

**Vereinbarung über Auftragsverarbeitung von Daten nach Art. 28 Abs. 3 Datenschutz-  
Grundverordnung (DS-GVO)**

zwischen

- nachstehend „Auftraggeber“ genannt –

und

**Spesenfuchs GmbH**

**Kettengasse 7c**

**79206 Breisach**

- nachstehend „Auftragnehmer“ genannt –

- nachstehend einzeln oder gemeinsam auch „Partei“ bzw. „Parteien“ genannt –

- Stand: Februar 2021 –

## **Präambel**

Zwischen dem Auftraggeber und dem Auftragnehmer besteht ein Vertrag über die Nutzung des in § 1 näher bezeichneten Softwaremoduls Spesenfuchs (im Weiteren Lizenzvereinbarung) des Auftragnehmers durch den Auftraggeber. Der Auftragnehmer unterstützt den Auftraggeber bei der Umsetzung eigener Geschäftszwecke im Zusammenhang mit dem Vertrag – eine Übertragung von 'Funktionen' ist ausdrücklich nicht beabsichtigt.

## **§ 1 Vertragsgegenstand / Rechtsgrundlage**

### **(1) Gegenstand**

Der Auftragnehmer bietet seinen Kunden verschiedene Dienstleistungen rund um das Thema Reisekosten an. Dazu gehören im Kern die Erstellung und Speicherung von Reisekostenabrechnungen. In der Version „Team“ ist es zusätzlich möglich weitere Benutzer anzulegen, die ebenfalls Reisekostenabrechnungen erstellen und speichern können. Diese erbringt der Auftragnehmer auf Basis der mit dem Auftraggeber vereinbarten AGBs und dem auf der Webseite [spesenfuchs.de](https://www.spesenfuchs.de) beschriebenen Funktionsumfang. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den einzelnen vom Auftraggeber beim Auftragnehmer gebuchten Leistungen (nachfolgend zusammengefasst „Hauptvertrag“) in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte personenbezogene Daten des Auftraggebers in Berührung kommen können.

### **(2) Dauer**

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Lizenzvereinbarung.

## **§ 2 Konkretisierung des Auftragsinhaltes**

### **(1) Art und Zweck der vorhergesehenen Verarbeitung von Daten**

Der Zweck von Spesenfuchs ist es, Klein- und Kleinstunternehmen sowie Selbstständige bei der Durchführung ihrer Geschäftstätigkeit optimal zu unterstützen und zu entlasten. Hierbei erbringt Spesenfuchs insbesondere Leistungen der Datenverarbeitung sowie andere Dienstleistungen und Nebenleistungen. Der Auftragnehmer erhält dabei Zugriff auf die bei der Benutzung der in den vertragsgegenständlichen Softwaremodulen gespeicherten personenbezogenen Daten. Folgende Datenkategorien können vom Auftraggeber durch direkte Eingabe oder durch Hochladen in Spesenfuchs verarbeitet werden:

*Angaben zur Reise:* Name, Name des Reisenden, Zeitraum, Start- und Zielort, Belege

*Angaben zur Firma:* Firmenname, Vorname, Name, Anschrift, Telefon, Mobilnummer, Fax, Bankverbindung, Kreditorenkonto

*Angabe zu Mitbenutzern (User) in Spesenfuchs:* Stammdaten wie Personalnummer, Vorname, Name, E-Mail, Anschrift, Telefon, Mobilnummer, Fax, Bankverbindung, Kreditorenkonto

Alle Kernfunktionen von Spesenfuchs werden ausschließlich in Deutschland entwickelt und gehostet. Darüber hinaus gibt es ergänzende Zusatzfunktionen (z.B. Supportplattform, Zahlungsabwicklung), bei der auf durch den Auftraggeber genehmigte Subunternehmen (siehe <https://www.spesenfuchs.de/subunternehmer/>) zurückgegriffen wird, die in

Ausnahmefällen außerhalb der EU/EWR ihren Sitz haben. Jede Verlagerung einer Datenverarbeitung in ein Drittland außerhalb der EU/EWR bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau in den USA wird hergestellt durch Standarddatenschutz-klauseln (Art. 46 Abs. 2 litt. c und d DSGVO).

