Vereinbarung über eine Auftragsverarbeitung

zwischen

(im Folgenden **Auftraggeber**)

und

der **SPENDIT AG**, Reichenbachstraße 31, 80469 München

(im Folgenden **Auftragnehmer**)

Inhaltsverzeichnis

Präambel 3

§ 1 Definitionen 3

§ 2 Gegenstand und Dauer des Auftrags; Umfang, Art und Zweck der Datenverarbeitung 4

§ 3 Technisch-organisatorische Maßnahmen 5

§ 4 Berichtigung, Sperrung und Löschung / Betroffenenrechte 6

§ 5 Kontrollen und sonstige Pflichten des Auftragnehmers 7

§ 6 Subunternehmer (Unterauftragsverhältnisse) bzw. Auslagerungsunternehmen 8

§ 7 Kontrollrechte des Auftraggebers 9

§ 8 Mitteilung bei Verstößen des Auftragnehmers 9

§ 9 Weisungsbefugnis des Auftraggebers 10

§ 10 Löschung von Daten und Rückgabe von Datenträgern 11

§ 11 Subunternehmer außerhalb der EU 11

§ 12 Kosten 11

§ 13 Sonstiges, Allgemeines 11

Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien im Zusammenhang mit der Auftragsverarbeitung durch den Auftragnehmer bei der Durchführung des zwischen den Parteien geschlossenen Dienstleistungsvertrag (im Folgenden „Hauptvertrag“). Der Hauptvertrag besteht für das Produkt SpenditCard aus dem SPENDIT Portal Rahmenvertrag und den SpenditCard AGB, für das Produkt Lunchit aus dem SPENDIT Portal Rahmenvertrag und den Lunchit AGB und für das Produkt Mobility aus den spendit AGB. Die hierin enthaltenen Vereinbarungen finden Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

§ 1 Definitionen

(1) **Personenbezogene Daten**: Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person”) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(2) **Personenbezogene Daten des Auftraggebers**: Personenbezogene Daten des Auftraggebers sind personenbezogene Daten, die der Auftragnehmer für den Auftraggeber erhoben hat oder die der Auftraggeber dem Auftragnehmer bereitgestellt hat und die daraus im Rahmen der Verarbeitung resultierenden personenbezogenen Daten.

(3) **Datenverarbeitung oder das Verarbeiten von Daten**: Datenverarbeitung oder das Verarbeiten von Daten bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(4) **Datenverarbeitung im Auftrag**: Datenverarbeitung im Auftrag ist Datenverarbeitung durch den Auftragnehmer im Auftrag des Auftraggebers.

(5) **Weisung**: Eine Weisung erfolgt einerseits durch die Leistungsbeschreibung im Hauptvertrag. Diese ursprüngliche Weisung durch den Hauptvertrag kann durch den Auftraggeber durch zusätzliche

schriftliche Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Alle Weisungen sind vom Auftragnehmer zu dokumentieren.

(6) **Datenschutzvorschriften**: Datenschutzvorschriften meint alle gesetzlichen (Rechts-) Akte der Europäischen Union und/oder ihrer Mitgliedstaaten (insbesondere Gesetze, Richtlinien und Verordnungen) zum Schutz personenbezogener Daten.

(7) **EU**: EU meint die Mitgliedstaaten der Europäischen Union.

§ 2 Gegenstand und Dauer des Auftrags; Umfang, Art und Zweck der Datenverarbeitung

Art der Daten und Kreis der Betroffenen:

(1) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in der Leistungsbeschreibung des Hauptvertrags konkretisiert sind oder zu denen der Auftraggeber dem Auftragnehmer nachträglich eine Weisung erteilt hat.

(2) Die Dauer des Auftrags bestimmt sich nach den Regelungen des Hauptvertrages.

(3) Umfang und Art der Datenverarbeitung bestimmt sich nach der Leistungsbeschreibung des Hauptvertrages in Verbindung mit den Weisungen des Auftraggebers.

(4) Zweck der Datenverarbeitung ist die Erfüllung der in der Leistungsbeschreibung des Hauptvertrages konkretisierten Tätigkeiten durch den Auftragnehmer.

