AUFTRAGSVERARBEITUNG · ART. 28 ABS. 3 DSGVO

Vereinbarung zur Auftragsverarbeitung (AVV)

Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten, die Martini & Radl OG als Anbieter der Shopify-App „EU Widerrufs-Button Pro" im Auftrag des installierenden Händlers vornimmt. Sie wird bei der Installation der App elektronisch akzeptiert und ist gemäß Art. 28 Abs. 9 DSGVO auch ohne Unterschrift gültig.

STAND: 1. JUNI 2026

> **Hinweis — keine Rechtsberatung.** Diese Vereinbarung ist eine sorgfältig erstellte Vorlage für die Auftragsverarbeitung im Rahmen der App „EU Widerrufs-Button Pro". Sie stellt keine Rechtsberatung dar und ersetzt keine anwaltliche Prüfung im Einzelfall. Für rechtsverbindliche Aussagen zu deiner konkreten Konstellation ziehe bitte einen Fachanwalt für IT- bzw. Datenschutzrecht hinzu.

Vertragsparteien

Diese Vereinbarung wird geschlossen zwischen:

Verantwortlicher (Auftraggeber)

Der Shopify-Händler, der die App „EU Widerrufs-Button Pro" in seinem Store installiert und betreibt. Die Identifikation erfolgt eindeutig über die Shop-Domain und die im Shopify-Account hinterlegten Stammdaten.
— nachfolgend „Verantwortlicher" genannt —

Auftragsverarbeiter

Martini & Radl OG
Garnisongasse 4/11
1090 Wien, Österreich
UID: ATU78306557 · Firmenbuch: FN 579551 g · HG Wien
— nachfolgend „Auftragsverarbeiter" genannt —

— beide nachfolgend gemeinsam „Vertragsparteien" —

Präambel

Diese Vereinbarung legt fest, unter welchen Bedingungen der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Die Parteien konkretisieren damit ihre gegenseitigen datenschutzrechtlichen Rechte und Pflichten, wie sie Art. 28 DSGVO für die Erbringung der vereinbarten Leistungen vorgibt.

§ 1 Anwendungsbereich

Diese Vereinbarung gilt für die Verarbeitung (Art. 4 Nr. 2 DSGVO) aller personenbezogenen Daten (nachfolgend „Daten"), die Gegenstand der Leistungsvereinbarung sind oder im Zuge ihrer Durchführung anfallen und auf Weisung des Verantwortlichen verarbeitet werden. Nicht erfasst sind Daten von Mitarbeitenden des Auftragsverarbeiters, soweit sie ausschließlich dessen eigenes Beschäftigungsverhältnis betreffen.

Diese Vereinbarung geht anderen Abreden zwischen den Parteien zum selben Gegenstand vor, sofern nicht ausdrücklich etwas anderes vereinbart wird.

§ 2 Konkretisierung des Auftragsinhalts

Gegenstand, Art und Zweck der Verarbeitung ist die Bereitstellung der Shopify-App „EU Widerrufs-Button Pro" durch den Auftragsverarbeiter. Die App ermöglicht es dem Verantwortlichen, seinen Endkundinnen und Endkunden einen Widerrufs-Button und ein Widerrufsformular bereitzustellen sowie eingehende Widerrufserklärungen strukturiert zu empfangen, zu dokumentieren und per Bestätigungsmail zu beantworten. Die Dauer der Verarbeitung entspricht der Laufzeit der App-Installation bzw. des Nutzungsverhältnisses.

Folgende Arten personenbezogener Daten sind Gegenstand der Verarbeitung:

- Personenstammdaten (Vorname, Nachname, Kunden-ID)
- Kontaktdaten (E-Mail-Adresse, Liefer- und Rechnungsanschrift)
- Bestelldaten (Bestellnummer, Bestelldatum, widerrufene Artikel, Menge, Kaufpreis, Widerrufsdatum, Lieferbedingungen)
- Kommunikationsdaten (Inhalte aus dem Widerrufsformular, z. B. Widerrufsgrund und Freitext-Nachrichten)
- Nutzungsdaten (IP-Adresse, Zeitstempel der Formular- bzw. Button-Nutzung, User-Agent sowie technische Identifikatoren zur Absicherung des Formulars)

Kreis der betroffenen Personen:

- Endkundinnen und Endkunden (Käufer), die im Online-Shop des Verantwortlichen bestellt und den Widerrufsbutton zur Ausübung ihres gesetzlichen Widerrufsrechts genutzt haben.
- Interessenten / Shop-Besucher, die den Widerrufsbutton betätigen oder das Formular aufrufen, auch wenn der Vorgang nicht abgeschlossen wird (Erfassung von Nutzungsdaten / IP-Adresse).

