

Auftragsverarbeitungsvertrag (AVV)

nach Art. 28 DSGVO · Shopify-App „Raum Visualisierer“ · Stand: 19. Oktober 2026

Vertragsparteien und Präambel

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DSGVO, wenn ein Händler die App „Raum Visualisierer“ in seinem Shopify-Shop nutzt.

Verantwortlicher (im Folgenden „Auftraggeber“)

Firma: _____
Anschrift: _____
Shop-Domain (*.myshopify.com): _____
Vertreten durch: _____

Auftragsverarbeiter (im Folgenden „Auftragnehmer“)

Roots Organics GmbH, Georg-Wulf-Str. 15, 28199 Bremen, Deutschland
Amtsgericht Bremen, HRB 31278 HB, USt-IdNr. DE306263479
Vertreten durch die Geschäftsführerin Asli Bektas
Kontakt Datenschutz: anfragen@raumvisualisierer.de

Präambel

Der Auftragnehmer stellt dem Auftraggeber die Shopify-App „Raum Visualisierer“ bereit (im Folgenden „Hauptvertrag“: die Nutzung der App mit dem über Shopify gewählten Plan). Kunden des Auftraggebers sehen damit Teppiche in Beispielsräumen oder in einem Foto ihres eigenen Raums und lassen sich dazu Kennzahlen im Shopify-Admin anzeigen. Soweit der Auftragnehmer dabei personenbezogene Daten im Auftrag des Auftraggebers verarbeitet, gilt dieser Vertrag. Er geht bei Widersprüchen zum Datenschutz den Regelungen des Hauptvertrags vor.

§ 1 Gegenstand, Dauer, Art und Zweck der Verarbeitung

- Gegenstand:** Bereitstellung der Raumansicht im Shop des Auftraggebers, Analyse von Raumfotos seiner Kunden und Zählung der Nutzung für die Analyseseite im Shopify-Admin.
- Dauer:** Der Vertrag gilt, solange der Auftraggeber die App installiert hat. Er endet mit der Deinstallation; § 6 (Löschung) gilt darüber hinaus.
- Art und Zweck der Verarbeitung:**

Verarbeitung	Zweck	Daten	Speicherdauer
Analyse eigener Raumfotos	Boden, Möbel und Maßstab erkennen, Teppich im Foto zeigen	Raumfoto (kann zufällig Personen, Gegenstände oder Hinweise auf Wohnverhältnisse zeigen)	nur im Arbeitsspeicher während der Analyse; bei Übergabe per QR-Code höchstens 10 Minuten
Nutzungszählung	Kennzahlen für den Auftraggeber (angesehene Teppiche, Warenkorb, Räume)	zufällige Besucher- und Besuchskennung, Ereignisname, Zeitpunkt, Raum, Produkt-Handle, Geräteart (Smartphone ja/nein)	400 Tage, danach automatische Löschung

Verarbeitung	Zweck	Daten	Speicherdauer
Begrenzung von Missbrauch	Zahl der Fotoanalysen je Besucher und Tag begrenzen	IP-Adresse	nur im Arbeitsspeicher, höchstens bis Tagesende
Betriebs- und Sicherheitsprotokolle	Fehlersuche, Abwehr von Angriffen	IP-Adresse, Zeitpunkt, aufgerufene Adresse, Browserkennung	30 Tage

1. **Kategorien betroffener Personen:** Besucher und Kunden des Shops des Auftraggebers, die die Raumansicht nutzen; gegebenenfalls Personen, die auf hochgeladenen Raumfotos zu sehen sind.
2. **Keine besonderen Kategorien:** Eine Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) ist nicht vorgesehen. Der Auftragnehmer wertet Fotos nicht auf Personen aus.
3. **Nicht verarbeitet** werden Namen, E-Mail-Adressen, Bestellungen, Zahlungsdaten und Shopify-Kundennummern der Kunden.
4. **Ort der Verarbeitung:** ausschließlich in der Europäischen Union (Rechenzentrum Belgien, Region europe-west1). Eine Verlagerung in ein Drittland erfolgt nur nach § 4.