(5) Betroffen von der Verarbeitung sind nachstehende Kategorien von Betroffenen, von denen die gelisteten Arten von Daten verarbeitet werden:

(a) Kategorien der betroffenen Personen:

Auftraggeber (Kunde) und Beschäftigte des Auftraggebers

(b) Art der personenbezogenen Daten:

Stammdaten wie Namensdaten, Adress- und Kommunikationsdaten, Geschäfts- und Vertragsdaten, Abrechnungsdaten, Kontodaten, E-Mail-Adresse, Personalnummer, Geburtsdatum (optional), Eintrittsdatum im Unternehmen (optional), Namenstag (optional), Geschlecht (optional), (IT-) Nutzungsdaten

§ 3 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der allgemeinen und technischen und organisatorischen Maßnahmen zu, die erforderlich sind, um ein den jeweils geltenden Datenschutzvorschriften entsprechende(s) Datenschutzniveau bzw. Datensicherheit zu gewährleisten. Insbesondere wird der Auftragnehmer seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen der jeweils geltenden Datenschutzvorschriften gerecht wird. Dies kann insbesondere folgende Maßnahmen beinhalten:

(a) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten des Auftraggebers verarbeitet werden, zu verwehren (**Zutrittskontrolle**),

(b) zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),

(c) dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten des Auftraggebers zugreifen können, und dass personenbezogene Daten des Auftraggebers bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),

(d) dafür Sorge zu tragen, dass personenbezogene Daten des Auftraggebers bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten des Auftraggebers durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),

(e) dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten des Auftraggebers in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),

(f) dafür Sorge zu tragen, dass personenbezogene Daten des Auftraggebers, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),

(g) dafür Sorge zu tragen, dass personenbezogene Daten des Auftraggebers gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),

(h) dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene, personenbezogene Daten des Auftraggebers getrennt verarbeitet werden können (**Trennungskontrolle**),

(i) dafür Sorge zu tragen, dass personenbezogene Daten des Auftraggebers pseudonymisiert und verschlüsselt werden können;

(j) dafür Sorge zu tragen, dass die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicher- gestellt ist;

(k) dafür Sorge zu tragen, dass die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann;

(l) dafür Sorge zu tragen, dass ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung eingehalten wird.

(2) Der Auftragnehmer hat dem Auftraggeber vor Erteilung des Auftrages eine Beschreibung der technischen und organisatorischen Maßnahmen (im Folgenden „**TOM**“) für diese Auftragsverarbeitung zur Verfügung gestellt. Der Auftragnehmer ist verpflichtet, die TOM zu pflegen und fortlaufend zu überprüfen, zu bewerten und zu evaluieren sowie zu aktualisieren, wobei Änderungen mit dem Auftraggeber schriftlich abzustimmen sind. Die TOM sind als **Anhang 1** Bestandteil dieser Vereinbarung.

(3) Der Auftragnehmer weist dem Auftraggeber die von ihm getroffenen technischen und organisatorischen Maßnahmen auf Anfrage nach; der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch durch Vorlage von Testaten oder Berichten unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung) oder eine geeignete Zertifizierung durch ein IT-Sicherheits- und Datenschutzaudit oder durch ein Datenschutzkonzept erbracht werden.

§ 4 Berichtigung, Sperrung und Löschung / Betroffenenrechte

(1) Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu sperren oder zu löschen. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Sperrung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer wird den Auftraggeber nach Maßgabe der jeweils geltenden Datenschutzvorschriften dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person ("Betroffenenrechte") nachzukommen. Zu den Betroffenenrechten können insbesondere gehören:

(a) Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten;

(b) Recht auf Berichtigung, Löschung und Datenübertragbarkeit;

(c) Widerspruchsrecht und Recht auf nicht ausschließlich automatisierte Entscheidungsfindung im Einzelfall.

§ 5 Kontrollen und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer bestellt schriftlich einen Datenschutzbeauftragten. Datenschutzbeauftragter des Auftragnehmers:

Maximilian Hartung
SECUWING GmbH & Co. KG
Tel.: +49 821 90786450
Fax: +49 821 90786459
E-Mail: epost@datenschutz-agentur.de

(2) Über Änderungen des Datenschutzbeauftragten und/oder von dessen Kontaktdaten wird der Auftragnehmer den Auftraggeber unverzüglich schriftlich informieren.

(3) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befassten Mitarbeiter bei der Aufnahme ihrer Tätigkeit gemäß den jeweils geltenden Datenschutzvorschriften auf das Datengeheimnis auch für die Zeit nach Beendigung dieser Vereinbarung verpflichtet wurden und in die Schutzbestimmungen der jeweils geltenden Datenschutzvorschriften eingewiesen worden sind.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen; Ermittlungen und Maßnahmen der datenschutzrechtlichen Aufsichtsbehörden.

(5) Der Auftragnehmer wird die Einhaltung der datenschutzrechtlichen Bestimmungen in seinem Verantwortungsbereich regelmäßig kontrollieren und gegebenenfalls erforderliche Anpassungen von Regelungen und/oder Maßnahmen zur Durchführung dieses Auftrags vornehmen.