Ansprechpartner des Verantwortlichen, deren Daten im Rahmen der Konfiguration und Verwaltung der App (Admin-Bereich) verarbeitet werden.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung.

Die verarbeiteten Daten weisen einen normalen Schutzbedarf auf.

§ 3 Verpflichtungen und Weisungsbefugnis

Beide Parteien halten die ihnen durch das Datenschutzrecht (insbesondere die DSGVO) auferlegten Pflichten ein.

Die Verarbeitung erfolgt ausschließlich im Rahmen der dokumentierten Weisungen des Verantwortlichen. Die im Hauptvertrag beschriebene Leistung der App gilt als grundlegende Weisung. Ergänzende oder abweichende Weisungen kann der Verantwortliche in dokumentierter Form (z. B. per E-Mail oder über die Benutzeroberfläche der App) erteilen. Weisungsberechtigt sind grundsätzlich nur Personen mit administrativen Zugriffsrechten auf den jeweiligen Shopify-Store oder ausdrücklich benannte Personen.

Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtlich unzulässig, informiert er den Verantwortlichen unverzüglich und darf die Durchführung bis zur Klärung aussetzen.

Die Verarbeitung findet grundsätzlich in der Europäischen Union (EU) bzw. dem Europäischen Wirtschaftsraum (EWR) statt. Der Verantwortliche erteilt die allgemeine Weisung, für die Cloud-Infrastruktur spezialisierte Subunternehmer einzusetzen (siehe Anlage 2). Soweit dabei eine Übermittlung in Drittländer erfolgt, stellt der Auftragsverarbeiter sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. durch EU-Standardvertragsklauseln oder Angemessenheitsbeschluss).

Eine Verarbeitung außerhalb der primären Betriebsstätten (z. B. mobiles Arbeiten) ist gestattet, sofern die vereinbarten technischen und organisatorischen Maßnahmen konsequent eingehalten werden, insbesondere Geräteverschlüsselung und Multi-Faktor-Authentisierung.

Der Auftragsverarbeiter unterstützt den Verantwortlichen angemessen bei der Erfüllung von Betroffenenrechten (z. B. Auskunft, Berichtigung, Löschung). Direkt an den Auftragsverarbeiter gerichtete Ersuchen werden unverzüglich an den Verantwortlichen weitergeleitet.

Der Auftragsverarbeiter führt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO.

§ 4 Gesetzliche Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter gewährleistet, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet wurden und über die strikte Weisungs- und Zweckbindung dieses Auftragsverhältnisses belehrt sind.

Er unterstützt den Verantwortlichen bei dessen Rechenschaftspflichten (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO) und stellt auf Anfrage Informationen zu den umgesetzten technischen und organisatorischen Maßnahmen bereit.

Da der Auftragsverarbeiter nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, benennt er die Geschäftsführung als zentralen Ansprechpartner. Anfragen sind an datenschutz@euwiderruf.com zu richten.

Er informiert den Verantwortlichen unverzüglich über Kontrollen oder Maßnahmen von Aufsichtsbehörden, soweit diese die Verarbeitung des Verantwortlichen betreffen.

§ 5 Technische und organisatorische Maßnahmen (TOM) und Kontrolle

Die Parteien vereinbaren die in Anlage 1 niedergelegten technischen und organisatorischen Maßnahmen. Der Auftragsverarbeiter gewährleistet die Einhaltung dieser Sicherheitsstandards gemäß Art. 32 DSGVO.

Die Maßnahmen unterliegen dem technischen Fortschritt. Dem Auftragsverarbeiter ist es gestattet, alternative adäquate Maßnahmen umzusetzen, sofern das Sicherheitsniveau der in Anlage 1 festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

Der Nachweis der Einhaltung kann insbesondere durch aktuelle Testate, Zertifikate oder Berichte der eingesetzten Cloud-Infrastruktur-Provider (z. B. ISO 27001, SOC 2) geführt werden.

