

# Vereinbarung über Auftragsver- arbeitung iSd Art 28 DSGVO

ZWISCHEN

**WeShip Fullfillment GmbH**

Frikusweg 10

8141 Premstätten bei Graz

Österreich

FN 482394d

UID: ATU72873027

(im Folgenden »Auftragsverarbeiter« genannt)

UND

**Firma**

Adresse

PLZ Ort

(Firmenbuch-Nr.)

(UID)

(im Folgenden »Verantwortlicher« genannt)

**1.**

Der Auftragsverarbeiter übernimmt für den Verantwortlichen folgenden Auftrag: Das Dropshipping Konzept bietet dem Verantwortlichen die Möglichkeit, als selbstständiger Händler Produkte zu verkaufen und den Versand dieser Produkte über den Auftragsverarbeiter durchführen zu lassen. Sämtliche Produkte werden vom Auftragsverarbeiter und dessen Partner im Auftrag des Verantwortlichen an die Endkunden des Verantwortlichen geliefert. Der Auftrag umfasst alle notwendigen Arbeiten zur Erbringung dieser Dienstleistungen.

Hierbei verpflichtet sich der Auftragsverarbeiter zur Geheimhaltung und zur Einhaltung der gesetzlichen Datenschutzbestimmungen gegenüber dem Verantwortlichen.

**Art und Zweck der Datenverarbeitung:**

Der Zweck der Datenverarbeitung liegt in der Bereitstellung der Dienstleistung des Auftragsverarbeiters, insbesondere des Dropshipping-Konzepts in der Erbringung von Lagerhaltungs-, Logistik-, bzw. Versanddienstleistungen.

**Art der personenbezogenen Daten:**

Vor- und Nachname, Lieferadresse, unter Umständen E-Mail-Adresse und Telefonnummer des Kunden.

Kategorien betroffener Personen:

Kunden des Verantwortlichen

**2.**

Der Auftragsverarbeiter verpflichtet sich, Daten des Verantwortlichen ausschließlich im Rahmen des Auftrags und der Anweisungen des Verantwortlichen und nur insoweit zu verwenden, als dies zum Zwecke der Erfüllung seiner vertraglichen Verpflichtungen notwendig ist. Insbesondere hat der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen unverzüglich zu verschlüsseln, sobald mit pseudonymisierten Daten das Auslangen gefunden wird. Der Personenbezug ist gänzlich zu beseitigen (Anonymisierung), sobald dieser zur Erfüllung des gegenständlichen Vertrages nicht mehr notwendig ist. Eine Verwendung von Daten des Verantwortlichen für eigene Zwecke des Auftragsverarbeiters ist nur mit schriftlicher Zustimmung des Verantwortlichen zulässig.

**3.**

Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle mit der Dienstleistung befassten Personen vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses vertraglich verpflichtet hat. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit dem Datenverkehr befassten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht. Die Verpflichtung zur Verschwiegenheit gilt sowohl für Daten von natürlichen als auch von juristischen Personen und Personengemeinschaften. Der Auftragsverarbeiter erklärt rechtsver-

bindlich, dass er alle mit der Dienstleistung befassten Personen vor Aufnahme der Tätigkeit nachweislich über die Folgen einer Verletzung des Datengeheimnisses belehrt hat.

**4.**

Den Auftragsverarbeiter trifft die Verantwortung dafür, dass seine Mitarbeiter und Beauftragten über die für sie geltenden Bestimmungen aus dieser Vereinbarung ausreichend informiert sind.

**5.**

Der Auftragsverarbeiter darf Sub-Auftragsverarbeiter (andere Personen, Unternehmen oder Niederlassungen, z.B. im Rahmen von Subvergaben, Werkverträgen, Beauftragung, Leiharbeit) nur mit ausdrücklicher schriftlicher Zustimmung des Verantwortlichen heranziehen. Der Auftragsverarbeiter muss die Verpflichtungen aus dieser Vereinbarung an seine Sub-Auftragsverarbeiter nachweislich überbinden.

**6.**

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

**7.**

Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er ausreichende technische Sicherheitsmaßnahmen ergriffen hat, um zu verhindern, dass Daten des Verantwortlichen ordnungswidrig verwendet oder unbefugten Dritten zugänglich werden (unbefugte Dritte sind natürliche oder juristische Personen, deren Tätigkeit dem Auftragsverarbeiter nicht gem. Punkt 5 dieser Vereinbarung zuzurechnen ist bzw. die vom Auftragsverarbeiter keiner vertraglichen Verpflichtung im Sinne des Punkt 3 dieser Vereinbarung unterworfen wurden).

**8.**

Der Auftragsverarbeiter wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung unter Umständen ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat. Die Prüfung zur Führungspflicht obliegt dem Auftragsverarbeiter selbst.

