

## **Auftragsdatenverarbeitungsvertrag (ADV)**

Dieser Vertrag ist ein Anhang zum Servicevertrag bzw. SaaS-Vertrag (nachfolgend als „**Hauptvertrag**“ bezeichnet) zwischen Spacewise AG, Rotfluhstrasse 63, 8702 Zollikon, Schweiz (nachstehend als „**Auftragsverarbeiter**“ bezeichnet) und dem Kunden gemäss dem Hauptvertrag.

### **1. Gegenstand des Vertrags**

- 1.1. Dieser Vertrag regelt neben dem Hauptvertrag die Verarbeitung von personenbezogenen Daten des Kunden durch den Auftragsverarbeiter. Der Zweck der Datenverarbeitung und die Liste der betroffenen Personengruppen und Datentypen sind in Anlage 1 zu diesem Vertrag enthalten.
- 1.2. Für diesen Vertrag gelten die Bestimmungen des Schweizerischen Datenschutzgesetzes (DSG) und, soweit die Verarbeitung in den Geltungsbereich der Europäischen Datenschutzgrundverordnung (DSGVO) fällt, die Bestimmungen der DSGVO.
- 1.3. Der Vertrag regelt insbesondere die Datenschutzmassnahmen im Sinne von Art. 10a DSG und Art. 28 DSGVO und die Rechte und Pflichten des Kunden und des Auftragsverarbeiters zur Erfüllung der Anforderungen des DSG und der DSGVO.

### **2. Rechte des Kunden**

- 2.1. Der Kunde ist für die Datenverarbeitung im Rahmen dieses Vertrages verantwortlich. Bei der Erhebung, Verarbeitung und Nutzung seiner Daten ist er für die Prüfung der Zulässigkeit und die Einhaltung der geltenden Datenschutzbestimmungen sowie für die Wahrung der Rechte der Betroffenen verantwortlich.
- 2.2. Der Auftragsverarbeiter darf die Daten nur im Rahmen dieses Vertrages und nach Anweisung des Kunden erheben, verarbeiten und nutzen. Eine Verwendung für andere Zwecke, auch für eigene Zwecke des Auftragsverarbeiters, ist nicht gestattet, ausser der Mieter des Kunden hat ausdrücklich zugestimmt.
- 2.3. Der Kunde behält sich das Recht vor, im Rahmen des Hauptvertrages Anweisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen.
- 2.4. Änderungen der verarbeiteten Datentypen und Verfahrensänderungen sind gemeinsam zu vereinbaren und zu dokumentieren.
- 2.5. Anweisungen können vom Kunden allgemein oder im Einzelfall erteilt werden. Sie müssen schriftlich erfolgen. Einzelne Anweisungen können auch mündlich erteilt werden, müssen aber durch den Kunden unverzüglich schriftlich bestätigt werden. Der Kunde benennt dem Auftragsverarbeiter jene Personen, die Anweisungen zu erteilen befugt sind.

### **3. Pflichten des Auftragsverarbeiters**

- 3.1. Der Auftragsverarbeiter handelt ausschliesslich im Rahmen der getroffenen Vereinbarungen und nach den Anweisungen des Kunden.
- 3.2. Der Auftragsverarbeiter versichert, dass er die Vorgaben Art. 10a DSG bzw. Art. 28 DSGVO erfüllt und prüft und dokumentiert die Erfüllung seiner gesetzlichen Pflichten durch regelmässige interne Kontrollen.
- 3.3. Die Datenverarbeitung erfolgt nur auf dem Gebiet der Schweiz und im Europäischen Wirtschaftsraum (EWR). Eine Datenverarbeitung in anderen Ländern (sog. Drittstaaten) ist nur nach vorheriger schriftlicher Zustimmung des Kunden und bei Vorliegen der entsprechenden gesetzlichen Voraussetzungen zulässig.
- 3.4. Der Auftragsverarbeiter verpflichtet sich, nach vorheriger Absprache Vor-Ort-Kontrollen des Kunden zu unterstützen, die erforderlichen Unterlagen und Informationen zur Verfügung zu stellen und bei Datenschutz- und datenschutzrelevanten Kontrollen durch die Aufsichtsbehörden innerhalb angemessener Frist alle erforderlichen Auskünfte zu erteilen.
- 3.5. Der Auftragsverarbeiter unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Erfüllung der Pflichten nach den Artikeln 32 bis 36 DSGVO.
- 3.6. Sollte eine Anweisung des Kunden gegen die geltenden Datenschutzbestimmungen verstossen, wird der Kunde vom Auftragsverarbeiter darauf hingewiesen.
- 3.7. Der Auftragsverarbeiter verpflichtet sich, den Kunden unverzüglich über Verstösse gegen die Datenschutzbestimmungen zu informieren.
- 3.8. Sind die Daten des Kunden beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Massnahmen Dritter gefährdet oder müssen sie Dritten, insbesondere Behörden, bekannt gegeben werden, so hat der Auftragsverarbeiter dies dem Kunden unverzüglich mitzuteilen. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Herrschaft über die Daten beim Kunden liegt.
- 3.9. Leistungen gemäss Ziffern 3.4 und 3.5 erfolgen gegen Entschädigung zu den Stundensätzen gemäss Hauptvertrag.