Der Verantwortliche kann Überprüfungen durchführen oder durchführen lassen. Vor-Ort-Kontrollen sind mit angemessener Frist (mind. 14 Tage) anzukündigen, haben zu den üblichen Geschäftszeiten stattzufinden und dürfen den Betriebsablauf nicht unzumutbar stören.

Die Kosten einer Vor-Ort-Überprüfung trägt der Verantwortliche, es sei denn, die Überprüfung deckt schwerwiegende Verstöße des Auftragsverarbeiters auf.

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Bedarf bei einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) durch Bereitstellung notwendiger technischer Informationen über die Applikationsarchitektur.

§ 6 Meldepflichten bei Datenschutzverstößen

Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich (spätestens innerhalb von 48 Stunden nach Bekanntwerden), wenn Verletzungen des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO) festgestellt werden.

Die Mitteilung enthält mindestens: eine Beschreibung der Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Datensätze sowie die ergriffenen oder vorgeschlagenen Gegenmaßnahmen.

Der Auftragsverarbeiter unterstützt den Verantwortlichen angemessen bei dessen Meldepflichten gegenüber Aufsichtsbehörden (Art. 33 DSGVO) und betroffenen Personen (Art. 34 DSGVO).

Eigenständige Meldungen an Aufsichtsbehörden oder betroffene Personen erfolgen nur nach vorheriger Weisung des Verantwortlichen, es sei denn, der Auftragsverarbeiter ist gesetzlich unmittelbar zur Meldung verpflichtet.

§ 7 Löschung und Rückgabe von Daten

Sämtliche im Auftrag verarbeiteten Daten verbleiben im Eigentum des Verantwortlichen.

Während der aktiven Nutzung werden Widerrufs-Datensätze entsprechend dem vom Verantwortlichen gebuchten Tarif vorgehalten (Free: 3 Monate, Basic: 12 Monate, Premium: 24 Monate) und nach Ablauf dieser Frist automatisiert gelöscht.

Nach Beendigung der Leistungen (insbesondere durch Deinstallation der App) löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen sämtliche im Auftrag verarbeiteten Daten datenschutzgerecht oder gibt sie zurück, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Erfolgt vor der Deinstallation keine abweichende Weisung, werden die Daten automatisiert innerhalb von 30 Tagen nach Erhalt der Deinstallations- bzw. Lösch-Signale der Plattform (z. B. Shopify Mandatory Webhooks) vollständig gelöscht. Ein Löschprotokoll wird auf Anforderung in elektronischer Form bereitgestellt. Eine Rückgabe in einem gängigen, maschinenlesbaren Format (z. B. CSV) ist vor der Deinstallation möglich.

Der Verantwortliche ist für die Einhaltung eigener gesetzlicher Aufbewahrungsfristen (z. B. nach § 132 BAO bzw. § 257 HGB für steuerrelevante Widerrufs- oder Transaktionsdaten) selbst verantwortlich.

Test- und Ausschussmaterial (z. B. temporäre Logfiles oder Zwischenspeicherungen) wird nach Beendigung des jeweiligen Verarbeitungsschritts unverzüglich gelöscht, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

§ 8 Subunternehmen (Unterauftragsverarbeiter)

Der Auftragsverarbeiter erhält die allgemeine Genehmigung des Verantwortlichen zur Beauftragung von Subunternehmen. Die aktuell eingesetzten Subunternehmen sind in Anlage 2 aufgeführt.

Der Auftragsverarbeiter informiert den Verantwortlichen mindestens zwei Wochen im Voraus in Textform über beabsichtigte Änderungen dieser Liste. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund Einspruch erheben. Erfolgt kein Einspruch, gilt die Änderung als genehmigt.

Der Auftragsverarbeiter stellt sicher, dass die vertraglichen Vereinbarungen mit dem Subunternehmen dem Datenschutzniveau dieser Vereinbarung entsprechen (Art. 28 Abs. 3 und 4 DSGVO).

Erbringt ein Subunternehmer Leistungen außerhalb der EU / des EWR, stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch geeignete Garantien gemäß Art. 44 ff. DSGVO sicher.

Kommt ein Subunternehmen seinen Pflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für deren Einhaltung.

Nicht als Subunternehmen gelten reine Nebenleistungen (z. B. Telekommunikation, Post- und Logistikdienste) ohne Zugriffsmöglichkeit auf die Daten des Verantwortlichen.

