

Auftragsverarbeitungsvertrag

AVV nach Art. 28 DSGVO zwischen Online-Shop-Betreiber (Verantwortlicher)
und dem SaaS-Provider (Auftragsverarbeiter)

1. Präambel, Parteien, Gegenstand und Laufzeit

Dieser Auftragsverarbeitungsvertrag (AVV) regelt die Rechte und Pflichten von

[Name Online-Shop-Betreiber],

[Anschrift]

("Verantwortlicher")

und

OIDO order & pay systems S.L., NIF B72461288, Avda. Comte Güell, 12, 08871 Sitges, Spanien

("Auftragsverarbeiter")

bei der Verarbeitung personenbezogener Daten im Zusammenhang mit der Nutzung der Online-Shop-Software **OIDO Online-Shop** durch den Verantwortlichen. Er konkretisiert die datenschutzrechtlichen Pflichten aus Art. 28 DSGVO und ist Bestandteil des zugrunde liegenden Hauptvertrags (SaaS-/Lizenzvertrag vom [Datum]).

Gegenstand der Verarbeitung ist das Hosting, der Betrieb und die Speicherung der Shop-, Bestell-, Zahlungs- und Kundendaten des Verantwortlichen in der vom Auftragsverarbeiter betriebenen SaaS-Plattform, einschließlich der Protokollierung buchhaltungs- und steuerrelevanter Finanzdaten (z. B. Rechnungen, Zahlungsbelege, Bestellhistorien).

Laufzeit: Dieser AVV gilt für die Dauer des Hauptvertrags. Für Daten, die einer gesetzlichen Aufbewahrungspflicht unterliegen (§ 257 HGB, § 147 AO), gelten die gesonderten Regelungen zu Nr. 6 (Datenrückgabe/-löschung) auch nach Beendigung des Hauptvertrags fort.

2. Art, Zweck, betroffene Personen und Datenarten

Zweck: Bereitstellung und Betrieb der Online-Shop-Software als SaaS, einschließlich Zahlungsabwicklung, Bestellverwaltung, Rechnungsstellung und revisionssicherer Archivierung.

Kategorie betroffener Personen	Kategorien der Daten
Kunden des Online-Shops	Name, Anschrift, E-Mail, Telefon, Zahlungsdaten, Bestellhistorie
Mitarbeiter des Verantwortlichen	Zugangsdaten, Nutzerprotokolle (Logins)
Zahlungsdienstleister-Kontakte	Transaktions-IDs, Zahlungsstatus

Finanzrelevante Daten (Rechnungen, Zahlungsbelege, Auftragsbestätigungen) werden zusätzlich zu den handels-/steuerrechtlichen Zwecken des Verantwortlichen (§ 257 HGB, § 147 AO) verarbeitet und gespeichert.

3. Pflichten des Auftragsverarbeiters (Art. 28 Abs. 3 DSGVO)

Der Auftragsverarbeiter verpflichtet sich:

1. Die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen zu verarbeiten (Art. 28 Abs. 3 lit. a DSGVO), einschließlich Übermittlungen in Drittländer.
2. Sicherzustellen, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind (lit. b).
3. Alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (TOM) zu treffen, insbesondere: Verschlüsselung, Zugriffskontrolle, Protokollierung, Unveränderbarkeit steuerrelevanter Daten (GoBD-Konformität), Verfahrensdokumentation sowie regelmäßige Datensicherung (lit. c). Details siehe **Anlage 1 – TOM**.
4. Die Bedingungen für die Hinzuziehung weiterer Auftragsverarbeiter gemäß Nr. 4 einzuhalten (lit. d).
5. Den Verantwortlichen bei der Erfüllung von Betroffenenrechten (Art. 12–22 DSGVO) durch geeignete technische und organisatorische Maßnahmen zu unterstützen (lit. e).
6. Bei der Einhaltung der Pflichten nach Art. 32–36 DSGVO zu unterstützen (lit. f).
7. Nach Wahl des Verantwortlichen alle Daten nach Ende der Erbringung der Dienstleistungen zu löschen oder zurückzugeben, vorbehaltlich gesetzlicher Aufbewahrungspflichten (lit. g, siehe Nr. 6).
8. Dem Verantwortlichen alle zum Nachweis der Einhaltung dieser Pflichten erforderlichen Informationen zur Verfügung zu stellen und Prüfungen/Inspektionen zu ermöglichen (lit. h, siehe Nr. 5).