(6) Der Auftragnehmer übermittelt dem Auftraggeber auf Wunsch des Auftraggebers schriftlich

(a) Angaben über Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,

(b) Angaben über die Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,

(c) eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,

(d) Angaben über Empfänger oder Kategorien von Empfängern, denen die personenbezogenen Daten des Auftraggebers mitgeteilt werden können,

(e) die Regelfristen für die Löschung der personenbezogenen Daten des Auftraggebers,

(f) Hinweise auf eine geplante Datenübermittlung in Drittstaaten und

(g) eine Beschreibung, die es ermöglicht, zu beurteilen, ob die technischen und organisatorischen Maßnahmen zur Gewährleistung eines entsprechenden Datenschutzniveaus getroffen wurden.

(7) Der Auftragnehmer wird ein den datenschutzrechtlichen Vorgaben entsprechendes Verzeichnis von Verarbeitungstätigkeiten ("Verfahrensmeldung“) führen und dieses auf Anfrage der zuständigen Aufsichtsbehörde zur Verfügung stellen. Der Auftragnehmer wird den Auftraggeber über etwaige Anfragen der Aufsichtsbehörden unverzüglich informieren. Auskünfte an sonstige Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(8) Der Auftragnehmer wird den Auftraggeber nach Maßgabe der jeweils geltenden Datenschutzvorschriften bei einer etwaig erforderlichen Datenschutz-Folgenabschätzung und Konsultation mit den Aufsichtsbehörden unterstützen.

§ 6 Subunternehmer (Unterauftragsverhältnisse) bzw. Auslagerungsunternehmen

(1) Der Auftragnehmer darf bei der Datenverarbeitung Subunternehmer zu den jeweils genannten Leistungen einschalten. Die eingesetzten Subunternehmer sind im Anhang „Liste der Subunternehmer“ aufgeführt.

(2) Der Auftragnehmer ist berechtigt, Subunternehmer zu beauftragen oder bereits beauftragte zu ersetzen. Der Auftragnehmer wird den Auftraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Subunternehmers informieren. Der Auftraggeber kann gegen eine beabsichtigte Änderung innerhalb angemessener Zeit Einspruch erheben. Erhebt der Auftraggeber Einspruch, wird der Auftragnehmer den betroffenen Subunternehmer nicht beauftragen bzw. ersetzen.

(3) Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden, müssen die vertraglichen Vereinbarungen mit den Subunternehmern so gestaltet werden, dass sie den Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages entsprechen. Dem Auftraggeber sind Kontroll- und Überprüfungsrechte entsprechend § 7 dieser Vereinbarung in diesen Verträgen mit den Subunternehmern in der Weise einzuräumen, dass sie den Auftraggeber, unbeschadet der Verantwortlichkeit des Auftragnehmers für die Subunternehmer, unmittelbar auch gegenüber den Subunternehmern berechtigen. Der

Auftragnehmer ist verpflichtet, dem Auftraggeber auf eine entsprechende Anforderung hin Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen durch die Subunternehmer zu erteilen.

(4) Der Auftragnehmer ist gegenüber dem Auftraggeber für sämtliche Handlungen und Unterlassungen der von Ihm eingesetzten Subunternehmer verantwortlich.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber kann sich nach Anmeldung zu Prüfzwecken in den Betriebsstätten des Auftragnehmers, in welchen die Verarbeitung der personenbezogenen Daten des Auftraggebers stattfindet, zu den üblichen Geschäftszeiten des Auftragnehmers von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse und der für die Auftragsverarbeitung einschlägigen Datenschutzvorschriften überzeugen.

(2) Der Auftragnehmer verpflichtet sich, den Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben und die entsprechenden Nachweise gemäß § 3 Abs. 3 dieser Vereinbarung verfügbar zu machen, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind.

§ 8 Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

(2) Dem Auftragnehmer sind die geltenden datenschutzrechtlichen Melde- bzw. Benachrichtigungspflichten gegenüber Aufsichtsbehörden und Betroffenen, insbesondere deren zeitliche und inhaltliche Vorgaben, bekannt. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers.

(3) Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Melde- bzw. Benachrichtigungspflichten treffen, hat der Auftragnehmer ihn hierbei zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

(4) Der Auftragnehmer hat etwaige Verstöße, einschließlich aller hiermit im Zusammenhang stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen, entsprechend der jeweils geltenden Datenschutzvorschriften zu dokumentieren. Die Dokumentation ist dem Auftraggeber auf Aufforderung unverzüglich herauszugeben.

(5) Der Auftragnehmer hat ein angemessenes Schutzniveau durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen, sicherzustellen.