§ 9 Kontrollrechte (Datenschutzkontrolle)

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der in dieser Vereinbarung und Art. 28 DSGVO genannten Pflichten zur Verfügung.

Der Verantwortliche kann nach rechtzeitiger Anmeldung (in der Regel mind. zwei Wochen im Voraus) Überprüfungen durchführen oder durch benannte Prüfer durchführen lassen. Der Auftragsverarbeiter ist berechtigt, externe Prüfer abzulehnen, die in einem Wettbewerbsverhältnis zu ihm stehen.

Da die Verarbeitung in einer Cloud-Infrastruktur erfolgt, erkennt der Verantwortliche an, dass der Nachweis angemessener Maßnahmen vorrangig durch Zertifikate, Testate oder Berichte der eingesetzten Subunternehmer sowie durch Eigenerklärungen geführt wird. Ein physisches Betretungsrecht besteht nur, soweit eine Fernprüfung nachweislich nicht ausreicht.

§ 10 Haftung und Schadenersatz

Die Parteien haften für Schäden nach Maßgabe des Art. 82 DSGVO.

Im Verhältnis der Parteien zueinander ist die Haftung des Auftragsverarbeiters für leicht fahrlässig verursachte Schäden auf den Betrag begrenzt, den der Verantwortliche innerhalb der letzten 12 Monate vor Eintritt des Schadensereignisses als Entgelt für die Nutzung der App entrichtet hat. Diese Begrenzung gilt nicht für Schäden aus grob fahrlässiger oder vorsätzlicher Pflichtverletzung.

Die Haftungsverteilung nach Art. 82 Abs. 3 DSGVO bleibt unberührt. Der Auftragsverarbeiter haftet im Innenverhältnis insbesondere dann nicht, wenn der Schaden durch eine fehlerhafte Weisung oder unzureichende Mitwirkung des Verantwortlichen entstanden ist.

§ 11 Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform (z. B. E-Mail oder elektronische Bestätigung im App-Interface) und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung dieser Bedingungen handelt.

Sollten einzelne Regelungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Regelungen unberührt. Die Parteien ersetzen die unwirksame Regelung durch eine wirksame, die dem wirtschaftlichen Zweck am nächsten kommt.

Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen des internationalen Privatrechts und des UN-Kaufrechts. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragsverarbeiters (Wien).

Abschluss der Vereinbarung

Diese Vereinbarung wird vom Verantwortlichen im Rahmen der App-Installation durch elektronische Bestätigung (Opt-In) akzeptiert. Sie ist gemäß Art. 28 Abs. 9 DSGVO auch ohne handschriftliche Unterschrift rechtsgültig. Für den Auftragsverarbeiter handelt Martini & Radl OG,

vertreten durch die Geschäftsführung.

Anlage 1: Technische und organisatorische Maßnahmen (TOMs)

Diese Anlage konkretisiert die gemäß § 5 getroffenen Sicherheitsmaßnahmen (Art. 32 DSGVO).

Der Auftragsverarbeiter betreibt keine eigenen Rechenzentren. Die Verarbeitung erfolgt über moderne Cloud-Infrastruktur; der Auftragsverarbeiter kombiniert eigene organisatorische Maßnahmen mit den Sicherheitsstandards der eingesetzten Subunternehmer (siehe Anlage 2).

1. Vertraulichkeit

Zutrittskontrolle. Die physische Sicherheit der Server wird durch die zertifizierten Provider gewährleistet (ISO 27001, SOC 2 Type II).

Zugangskontrolle.

- Administrative Zugänge zu geschäftskritischen Cloud-Plattformen sind zwingend durch Multi-Faktor-Authentisierung (TOTP) abgesichert.
- Einsatz eines Passwort-Managers zur verschlüsselten Verwaltung von Zugangsdaten.
- Vollständige Festplattenverschlüsselung auf allen Arbeitsgeräten.

Zugriffskontrolle.

- Zugriff auf Cloud-Konsole und Datenbank ausschließlich über MFA-geschützte Konten.
- Anwendungsseitige Zugriffe über sicher verwaltete Umgebungsvariablen (Secrets), nicht im Klartext im Quellcode.
- Berechtigungsvergabe nach dem Need-to-know-Prinzip; individuelle Benutzerkonten, keine Shared Accounts.