### **4. Technische und organisatorische Massnahmen zur Datensicherheit**

- 4.1. Der Auftragsverarbeiter ist verpflichtet, die Grundsätze ordnungsgemässer Datenverarbeitung zu beachten und deren Einhaltung zu überwachen.
- 4.2. Auftragsverarbeiter gewährleistet die Installation und Aufrechterhaltung der notwendigen und angemessenen Datenschutzmassnahmen gemäss Art. 7 DSG und Art. 32 DSGVO. Die verbindlichen technischen und organisatorischen Massnahmen sind in Anlage 2 aufgeführt und Bestandteil dieses Vertrages.

## **5. Rechte der betroffenen Personen**

- 5.1. Macht eine betroffene Person datenschutzrechtliche Ansprüche geltend (z.B. das Recht auf Information), unterstützt der Auftragsverarbeiter den Kunden bei der Erfüllung der Ansprüche.
- 5.2. Wendet sich eine betroffene Person zur Geltendmachung ihrer Rechte (insbesondere Art. 8 DSG und Kapitel 3 DSGVO) direkt an den Auftragsverarbeiter, so wird er die Anfrage unverzüglich an den Kunden weiterleiten.

## **6. Unterauftragnehmer**

- 6.1. Der Auftragsverarbeiter kann Unteraufträge zur Datenverarbeitung vergeben; derzeit sind dies die Unterauftragnehmer gemäss Anlage 1 zu diesem ADV. Der Auftragsverarbeiter informiert den Kunden vor einer beabsichtigten Änderung. Der Kunde kann einen Subunternehmer ohne Angabe von Gründen ablehnen, wobei eine Ablehnung des Auftragsverarbeiters zur ausserordentlichen Kündigung des Vertrages berechtigt.
- 6.2. Der Auftragsverarbeiter wählt den Unterauftragnehmer sorgfältig aus und beauftragt nur solche Dritte, die einen der Erfüllung der Aufgabe angemessenen Sicherheitsstandard erfüllen. Die vertraglichen Vereinbarungen mit dem Unterauftragnehmer sind so zu gestalten, dass sie den datenschutzrechtlichen Bestimmungen dieses Vertrages entsprechen, insbesondere durch ausreichende Garantien, dass geeignete technische und organisatorische Massnahmen getroffen werden, um sicherzustellen, dass die Verarbeitung in Übereinstimmung mit den gesetzlichen Bestimmungen erfolgt.
- 6.3. Das Untervertragsverhältnis wird schriftlich gemäss Art. 28 DSGVO abgeschlossen, wobei dem Kunden auch ein Besichtigungs- und Kontrollrecht eingeräumt wird. Der Kunde trägt allfällige Kosten hierfür. Auftragsverarbeiter stellt auf Anfrage eine Kopie des Unterauftrages und alle notwendigen Informationen zur Verfügung.
- 6.4. Nicht als Untervertragsverhältnis im Sinne dieser Regelung zu verstehen sind solche Leistungen, die Auftragsverarbeiter von Dritten zur Unterstützung bei der Ausführung des Auftrages, z.B. Telekommunikationsdienste oder Wartung, genutzt werden.