Der Auftragnehmer kann die vom Auftraggeber zur Verfügung gestellten und im Rahmen seiner Leistungserbringung zusätzlich gewonnenen Daten für rein statistische Zwecke aggregieren und daraus Statistiken ohne Nennung des Auftraggebers und in eigenem Namen veröffentlichen. Dies beschränkt sich auf ausschließlich anonymisierte, aggregierte Daten ohne jeglichen Personenbezug.

## **(2) Kategorien betroffener Personen**

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Mitarbeiter des Auftraggebers
- Stellvertreter

## **§ 3 Rechte und Pflichten des Auftragnehmers**

- (1) Der Auftragnehmer verarbeitet die Daten entsprechend der gesetzlichen Bestimmungen, der Bestimmungen dieses Vertrags für die in § 2 (1) beschriebenen Zwecke und nach Weisung des Auftraggebers. Ist der Auftragnehmer aufgrund einer gesetzlichen Bestimmung gehindert, die Daten entsprechend dieses Vertrags und der Weisungen des Auftraggebers zu verarbeiten, informiert er den Auftraggeber vor der Verarbeitung hierüber, es sei denn, eine solche Inkenntnissetzung ist aus wichtigen Gründen des öffentlichen Interesses gesetzlich untersagt. Der Auftragnehmer darf die Daten für keine anderen Zwecke verwenden und ist insbesondere nicht berechtigt, die ihm überlassenen Daten an Dritte weiterzugeben. Kopien und Duplikate werden ohne vorherige Einwilligung des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung. Im Fall der Wartung, Fernwartung und/oder IT-Fehleranalyse ist der Zugriff auf Daten des Auftraggebers nach Möglichkeit zu vermeiden. Ist ein Datenzugriff nicht vermeidbar, muss der Auftraggeber den Datenzugriff auf das Minimum beschränken.
- (2) In dem vom Auftraggeber gesetzten Rahmen ist der Auftragnehmer allein für die Art und Weise und die Mittel der Datenverarbeitung verantwortlich.
- (3) Alle Kernfunktionen von Spesenfuchs werden ausschließlich in Deutschland entwickelt und gehostet. Darüber hinaus gibt es ergänzende Zusatzfunktionen (z.B. Supportplattform, Zahlungsabwicklung), bei der auf durch den Auftraggeber genehmigte Subunternehmen (siehe <https://www.spesenfuchs.de/subunternehmer/>) zurückgegriffen wird, die in Ausnahmefällen außerhalb der EU/EWR ihren Sitz haben. Jede Verlagerung einer Datenverarbeitung in ein Drittland außerhalb der EU/EWR bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau in den USA wird hergestellt durch Standarddatenschutz-klauseln (Art. 46 Abs. 2 litt. c und d DSGVO).
- (4) Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