Trennungskontrolle. Mandantentrennung über eine Multi-Tenant-Architektur: Daten werden auf Datenbankebene über eindeutige Mandanten-Identifikatoren (Shop-IDs) logisch strikt getrennt. Entwicklungs- (Dev), Test- (Staging) und Produktionsumgebung (Prod) sind getrennt; in Dev/Test werden grundsätzlich keine Echtdaten verwendet.

2. Integrität

Übertragungskontrolle.

- Jegliche Datenübertragung zwischen Endgerät, Shopify-API und App-Servern erfolgt verschlüsselt (mind. TLS 1.2, bevorzugt TLS 1.3).
- Unverschlüsselte Anfragen werden automatisch auf HTTPS umgeleitet (HSTS).

Auch die interne Kommunikation zwischen den Cloud-Diensten erfolgt verschlüsselt.

E-Mail-Adressen und IP-Adressen werden, soweit nicht für den Versand benötigt, pseudonymisiert (Hash-Verfahren) gespeichert.

Eingabekontrolle.

Sämtliche Änderungen am Quellcode werden lückenlos versioniert; jeder Commit ist einem autorisierten Entwickler zugeordnet.

Jede Bereitstellung (Deployment) wird mit Zeitstempel protokolliert.

Kritische administrative Zugriffe auf die Datenbank werden providerseitig protokolliert.

3. Verfügbarkeit und Belastbarkeit

Nutzung skalierbarer Cloud-Infrastruktur mit Multi-Availability-Zone-Architektur zum Schutz gegen punktuelle Ausfälle.

Cloud-native Schutzmechanismen (WAF) zur Abwehr von Angriffen auf die Verfügbarkeit.

Vollautomatisierte tägliche Backups mit einer Aufbewahrungsfrist von mindestens 30 Tagen; regelmäßige Verifikation der Wiederherstellungsprozesse.

4. Verfahren zur regelmäßigen Überprüfung

Integration automatisierter Sicherheits-Audits in die CI-Pipeline; Builds mit kritischen Schwachstellen in Abhängigkeiten werden blockiert.

Automatisierte Test-Suiten zur Sicherstellung der Code-Integrität vor jedem Release.

Sorgfältige Auswahl und regelmäßige Prüfung von Subunternehmern (Zertifizierungen ISO 27001, SOC 2) sowie Abschluss entsprechender AVV und geeigneter Garantien bei Drittland-Transfers.

Führung eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO), mindestens jährliche Prüfung; regelmäßige Sensibilisierung aller Beteiligten.

Anlage 2: Genehmigte Unterauftragsverarbeiter (Subunternehmen)

Gemäß § 8 genehmigt der Verantwortliche die Beauftragung der nachfolgend aufgeführten Unterauftragsverarbeiter. Mit diesen Dienstleistern bestehen Vereinbarungen gemäß Art. 28 Abs. 2 bis 4 DSGVO. Sofern Daten in Drittstaaten übermittelt werden, erfolgt dies auf Grundlage geeigneter Garantien gemäß Art. 44 ff. DSGVO (insbesondere EU-U.S. Data Privacy Framework oder EU-Standardvertragsklauseln).

DIENSTLEISTER	SITZ	LEISTUNG / ZWECK	VERARBEITUNGSORT
Shopify International Ltd.	2nd Floor Victoria Buildings, 1-2 Haddington Road, Dublin 4, Irland	E-Commerce-Plattform, App-Laufzeit & API-Schnittstelle	EU (Irland) / global
Railway Corp.	548 Market St, San Francisco, CA 94104, USA	Application-Hosting & Datenbank (PostgreSQL)	EU-Region; SCC bei Drittlandbezug
Resend, Inc.	2261 Market St #4008, San Francisco, CA 94114, USA	Versand der Bestätigungs-Mails	USA — SCC / EU-U.S. DPF

HINWEIS: DIESE LISTE KANN SICH ÄNDERN. DER VERANTWORTLICHE WIRD BEI BEABSICHTIGTEN ÄNDERUNGEN GEMÄSS § 8 (2) RECHTZEITIG INFORMIERT.

EINE PDF-KOPIE DIESER VEREINBARUNG SENDEN WIR AUF ANFRAGE AN DATENSCHUTZ@EUWIDERRUF.COM. STAND: 1. JUNI 2026.