**9.**

Der Auftragsverarbeiter trägt für die technischen und organisatorischen Voraussetzungen Vor-sorge, dass der Verantwortliche seine datenschutzrechtlichen Verpflichtungen nach Kapitel III der DSGVO (insb. das Auskunftsrecht, das Recht auf Berichtigung oder Löschung sowie das Widerspruchsrecht) gegenüber einer betroffenen Person innerhalb der für den Verantwortlichen geltenden gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Verantwortlichen alle dafür notwendigen Informationen. Der Auftragsverarbeiter wird den Verantwortlichen diesbezüglich vollumfänglich unterstützen. Dem Verantwortlichen sind alle Informationen zur

**10.**

Verfügung zu stellen, die zur Kontrolle der Einhaltung der Verpflichtungen des Auftragsverarbeiters notwendig sind.

**11.**

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich bei Verdacht auf Verstöße gegen vertragliche oder gesetzliche Datenschutzbestimmungen, insbesondere bei einem Verdacht des data breach, bei Verstößen gegen solche Bestimmungen oder andere Unregelmäßigkeiten im Zusammenhang mit den Daten des Verantwortlichen sowie über Ermittlungen, Kontrollen und Maßnahmen durch die Aufsichtsbehörde(n). Der Auftragsverarbeiter wird den Verantwortlichen diesbezüglich vollumfänglich unterstützen.

Der Auftragsverarbeiter wird den Verantwortlichen auch bei den sonstigen den Verantwortlichen sich aus der DSGVO treffenden Pflichten vollumfänglich unterstützen. Dies betrifft ua Unterstützungsleistungen bei Datenschutzfolgenabschätzungen.

**12.**

Erhält der Auftragsverarbeiter einen behördlichen Auftrag, Daten des Verantwortlichen heraus-zugeben, so hat er - sofern gesetzlich zulässig - den Verantwortlichen unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragsverarbeiters eines schriftlichen Auftrages.

**13.**

Der Verantwortliche hat das Recht, eigene Mitarbeiter oder im Auftrag des Verantwortlichen tätige externe Experten jederzeit in die Geschäftsräume des Auftragsverarbeiters zu entsenden, um Geschäftsprozesse, Abrechnungsunterlagen und die aus den datenschutzrechtlichen Bestimmungen resultierenden Verpflichtungen und Schutzmaßnahmen auf ihre Zweckmäßigkeit, Richtigkeit und Vollständigkeit sowie ihre Gesetzeskonformität hin zu prüfen. Zu diesem Zweck wird der Auftragsverarbeiter die für eine ordnungsgemäße Prüfung erforderlichen Unterlagen vorlegen und die benötigten Auskünfte erteilen.

**14.**

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von drei Monaten zum Monatsletzten gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

**15.**

Der Auftragsverarbeiter haftet für den Ersatz von Schäden, die dem Verantwortlichen aufgrund von Verstößen des Auftragsverarbeiters bzw dessen Sub-Auftragsver-

arbeitern gegen Daten-schutzvorschriften oder diese Vereinbarung entstehen und hält diesbezüglich den Verantwortli-chen schad- und klaglos.

**16.**

Der Auftragsverarbeiter ist nach Beendigung der Dienstleistung verpflichtet, dem Verantwortlichen alle Verarbeitungsergebnisse und Unterlagen, die Daten des Verantwortlichen enthalten, zu übergeben bzw. in dessen Auftrag unwiederbringlich zu vernichten, soweit nicht im Einzelfall gesetzliche Bestimmungen oder behördliche Anforderungen einer solchen Vernichtung entgegenstehen.

**17.**

Die vorliegende Vereinbarung ist an etwaige geänderte Datenschutz-Bestimmungen, sofern sie für die gegenständliche Vereinbarung relevant sind, anzupassen.

**18.**

Diese Vereinbarung gilt für alle bestehenden und zukünftigen vertraglichen Beziehungen zwischen Verantwortlichem und Auftragsverarbeiter; dies sowohl während als auch nach Beendigung einzelner oder aller Vertragsverhältnisse.

**19.**

Zu dieser Vereinbarung bestehen keine mündlichen Nebenabreden. Allfällige Änderungen und Ergänzungen zu dieser Vereinbarung haben in Schriftform zu erfolgen. Dies gilt auch für die Vereinbarung des Abgehens von diesem Formerfordernis selbst.

**20.**

Diese Vereinbarung unterliegt österreichischem Recht unter Ausschluss der kollisionsrechtlichen Verweisungsnormen und des UN-Kaufrechts.

Als Gerichtsstand für sämtliche Auseinandersetzungen im Zusammenhang mit dieser Vereinba-rung wird das sachlich zuständige Gericht in Graz als ausschließlich zuständig vereinbart.

.....

DATUM



.....

DI CHRISTIAN FAST, BA

AUFTRAGSVERARBEITER

VERANTWORTLICHER

## **Anlage ./I – Technisch-organisatorische Maßnahmen**

### **Vertraulichkeit**

- Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, durch z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Verschlüsselung von Datenträgern;
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten;
- Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
- Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

### **Integrität**

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

### **Verfügbarkeit und Belastbarkeit**

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline);, unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherheitskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
- Rasche Wiederherstellbarkeit;
- Lösungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Datenschutzfreundliche Voreinstellungen;
- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.