4. Unterauftragsverarbeitung, Speicherort und Drittlandtransfer

Unterauftragsverarbeiter: Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (z. B. Hosting-, Zahlungs- oder Backup-Dienstleister) nur mit vorheriger allgemeiner oder spezifischer Genehmigung des Verantwortlichen einsetzen. Die aktuell eingesetzten Unterauftragsverarbeiter sind in **Anlage 2** aufgeführt; Änderungen werden mit angemessener Frist (mind. 30 Tage) vorab mitgeteilt; der Verantwortliche kann widersprechen.

Speicherort: Die Verarbeitung erfolgt in Rechenzentren in **Frankfurt am Main, Deutschland**. Bei Verlagerung in einen anderen EU-/EWR-Staat teilt der Auftragsverarbeiter dem Verantwortlichen den neuen Standort unverzüglich mit, damit dieser seiner Mitteilungspflicht nach § 146 Abs. 2a AO gegenüber dem Finanzamt nachkommen kann. Eine Verlagerung in Drittstaaten außerhalb der EU/des EWR bedarf der vorherigen Zustimmung des Verantwortlichen und setzt voraus, dass (a) geeignete Garantien nach Art. 44 ff. DSGVO (z. B. EU-Standardvertragsklauseln) sowie (b) der uneingeschränkte, jederzeitige elektronische Datenzugriff der zuständigen Finanzbehörden (Z1/Z2/Z3-Zugriff nach § 147 Abs. 6 AO, GoBD) sichergestellt sind.

Der Auftragsverarbeiter gewährleistet in jedem Fall, dass steuerlich relevante Daten unveränderbar, vollständig und maschinell auswertbar für die Dauer der jeweils anwendbaren gesetzlichen Aufbewahrungsfrist gespeichert bleiben.

5. Kontrollrechte, Unterstützung, Meldung von Datenschutzverletzungen

Kontrollrechte: Der Verantwortliche ist berechtigt, die Einhaltung dieses AVV vor Vertragsbeginn und danach in angemessenen Abständen auf eigene Kosten zu überprüfen, z. B. durch Anforderung von Prüfberichten oder durch Vor-Ort-Audits mit angemessener Vorankündigung (mind. 14 Tage).

Unterstützungspflichten: Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Anfragen betroffener Personen (Auskunft, Berichtigung, Löschung, Datenübertragbarkeit) sowie bei Datenschutz-Folgenabschätzungen und Konsultationen der Aufsichtsbehörde.

Meldepflicht bei Datenschutzverletzungen: Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich nach Kenntnisnahme, mit allen für die Meldung nach Art. 33 DSGVO erforderlichen Angaben.

6. Datenrückgabe/-löschung bei Vertragsende, Haftung, Schlussbestimmungen

Bei Beendigung des Hauptvertrags stellt der Auftragsverarbeiter dem Verantwortlichen innerhalb von **30 Tagen** einen vollständigen, maschinell auswertbaren Export aller Daten (inkl. steuerlich relevanter Belege und Verfahrensdokumentation, GoBD-konform) zur Verfügung.

Soweit Daten einer gesetzlichen Aufbewahrungsfrist unterliegen (z. B. § 257 HGB, § 147 AO: 6/8/10 Jahre), speichert der Auftragsverarbeiter diese Daten nach Wahl des Verantwortlichen entweder (a) für eine zusätzliche, gesondert zu vergütende Übergangsfrist von **90 Tagen** zur Datenmitnahme weiter, oder (b) löscht sie unmittelbar nach erfolgreichem Export. Nach Ablauf der vereinbarten Übergangsfrist werden alle Daten unwiderruflich gelöscht, sofern keine anderslautende gesetzliche Pflicht oder Vereinbarung besteht. Die Verantwortung für die fristgerechte Sicherung eigener Aufbewahrungspflichten verbleibt beim Verantwortlichen.

Haftung: Es gilt die gesetzliche Haftungsregelung nach Art. 82 DSGVO; im Innenverhältnis haftet jede Partei für von ihr verursachte Schäden.

Schlussbestimmungen: Änderungen bedürfen der Textform. Es gilt spanisches Recht. Gerichtsstand ist der Sitz des **Auftragsverarbeiters**, soweit gesetzlich zulässig.

Anlagen 1 (TOM) und 2 (Unterauftragsverarbeiter) sind Bestandteil dieses AVV.