- (5) Der Auftragnehmer unterstützt den Auftraggeber, insbesondere bei Datenschutzüberprüfungen durch die Aufsichtsbehörden, sofern diese Überprüfungen die Datenverarbeitung gemäß dieses Vertrags betreffen, und ist zur sofortigen Umsetzung der Auflagen der Aufsichtsbehörde in Absprache mit dem Auftraggeber verpflichtet. Der Auftragnehmer selbst überwacht auch die Einhaltung der gesetzlichen Bestimmungen sowie die Bestimmungen dieses Vertrags im eigenen Bereich. Der Auftragnehmer führt in regelmäßigen Abständen Kontrollen durch, um die Wirksamkeit und den Erfolg der umgesetzten technischen und organisatorischen Datenschutzmaßnahmen zu prüfen.
- (6) Der Auftragnehmer ist zur Unterstützung des Auftraggebers entsprechend dessen Weisungen verpflichtet, wenn der Auftraggeber seine Pflichten gegenüber betroffenen Person erfüllt, die ihre Rechte nach den gesetzlichen Bestimmungen ausüben (z. B. Recht auf Auskunft, Berichtigung). Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, so wird dieser keine Auskünfte erteilen, sondern die betroffene Person an den Auftraggeber verweisen; er wird den Auftraggeber entsprechend informieren.
- (7) Der Auftragnehmer wird, soweit ein Zusammenhang mit der Datenverarbeitung durch den Auftraggeber besteht, den Auftraggeber auch bei der Wahrnehmung seiner sonstigen gesetzlichen Pflichten unterstützen. Er wird insbesondere den Auftraggeber unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen und / oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten informieren. Der Auftragnehmer ist sich bewusst, dass der Auftraggeber verpflichtet ist, den Aufsichtsbehörden Datenschutzverletzungen unverzüglich zu melden. Die entsprechenden Informationen sind zu dokumentieren; sie müssen die für die Meldung an die Aufsichtsbehörden erforderlichen Details enthalten. Im Fall von Datenschutzverletzungen unterstützt der Auftragnehmer den Auftraggeber auf Aufforderung bei der Benachrichtigung der betroffenen Personen und der Aufsichtsbehörde.
- (8) Der Auftragnehmer hat den Auftraggeber umgehend über sämtliche an den Auftragnehmer gerichtete Mitteilungen der Aufsichtsbehörden (z. B. Anfragen, Benachrichtigung über Maßnahmen oder Auflagen) in Verbindung mit der Verarbeitung von Daten nach diesem Vertrag zu informieren. Vorbehaltlich zwingender gesetzlicher Auflagen darf der Auftragnehmer Auskünfte an Dritte, auch an Aufsichtsbehörden, nur nach vorheriger Zustimmung (schriftlich oder per E-Mail) durch und in Abstimmung mit dem Auftraggeber erteilen.
- (9) Fertigstellung der Auftragsarbeit oder früher auf Verlangen des Auftraggebers löscht der Auftragnehmer alle personenbezogenen Daten bzw. vernichtet Datenträger mit personenbezogenen Daten datenschutzgerecht entsprechend aktueller und anerkannter technischer Standards in der Weise, dass eine Wiederherstellung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Ausgenommen hiervon sind anonymisierte Testdaten, die zu Testzwecken benötigt werden.
- (10) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

#### **§ 4 Kontrollrechte des Verantwortlichen**

1. Der Verantwortliche hat nach Vorankündigung das Recht, die Einhaltung der über die datenschutzrechtlichen Prozesse und der vertraglichen Vereinbarung durch den Auftragsverarbeiter oder das externe Rechenzentrum/den Unterauftragsverarbeiter zu kontrollieren. Dies kann entweder durch die Einholung von Auskünften oder die Vorlage von

aktuellen Testaten, Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter) oder durch eine geeignete Zertifizierung mittels IT-Sicherheits- oder Datenschutzaudit erfolgen. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

2. Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

## **§ 5 Technische und organisatorische Sicherheitsmaßnahmen**

- (1) Der Auftragnehmer stellt sicher, dass der Umgang mit den Daten des Auftraggebers ausschließlich unter Beachtung der nach den gesetzlichen Bestimmungen und dieses Vertrags erforderlichen technischen und organisatorischen Maßnahmen erfolgt. Über bestehende Technische und organisatorische Sicherheitsmaßnahmen informiert der Auftragsverarbeiter über folgende Webseite <https://www.spesenfuchs.de/tom/>.
- (2) Soweit Leistungen im Bereich Wartung, Fernwartung und/ oder IT-Fehleranalyse erbracht werden, gelten ergänzend folgende Regelungen:
  - a. Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren. Vor Durchführung der Arbeiten werden sich der Auftraggeber und der Auftragnehmer über etwa notwendige Datensicherungsmaßnahmen verständigen.
  - b. Alle Leistungen werden vom Auftragnehmer dokumentiert und protokolliert.
  - c. Wirkdaten (Produktivdaten, z. B. Daten des Auftraggebers, Netzdaten zur Erbringung des Telekommunikationsdienstes des Auftraggebers) dürfen nur auf ausdrückliches Verlangen des Auftraggebers und nur zu Fehleranalysezwecken verwendet werden. Diese Daten dürfen ausschließlich auf dem bereitgestellten Equipment des Auftraggebers verwendet werden oder auf Equipment des Auftragnehmers, das zuvor vom Auftraggeber für diesen Zweck freigegeben wurde. Wirkdaten dürfen nicht ohne ausdrückliche Einwilligung des Auftraggebers in Textform auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.
- (3) Datenschutzfreundliche Voreinstellungen: Sofern Daten zur Erreichung des Verwendungszwecks nicht erforderlich sind, werden die technischen Voreinstellungen so festgelegt, dass Daten nur durch eine Aktion der Betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.

## **§ 6 Vertraulichkeit**

- (1) Der Auftragnehmer gewährleistet, dass nur solche Personen zur Verarbeitung der personenbezogenen Daten befugt werden, die sich zuvor zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Er gewährleistet, dass personenbezogene Daten nicht unbefugt erhoben, verarbeitet oder genutzt werden, insbesondere für keine anderen Zwecke und dass sie nicht an Dritte übermittelt werden. Der

Auftragnehmer stellt sicher, dass die mit der Datenverarbeitung betrauten Personen mit den Vorgaben und Weisungen dieser Vereinbarung im Voraus vertraut gemacht werden.

- (2) Sofern der Auftragnehmer im Rahmen seiner Tätigkeit die Möglichkeit hat, auf elektronische Kommunikationsdaten zuzugreifen, gewährleistet er, dass sich die Vertraulichkeitsverpflichtung der mit der Verarbeitung betrauten Personen erstreckt auf den Inhalt und die näheren Umstände der elektronischen Kommunikation der betroffenen Personen, insbesondere die Beteiligung einer betroffenen Person an einem elektronischen Kommunikationsvorgang und die näheren Umstände fehlgeschlagener Kommunikationsversuche.

## **§ 7 Weitere Auftragnehmer**

Der Auftraggeber stimmt einer Beauftragung von Subunternehmern zu. Ein Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer Dritte mit der Verarbeitung von Daten des Auftraggebers beauftragt oder Dritte die Zugriffsmöglichkeit auf diese Daten erhalten.

- (1) Über bestehende Unterbeauftragungsverhältnisse informiert der Auftragnehmer über folgende Webseite <https://www.spesenfuchs.de/subunternehmer/>. Bei einer Änderung der Subunternehmer informiert der Auftragnehmer in Spesenfuchs. Der Auftraggeber kann der Änderung innerhalb einer Frist von zwei Wochen aus wichtigem Grund gegenüber dem Auftragnehmer widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als erteilt.
- (2) Der Auftragnehmer stellt sicher, dass der weitere Auftragnehmer (Sub und Sub-Subunternehmer) gegenüber seinem jeweiligen Vertragspartner in entsprechender Weise verpflichtet ist, wie der Auftragnehmer gegenüber dem Auftraggeber nach diesem Vertrag verpflichtet ist. Der Auftragnehmer hat die Einhaltung der Pflichten des UnterAuftragnehmers, insbesondere die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen, vor Beginn der Datenverarbeitung und sodann regelmäßig zu überprüfen. Entsprechendes gilt im Verhältnis des Subunternehmers zum SubSubunternehmer. Das Ergebnis ist jeweils zu dokumentieren und dem Auftraggeber auf Aufforderung zur Verfügung zu stellen.
- (3) Die Weiterleitung von Daten von dem Auftragnehmer an weitere Auftragnehmer bzw. der Beginn der Leistungen im Bereich Wartung / Fernwartung / IT-Fehleranalyse ist nur dann zulässig, wenn der weitere Auftragnehmer seine Mitarbeiter entsprechend § 6 dieses Vertrags auf die Wahrung der Vertraulichkeit verpflichtet und sie entsprechend belehrt hat und die vereinbarten technischen und organisatorischen Sicherheitsmaßnahmen umgesetzt hat.

