzungen dieses AVV bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Textformerfordernisses.

(3) Sollten einzelne Bestimmungen dieses AVV unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hiervon nicht berührt. Die Parteien verpflichten

sich, die unwirksame Bestimmung durch eine wirksame Regelung zu ersetzen, die dem wirtschaftlichen und datenschutzrechtlichen Zweck der unwirksamen Bestimmung möglichst nahekommt.

(4) Im Falle von Widersprüchen zwischen diesem AVV und sonstigen Vereinbarungen zwischen den Parteien hat dieser AVV in Bezug auf datenschutzrechtliche Fragestellungen Vorrang.

(5) Der Auftragsverarbeiter ist berechtigt, diesen AVV bei Änderungen der Rechtslage oder der technischen Infrastruktur anzupassen. Dabei gilt folgende Unterscheidung:

- Redaktionelle Anpassungen (z. B. Korrektur von Schreibfehlern, Aktualisierung von Kontaktdaten) sowie Änderungen, die durch gesetzliche Vorgaben zwingend erforderlich werden, werden dem Verantwortlichen mindestens 30 Tage vor Inkrafttreten per E-Mail und/oder In-App-Benachrichtigung mitgeteilt. Widerspricht der Verantwortliche nicht innerhalb von 30 Tagen, gilt die Änderung als genehmigt.

- Wesentliche inhaltliche Änderungen, insbesondere solche, die den Umfang der Verarbeitung, die Pflichtinhalte nach Art. 28 Abs. 3 DSGVO, die Liste der Unterauftragsverarbeiter, die technischen und organisatorischen Maßnahmen oder den Drittlandtransfer betreffen, bedürfen der ausdrücklichen Zustimmung des Verantwortlichen in Textform (E-Mail genügt).

Anlage 1 – Technische und organisatorische Maßnahmen (TOMs)

Die folgenden Maßnahmen beschreiben den Stand zum Zeitpunkt des Vertragsschlusses und werden laufend dem Stand der Technik angepasst.

Maßnahme	Beschreibung
Verschlüsselung in Transit	TLS 1.2+ für alle Verbindungen (Storefront, API, Admin, E-Mail-Versand)
Verschlüsselung at Rest	SQLite-Datenbank auf verschlüsseltem Fly.io Volume; verschlüsselte Backups
Zugriffskontrolle	Least-Privilege-Prinzip; Zugriff auf Produktionsdaten nur für den Betreiber; Multi-Factor Authentication für Infrastruktur-Zugänge
Mandantentrennung	Logische Trennung der Händlerdaten auf Datenbankebene (Shop-basierte Isolierung)
Eingabekontrolle	Serverseitige Input-Validierung; Anti-Spam-Maßnahmen (Honeypot, Rate Limiting)
Verfügbarkeitskontrolle	Hosting auf Fly.io (EU-Region: Frankfurt) mit automatischem Healthcheck und Neustart
Auftragskontrolle	Verarbeitung ausschließlich gemäß dokumentierter Weisung; keine Weitergabe an Dritte außer an genehmigte Unterauftragsverarbeiter
Trennungskontrolle	Strikte Zweckbindung der Datenverarbeitung; getrennte Verarbeitung von Händler- und Endkundendaten
Löschkonzept	Automatische Löschung gemäß konfigurierter Aufbewahrungsfrist (90 Tage im Free Plan); Löschung nach Deinstallation innerhalb von 30 Tagen
Datensparsamkeit	Erhebung nur der für den Widerrufsprozess zwingend erforderlichen Daten; keine dauerhafte Speicherung von IP-Adressen

Anlage 2 – Genehmigte Unterauftragsverarbeiter (Sub-Processors)

Stand: Juni 2026. Änderungen werden gemäß § 6 Abs. 3 mitgeteilt.

Anbieter	Zweck	Standort / Region	Drittlandtransfer / Schutzmaßnahme	Vertragliche Grundlage
Fly.io Inc.	Application Hosting / Server	Frankfurt, Deutschland (EU)	EU – kein Drittlandtransfer	DPA mit Fly.io (inkl. SCCs)
Mailjet SAS	E-Mail-Versand (Eingangsbestätigung)	Frankreich (EU)	EU – kein Drittlandtransfer	DPA mit Mailjet
Shopify Inc.	E-Commerce-Plattform; API-Zugriff auf Bestelldaten zur Order-Verifikation	Kanada / Global	Angemessenheitsbeschluss (Kanada); ergänzend SCCs	Shopify Partner Agreement; Shopify DPA

Hinweis: Der Auftragsverarbeiter bemüht sich, die Datenverarbeitung so weit wie möglich in der EU/im EWR zu halten. Mit jedem Unterauftragsverarbeiter wurde ein Data Processing Agreement (DPA) abgeschlossen. Bei Unterauftragsverarbeitern mit Sitz in Drittländern wird durch vertragliche Maßnahmen (insbesondere SCCs) und/oder Zertifizierung unter dem EU-US Data Privacy Framework ein angemessenes Schutzniveau sichergestellt.