§ 2 Weisungsbefugnis des Auftraggebers

1. Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, auch hinsichtlich der Übermittlung in ein Drittland (Art. 28 Abs. 3 lit. a DSGVO). Die Weisungen sind abschließend in diesem Vertrag, im Hauptvertrag und in den Einstellungen festgelegt, die der Auftraggeber in der App wählt (zum Beispiel Plan, angezeigte Produkte, Installation und Deinstallation).
2. Ausnahme: Ist der Auftragnehmer nach Unionsrecht oder dem Recht eines Mitgliedstaats zu einer Verarbeitung verpflichtet, teilt er dies dem Auftraggeber vorab mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.
3. Weitere Weisungen erteilt der Auftraggeber in Textform (E-Mail an anfragen@raumvisualisierer.de). Mündliche Weisungen bestätigt er unverzüglich in Textform. Weisungsberechtigt ist, wer den Shop im Shopify-Admin verwaltet oder vom Auftraggeber benannt ist.
4. Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, informiert er den Auftraggeber unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). Er darf die Ausführung aussetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.
5. Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, behandeln die Parteien als Änderungswunsch; ein angemessener Mehraufwand kann gesondert vereinbart werden.

§ 3 Pflichten des Auftragnehmers

1. **Vertraulichkeit:** Der Auftragnehmer setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen, und die mit den Datenschutzvorschriften vertraut gemacht wurden (Art. 28 Abs. 3 lit. b, Art. 29 DSGVO). Die Verpflichtung gilt über das Ende der Tätigkeit hinaus.
2. **Sicherheit:** Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt; wesentliche Änderungen dokumentiert er und teilt sie auf Anfrage mit.
3. **Unterstützung bei Betroffenenrechten:** Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten Maßnahmen bei Anfragen betroffener Personen nach Art. 12 bis 22 DSGVO (Art. 28 Abs. 3

lit. e DSGVO). Anfragen, die direkt beim Auftragnehmer eingehen, leitet er unverzüglich an den Auftraggeber weiter. Hinweis: Da keine Namen oder Kundennummern gespeichert werden, lässt sich eine Anfrage in der Regel keinem Datensatz zuordnen.

4. **Unterstützung bei Art. 32 bis 36 DSGVO:** Der Auftragnehmer unterstützt den Auftraggeber bei der Sicherheit der Verarbeitung, bei Meldungen von Datenschutzverletzungen, bei einer Datenschutz-Folgenabschätzung und einer vorherigen Konsultation der Aufsichtsbehörde, soweit die ihm vorliegenden Informationen reichen (Art. 28 Abs. 3 lit. f DSGVO).
5. **Meldung von Verletzungen:** Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, an die im Shopify-Konto hinterlegte E-Mail-Adresse des Shops. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung, Kategorien und ungefähre Zahl der Betroffenen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen und eine Kontaktstelle. Die Meldung an die Aufsichtsbehörde und an Betroffene bleibt Aufgabe des Auftraggebers.
6. **Verzeichnis:** Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.
7. **Datenschutzbeauftragter:** Ist der Auftragnehmer gesetzlich zur Benennung verpflichtet (Art. 37 DSGVO, § 38 BDSG), teilt er dem Auftraggeber dessen Kontaktdaten mit. Derzeit ist kein Datenschutzbeauftragter benannt; Ansprechpartner ist anfragen@raumvisualisierer.de.
8. **Zweckbindung:** Der Auftragnehmer verwendet die Daten nicht für eigene Zwecke, verkauft sie nicht, nutzt sie nicht für Werbung und führt sie nicht shopübergreifend zusammen. Kopien oder Duplikate entstehen nur, soweit sie für den Betrieb (zum Beispiel Datensicherungen) nötig sind.
9. **Behördliche Maßnahmen:** Über Kontrollen oder Maßnahmen einer Aufsichtsbehörde, die diese Verarbeitung betreffen, informiert der Auftragnehmer den Auftraggeber unverzüglich.