## **7. Kontrollrechte des Kunden**

- 7.1. Der Auftragsverarbeiter liefert dem Kunden alle notwendigen Informationen, um die Einhaltung der in diesem Vertrag festgelegten Verpflichtungen nachzuweisen.
- 7.2. Der Kunde ist berechtigt, schriftliche Auskünfte und Nachweise über die getroffenen Datenschutzmassnahmen und deren technische und organisatorische Umsetzung zu verlangen.

- 7.3. Der Kunde kann sich vor Beginn der Datenverarbeitung und dann in regelmässigen Abständen nach vorheriger Abstimmung vor Ort beim Auftragsverarbeiter von der Angemessenheit der Massnahmen zur Einhaltung der technischen und organisatorischen Datenschutzerfordernungen überzeugen. Der Auftragsverarbeiter ermöglicht solche Überprüfungen, liefert die notwendigen Informationen und bietet die notwendige Unterstützung
- 7.4. Die Kontrollen sollen ohne vermeidbare Störungen des Geschäftsbetriebs von Auftragsverarbeiter durchgeführt werden. Sofern aus dringenden, vom Kunden zu dokumentierenden Gründen nicht anders angegeben, finden die Prüfungen nach angemessener Vorankündigung und während den Geschäftszeiten des Auftragsverarbeiters und nicht häufiger als alle 12 Monate statt. Wenn der Auftragsverarbeiter nachweist, dass die vereinbarten Datenschutzverpflichtungen korrekt umgesetzt wurden, sollten die Kontrollen auf Stichproben beschränkt werden.
- 7.5. Leistungen des Auftragsverarbeiters gemäss diesem Abschnitt 7 sind zu den Stundensätzen gemäss Hauptvertrag zu entschädigen.

## **8. Geheimhaltung**

- 8.1. Die Parteien verpflichten sich, alle ihnen im Zusammenhang mit der Auftragsabwicklung zur Verfügung gestellten Unterlagen und Daten sowie die Arbeitsergebnisse vertraulich zu behandeln und insbesondere nicht unbefugten Personen zugänglich zu machen
- 8.2. Personen, die an der Datenverarbeitung beteiligt sind, ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Dieses Verbot bleibt auch nach Beendigung der Tätigkeit bestehen. Die betroffenen Personen sind schriftlich auf das Datengeheimnis zu verpflichten.
- 8.3. Diese Verpflichtungen gelten auch nach Beendigung des Vertrages.

## **9. Vertragsdauer und Beendigung**

- 9.1. Die Laufzeit dieses Auftragsverarbeitungsvertrags richtet sich nach dem Hauptvertrag.
- 9.2. Der Kunde nimmt zur Kenntnis, dass er die Daten jederzeit als CSV-Datei von der Plattform des Auftragsverarbeiters extrahieren kann. Nach Beendigung dieses Vertrages hat der Auftragsverarbeiter alle Datenträger und alle Daten (einschliesslich angefertigter Kopien oder Duplikate) auf Verlangen nach dessen Anweisung sicher zu löschen oder zu vernichten, es sei denn, es besteht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten.
- 9.3. Diese Verpflichtung gilt in gleichem Umfang für allfällige Subunternehmer.

## **10. Schlussbestimmungen**

- 10.1. Im Übrigen gelten die Schlussbestimmungen gemäss Hauptvertrag auch für diesen ADV.

## Anlage 1 – Angaben zur Verarbeitung von Personen- und anderen Daten

### 1. Art und Zweck der Verarbeitung

Die Verarbeitung erfolgt durch Speicherung auf den Systemen des Auftragsverarbeiters, Ermöglichung von Zugriffen durch Mitarbeiter der Parteien bzw. Übermittlung an den Kunden über das Internet, Übermittlung an Dritte im Auftrag des Kunden, Löschung der Daten. Die Verarbeitung dient der Erfüllung des Hauptvertrages (Software as a Service).

### 2. Kategorien betroffener Personen

Von der Verarbeitung betroffen sind folgende Kategorien betroffener Personen: (1) Mieter des Kunden und (2) Mitarbeiter/Freelancer des Kunden.