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

- **Zutrittskontrolle:** Rechenzentrum in Frankfurt am Main, betrieben von Google Cloud, mit Zutrittskontrolle, Besucherprotokoll und Videoüberwachung (Verantwortung des Rechenzentrumsbetreibers); der Auftragsverarbeiter betreibt als virtuelle Organisation keine eigenen Büro- oder Serverräume.
- **Zugangskontrolle:** Individuelle Benutzerkonten, Firebase Authentication, starke Passworrichtlinie, Zwei-Faktor-Authentifizierung für Administratoren und Google-Cloud-Konten, Sperrung nach Fehlversuchen; personenbezogene Daten werden ausschließlich in der Cloud-Infrastruktur von Google Cloud verarbeitet und nicht an lokalen Standorten gespeichert. Der Zugriff der Mitarbeiter erfolgt remote über VPN; alle Arbeitsgeräte sind durch biometrische Authentifizierung und Passwort geschützt.
- **Zugriffskontrolle:** Rollen- und Berechtigungskonzept nach dem Need-to-know-Prinzip (Google Cloud IAM, Firebase Security Rules), Protokollierung von Administratorzugriffen (Audit-Logs), regelmäßige Überprüfung der Berechtigungen.

- **Trennungskontrolle:** Mandantentrennung: Daten jedes Shop-Betreibers werden logisch getrennt verarbeitet; Trennung von Entwicklungs-, Test- und Produktivsystemen.
- **Verschlüsselung / Pseudonymisierung:** TLS-Verschlüsselung bei der Übertragung; Verschlüsselung gespeicherter Daten und Backups; Pseudonymisierung bei Supportzugriffen, wo möglich.
- **Weitergabekontrolle:** Verschlüsselte Schnittstellen (API/HTTPS), Dokumentation der Empfänger und Übermittlungswege.
- **Eingabekontrolle / Unveränderbarkeit:** Revisionssichere, unveränderbare Archivierung steuerrelevanter Belege (GoBD) mit Verfahrensdokumentation.
- **Verfügbarkeit und Belastbarkeit:** Regelmäßige Backups auf redundanter Infrastruktur von Google Cloud, Updates und Patch-Management.
- **Auftragskontrolle:** Sorgfältige Auswahl und Überprüfung der Unterauftragsverarbeiter (Anlage 2), Verträge nach Art. 28 DSGVO, Verpflichtung der Mitarbeiter auf Vertraulichkeit.
- **Löschung und Rückgabe:** Dokumentiertes Löschkonzept mit Fristen, sichere Löschung von Daten, Datenexport bei Vertragsende gemäß Nr. 6.
- **Überprüfung und Bewertung:** Für die Infrastruktur nutzt der Auftragsverarbeiter die Zertifizierungen von Google Cloud.

Anlage 2 – Genehmigte Unterauftragsverarbeiter

Der Verantwortliche genehmigt mit Abschluss dieses AVV die folgenden Unterauftragsverarbeiter. Änderungen richten sich nach Nr. 4 (Vorabmitteilung mit mindestens 30 Tagen, Widerspruchsrecht).

1. Google Cloud EMEA Limited, Dublin, Irland

- **Leistung:** Hosting und Backend-Dienste der SaaS-Plattform (Google Cloud, Firebase), einschließlich Datenbank, Speicher und Backups
- **Verarbeitete Daten:** Alle Shop-, Bestell- und Kundendaten
- **Verarbeitungsort:** Frankfurt am Main, Deutschland (Region europe-west3); einzelne Firebase-Dienste können Daten außerhalb der gewählten Region verarbeiten
- **Drittlandtransfer / Garantie:** Auftragsverarbeitungsvertrag von Google; bei Verarbeitung außerhalb des EWR (insbesondere USA) Standardvertragsklauseln der EU-Kommission (Bestandteil der Google-Datenverarbeitungsvereinbarung) sowie EU-US Data Privacy Framework (Zertifizierung von Google LLC)

2. Stripe Payments Europe, Limited, Dublin, Irland

- **Leistung:** Zahlungsabwicklung über Stripe Connect (Shopbetreiber als Connected Account)
- **Verarbeitete Daten:** Zahlungsdaten, Transaktions-IDs, Zahlungsstatus
- **Verarbeitungsort:** EU/EWR
- **Drittlandtransfer / Garantie:** Stripe-Datenverarbeitungsvereinbarung und Stripe Connected Account Agreement; Stripe handelt teils als eigenständig Verantwortlicher

3. Sendinblue SAS (heute Brevo), 9-17, rue Salneuve 75017 Paris, Frankreich

- **Leistung:** Versand von Bestell- und Systemmails
- **Verarbeitete Daten:** Name, E-Mail-Adresse, Bestellinhalte
- **Verarbeitungsort:** EU/EWR
- **Drittlandtransfer / Garantie:** Nein; bei Einsatz von Unterauftragsverarbeitern in Drittländern Standardvertragsklauseln