§ 4 Unterauftragsverarbeiter und Drittlandübermittlung

1. Der Auftraggeber erteilt eine allgemeine Genehmigung für den Einsatz weiterer Auftragsverarbeiter (Art. 28 Abs. 2 DSGVO). Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter stehen in Anlage 2 und gelten als genehmigt.
2. Über jede beabsichtigte Hinzuziehung oder Ersetzung informiert der Auftragnehmer den Auftraggeber mindestens 30 Tage vorher per E-Mail. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Finden die Parteien keine Lösung, kann der Auftraggeber die App ohne weitere Kosten deinstallieren und den Hauptvertrag zum Zeitpunkt der Änderung beenden.
3. Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich zu denselben Datenschutzpflichten wie in diesem Vertrag, insbesondere zu hinreichenden Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Er haftet gegenüber dem Auftraggeber für die Einhaltung dieser Pflichten durch den Unterauftragsverarbeiter.
4. Keine Unteraufträge sind Nebenleistungen, bei denen der Dienstleister keinen Zugriff auf die Daten hat, etwa Telekommunikation oder Postdienste. Die Shopify-Plattform selbst ist kein Unterauftragsverarbeiter des Auftragnehmers; sie ist Dienstleister des Auftraggebers.
5. **Drittlandübermittlung:** Daten werden nur in einem Land außerhalb des Europäischen Wirtschaftsraums verarbeitet oder dorthin übermittelt, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, etwa ein Angemessenheitsbeschluss (zum Beispiel das EU-US Data Privacy Framework für zertifizierte Unternehmen) oder die Standardvertragsklauseln der EU-Kommission mit ergänzenden Maßnahmen. Die Speicherung der Daten erfolgt in der EU (Belgien).

§ 5 Kontrollrechte und Nachweise

1. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO). Als Nachweis dienen insbesondere diese Vereinbarung mit Anlage 1, aktuelle Nachweise der Unterauftragsverarbeiter (zum Beispiel ISO/IEC 27001, SOC 2 von Google Cloud) und schriftliche Auskünfte.
2. Der Auftraggeber kann Überprüfungen einschließlich Inspektionen selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen. Sie werden mindestens 14 Tage vorher angekündigt, finden zu Geschäftszeiten statt und stören den Betrieb nicht unverhältnismäßig. Prüfer, die mit dem Auftragnehmer im Wettbewerb stehen, können abgelehnt werden.
3. Eine Vor-Ort-Prüfung in Rechenzentren von Unterauftragsverarbeitern ersetzen deren Zertifikate und Prüfberichte.
4. Der Aufwand für Überprüfungen trägt jede Partei selbst. Übersteigt der Aufwand des Auftragnehmers einen Arbeitstag im Kalenderjahr, kann er eine angemessene Vergütung verlangen, außer die Prüfung deckt einen Verstoß des Auftragnehmers auf.

§ 6 Löschung, Haftung, Laufzeit und Schlussbestimmungen

1. **Löschung und Rückgabe:** Nach Ende der Leistungen löscht der Auftragnehmer alle personenbezogenen Daten des Auftraggebers (Art. 28 Abs. 3 lit. g DSGVO). Die Löschung erfolgt automatisch, sobald Shopify nach der Deinstallation die Löschanforderung „shop/redact“ sendet (in der Regel 48 Stunden nach der Deinstallation). Datensicherungen der Datenbank werden spätestens nach 7 Tagen überschrieben. Vor der Löschung kann der Auftraggeber in Textform eine Kopie der Nutzungszählungen in einem gängigen Format (CSV) verlangen. Eine Pflicht zur Aufbewahrung nach Unionsrecht oder dem Recht eines Mitgliedstaats bleibt unberührt.
2. **Haftung:** Die Haftung richtet sich nach Art. 82 DSGVO. Im Innenverhältnis haftet jede Partei für Schäden, die auf ihrem eigenen Verstoß beruhen. Im Übrigen gelten die Haftungsregeln des Hauptvertrags.
3. **Laufzeit und Kündigung:** Der Vertrag beginnt mit der Installation der App oder mit Unterzeichnung, wenn diese später erfolgt, und endet mit der Beendigung des Hauptvertrags. Das Recht zur außerordentlichen Kündigung bei einem schwerwiegenden Verstoß gegen diesen Vertrag oder das Datenschutzrecht bleibt unberührt.
4. **Form:** Änderungen und Ergänzungen bedürfen der Textform; der Vertrag kann elektronisch geschlossen werden (Art. 28 Abs. 9 DSGVO).
5. **Salvatorische Klausel:** Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung, die dem Zweck am nächsten kommt.
6. **Rangfolge:** Bei Widersprüchen gilt diese Vereinbarung vor dem Hauptvertrag; Standardvertragsklauseln, soweit vereinbart, gelten vor dieser Vereinbarung.
7. **Recht und Gerichtsstand:** Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Bremen, soweit der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