### 3. Art der verarbeiteten Daten

Es werden folgende Daten verarbeitet (personenbezogene und andere Daten):

#### a) Mieter des Kunden

<b>Stammdaten</b>	z.B. Vorname, Name, Geburtsdatum, Briefanrede, Adresse, Kundennummer, Standort, E-Mail, Korrespondenz-Sprache, Mobiltelefon, Telefon, Mieter, Mieter-Organisation, Notiz, Status, Kundengruppe
<b>Transaktion</b>	z.B. Nummer, Mietobjekt, Mietbeginn, Mietende, Preistotal, Zahlung
<b>Zahlung</b>	z.B. Datum, Beschreibung, Zahlung, CC Nummer, Referenz-Nr.
<b>Nutzungsdaten</b>	z.B. Mietobjekt, Mietbeginn, Mietende, Status, Abwicklungs-Status, Preistotal, Zahlung
<b>Mietobjekt gebucht</b>	z.B. Name, Bild, Standort Kategorie Sub-Kategorie Objektgruppe Aktiv ab, Aktiv bis, Marke, Modell, Inventarnummer, Seriennummer, Saisonschema, Kaution
<b>Zubehör gebucht</b>	z.B. Zubehör-Name Marke, Modell, Anzahl, Preis, Gesamtpreis
<b>Dienstleistung gebucht</b>	z.B. Name, Für Zubehör, Anz. Objekte, Prozentsatz, Fixpreis, Anz. Zeiteinheiten Zeiteinheit, Preis, Zeit-basierter Preis, Endpreis, Währung, Anz. Angebote, Prozent, Preis
<b>Zuschläge / Rabatte</b>	z.B. Beschreibung, Betrag

b) Mitarbeiter/Freelancer des Kunden

<b>Stammdaten</b>	z.B. Vorname, Name, Geburtsdatum, Kontakt, E-Mail, Korrespondenz-Sprache, Mobiltelefon, Telefon, Fax, Bürostandort, Benutzername, Konto, E-Mail
-------------------	---

**4. Unterauftragnehmer**

Der Auftragnehmer kann folgende Unter-Auftragnehmer beauftragen:

- a. Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA;
- b. Datatrans Ltd., Kreuzbühlstrasse 26, 8008 Zürich, Switzerland;
- c. Customer.io (Peaberry Software, Inc.), 9450 SW Gemini Dr, Ste 43920, Beaverton, Oregon, 97008, USA;
- d. Segment.io, Inc., 100 California Street, 7th Floor, San Francisco, CA 94111, USA;
- e. Stripe, Inc., 354 Oyster Point Blvd, South San Francisco, California 94080, USA;
- f. RunMyAccounts AG, Grundstrasse 16b, CH-8712 Stäfa, Switzerland;
- g. Close.com, PO Box 7775 #69574 San Francisco, CA 94120-777, USA;
- h. Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg;
- i. Sendgrid, 1801 California St. Denver, Colorado 80202, USA;

## **Anlage 2: Organisatorische und Technische Massnahmen der Datensicherheit**

### **1. Vertraulichkeit**

- 1.1. Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B. Schlüssel, Chipkarten, elektrische Türöffner, Portier, Alarmanlagen, Videoanlagen.
- 1.2. Zugangskontrolle: Schutz vor unbefugter Systembenutzung, z.B. Kennwörter (einschliesslich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung für Administratoren, Verschlüsselung von Daten.
- 1.3. 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, insbesondere von administrativen Benutzerkonten.
- 1.4. Klassifikationsschema für Daten: Kundendaten werden grundsätzlich als vertraulich eingestuft.

### **2. Integrität**

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

### **3. Verfügbarkeit und Belastbarkeit**

- 3.1. Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust (auch physischer Natur), z.B.: Backup-Strategie (online/offline; on- site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern.
- 3.2. Rasche Wiederherstellbarkeit.
- 3.3. Lösungsfristen: Sowohl für Daten selbst, nach der Deaktivierung des Kontos, als auch Metadaten wie Logfiles, etc. geltend folgende Löschrfristen: vierteljährlich.

#### **4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung**

- 4.1. Datenschutz-Management, einschliesslich regelmässiger Mitarbeiter-Schulungen und vertraglicher Verpflichtung der Mitarbeiter.
- 4.2. Incident-Response-Management.
- 4.3. Auftragskontrolle: Keine Auftragsverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters.

12. April 2022