## **§ 8 Vertragsdauer; Kündigung**

- (1) Dieser Vertrag gilt für die Dauer der tatsächlichen Leistungserbringung durch den Auftragnehmer. Dies gilt unabhängig von der Laufzeit etwaiger anderer Verträge (insbesondere des Hauptvertrags), die die Parteien ebenfalls bzgl. der Erbringung der vereinbarten Leistungen abgeschlossen haben.
- (2) Der Auftraggeber kann die Kooperation mit dem Auftragnehmer jederzeit ohne Einhaltung einer Frist beenden, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen diesen Vertrag vorliegt, wenn der Auftragnehmer Überprüfungen durch einen Auftraggeber vertragswidrig ganz oder teilweise verweigert. Etwaige andere Verträge, die ebenfalls die Erbringung der Leistungen des Auftragnehmers für den Auftraggeber regeln (insbesondere den Hauptvertrag), kann der Auftraggeber in dem Fall jederzeit ohne Einhaltung einer Frist kündigen.

## **§ 9 Ansprechpartner:**

Ansprechpartner beim Auftragnehmer ist:

Souheil Manaa  
Funktion: Geschäftsführer  
Kettengasse 7c  
79206 Breisach  
E-Mail: [info@spesenfuchs.de](mailto:info@spesenfuchs.de)

## **§ 10 Haftung**

Die Haftung des Auftragnehmers gegenüber dem Auftraggeber für schuldhafte Verletzungen dieses Vertrags regelt sich nach den gesetzlichen Bestimmungen. Der Auftragnehmer haftet nicht, wenn er bei der Erhebung bzw. Verarbeitung der Daten die Regelungen dieses Vertrags beachtet hat und insbesondere die technischen und organisatorischen Sicherheitsmaßnahmen wie vereinbart umgesetzt hat.

## **§ 11 Sonstiges**

- (1) Der Auftragnehmer darf keine der Daten aus dem Grund zurückbehalten, dass er selbst ein Recht gegenüber dem Auftraggeber hat.
- (2) Von der Ungültigkeit einer Bestimmung dieses Vertrags bleibt die Gültigkeit der übrigen Bestimmungen unberührt. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.
- (3) Sämtliche Änderungen dieses Vertrags sowie Nebenabreden bedürfen der Schriftform (einschließlich per E-Mail). Dies gilt auch für das Abbedingen dieser Schriftformklausel selbst.
- (4) Es besteht zwischen den Parteien Einigkeit darüber, dass die „Allgemeinen Geschäftsbedingungen“ des Auftraggebers und des Auftragnehmers auf diesen Vertrag keine Anwendung finden.
- (5) Der alleinige Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Freiburg. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes.
- (6) Dieser Vertrag unterliegt den gesetzlichen Bestimmungen der Bundesrepublik Deutschland.
- (7) Soweit diese Vereinbarung vor dem 25.05.2018 und damit vor dem Wirksamwerden der DSGVO abgeschlossen wurde, sind sich die Parteien einig, dass bis zu diesem Zeitpunkt das jeweils national geltende Datenschutzrecht entsprechend anzuwenden ist.

Auftraggeber:

Auftragnehmer:

Ort, Datum \_\_\_\_\_

Name:

\_\_\_\_\_

Unterschrift:

\_\_\_\_\_

Ort, Datum Breisach, Feb. 2021

Name:

Souheil Manaa

Unterschrift:

\_\_\_\_\_