Unterschriften

	Auftraggeber	Auftragnehmer
Ort, Datum		Bremen,
Name, Funktion		Asli Bektas, Geschäftsführerin
Unterschrift		

Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Die Dienste laufen vollständig auf Google Cloud in der Region europe-west1 (Belgien). Physische Sicherheit, Netz und Hardware stellt Google Cloud nach seinen zertifizierten Standards (unter anderem ISO/IEC 27001, 27017, 27018, SOC 2).

Bereich	Maßnahmen
Vertraulichkeit: Zutritt	Kein eigenes Rechenzentrum; Zutrittskontrolle der Google-Rechenzentren (Ausweis, Videoüberwachung, Sicherheitspersonal)
Vertraulichkeit: Zugang	Verwaltung nur über persönliche Google-Konten der berechtigten Mitarbeitenden mit Zwei-Faktor-Authentifizierung; keine geteilten Konten; Server ohne Anmeldung per SSH (verwaltete Dienste Cloud Run, Cloud SQL)
Vertraulichkeit: Zugriff	Rollen nach dem Prinzip der geringsten Rechte (IAM); Dienste laufen mit einem eigenen Dienstkonto; Zugangsdaten (Shopify-Schlüssel, Datenbank-Passwort, Signaturschlüssel) liegen verschlüsselt im Secret Manager, nicht im Quellcode
Vertraulichkeit: Trennung	Daten jedes Shops sind über die Shop-Domain getrennt; Abfragen erfolgen stets nur für den angemeldeten Shop; Entwicklungs- und Produktivsystem sind getrennt
Pseudonymisierung und Datensparsamkeit	Nutzungszählung nur mit zufälligen Kennungen; keine Namen, E-Mail-Adressen oder Bestellungen; Raumfotos werden nicht gespeichert; IP-Adressen nur im Arbeitsspeicher für Tageslimits
Integrität: Weitergabe	Alle Verbindungen ausschließlich verschlüsselt (HTTPS/TLS); Anfragen über den App-Proxy und Webhooks werden mit Shopifys HMAC-Signatur geprüft; der Analysedienst nimmt nur Anfragen mit einem signierten, befristeten Pass an
Integrität: Eingabe	Eingehende Ereignisse werden gegen eine feste Liste geprüft und begrenzt (höchstens 50 je Anfrage, 20.000 je Shop und Stunde); Protokollierung von Zugriffen in Cloud Logging (30 Tage)
Verfügbarkeit und Belastbarkeit	Verwaltete Dienste mit automatischem Neustart; Daten im Ruhezustand von Google verschlüsselt; automatische Datenbanksicherungen; Begrenzung von Warteschlange und Anfragen gegen Überlastung
Wiederherstellbarkeit	Wiederherstellung der Datenbank aus Sicherungen; Neuaufbau der Dienste aus dem Quellcode per Skript
Überprüfung und Bewertung	Datenschutz-Management mit jährlicher Überprüfung dieser Maßnahmen; Vorgehen bei Datenschutzverletzungen mit Meldung binnen 24 Stunden (§ 3 Abs. 5); datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)
Auftragskontrolle	Unterauftragsverarbeiter nur nach § 4 und Anlage 2, mit Vertrag nach Art. 28 DSGVO
Organisation	Verpflichtung der Mitarbeitenden auf Vertraulichkeit; Zugriff nur für namentlich festgelegte Personen; Schulung zum Datenschutz

Anlage 2: Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Garantien
Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Irland	Hosting der App und des Analysedienstes (Cloud Run), Datenbank (Cloud SQL), Schlüsselverwaltung (Secret Manager), Protokolle (Cloud Logging)	EU, Region europe-west1 (Belgien)	Cloud Data Processing Addendum von Google nach Art. 28 DSGVO; für mögliche Zugriffe verbundener Unternehmen außerhalb der EU (zum Beispiel Google LLC, USA, für Support und Sicherheit) EU-US Data Privacy Framework und Standardvertragsklauseln