(6) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

§ 9 Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrens-änderungen sind gemeinsam abzustimmen und zu dokumentieren.

(2) Soweit Weisungen des Auftraggebers Ermessensspielräume enthalten sollten, ist der Auftragnehmer verpflichtet, hierzu die Entscheidung des Auftraggebers einzuholen. Eine eigenständige Ermessensausübung oder Kulanzentscheidung steht dem Auftragnehmer nicht zu.

(3) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Text- form) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben oder ohne eine entsprechende, ausdrückliche und schriftliche Weisung des Auftraggebers an Stellen außerhalb der Mitgliedsstaaten des Europäischen Wirtschaftsraumes übermitteln. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(4) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen die jeweils geltenden Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

§ 10 Löschung von Daten und Rückgabe von Datenträgern

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende oder auf Anforderung dem Auftraggeber übergeben.

§ 11 Subunternehmer außerhalb der EU

(1) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der DSGVO enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

§ 12 Kosten

(1) Der Auftragnehmer trägt alle Kosten, welche Ihm durch die Erfüllung der in dieser Vereinbarung vorgesehenen Verpflichtungen entstehen.

(2) Die Parteien sind sich einig, dass der Auftragnehmer auch für die Erfüllung der in dieser Vereinbarung geregelten Verpflichtungen durch die in dem Hauptvertrag vorgesehene Vergütung entlohnt wird und dass der Auftragnehmer im Hinblick auf diese Vereinbarung keine darüber hinausgehende Vergütung erhält.

§ 13 Sonstiges, Allgemeines

(1) Sollten die personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den personenbezogenen Daten des Auftraggebers bei dem Auftraggeber liegt.

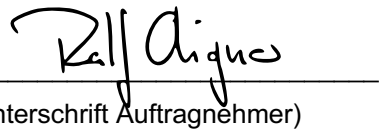
(2) Unbeschadet des Weisungsrechts des Auftraggebers gemäß § 9 dieser Vereinbarung ist der Auftragnehmer berechtigt, dem Auftraggeber Änderungen dieser Vereinbarung sechs Wochen vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens in Textform anzubieten. Die Zustimmung des Auftraggebers gilt als erteilt, wenn er seine Ablehnung nicht vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen angezeigt hat. Auf diese Genehmigungswirkung wird der Auftragnehmer den Auftraggeber in seinem Angebot besonders hinweisen. Im Übrigen können die Bestimmungen dieser Vereinbarung nur durch Vereinbarung in Textform geändert werden.

(3) Die Regelungen dieser Vereinbarung gelten auch nach einer Beendigung des Hauptvertrages bis zur vollständigen Vernichtung oder Rückgabe aller personenbezogenen Daten des Auftraggebers an den Auftraggeber fort.

(4) Im Übrigen gelten die Bestimmungen des Hauptvertrages entsprechend.

_____ _____

(Ort, Datum) (Unterschrift Auftraggeber)

München, 21.02.2023 

(Ort, Datum) (Unterschrift Auftragnehmer)

Anhang 1: Technische und organisatorische Maßnahmen

Anhang 2: Liste der Subunternehmer

SPENDIT AG

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 (1) DSGVO für Auftragsverarbeiter (Art. 30 (2) lit. d DSGVO)

Stand Mai 2020, gültig ab 25.05.2018

Document Revision History

Datum	Version	Erstellt durch	Betrifft	Kommentar
13.05.2020	1.0	S. Kerlin		Erstellung

Inhaltsverzeichnis

1 Hinweise 3

2 Pseudonymisierung 3

3 Verschlüsselung 3

4 Vertraulichkeit 3

4.1 Physikalische Sicherheit 3

4.2 Authentifizierung 4

4.3 Berechtigungskonzept 5

4.4 Weitergabe von Daten 5

4.5 Löschen von Daten 6

4.6 Mandantentrennung 6

5 Integrität 6

5.1 Protokollierung 6

6 Verfügbarkeit 7

6.1 Sicherstellen der Verfügbarkeit 7

6.2 Zweckbindung 7

7 Belastbarkeit der Systeme 8

8 Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder einem technischen Zwischenfall 8

9 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen 9

1 Hinweise

Diese Darstellung der technischen und organisatorischen Maßnahmen kann bis zum 25.05.2018 geändert werden. Ein Grund kann sein, konkrete Empfehlungen der Aufsichtsbehörden zur Darstellung umzusetzen oder sich andere Darstellungen etablieren.

Die getroffenen technischen und organisatorischen Maßnahmen bleiben davon unberührt. Eine Änderung der getroffenen Maßnahmen behält SPENDIT AG sich vor, sofern das Schutzniveau nach DS-GVO nicht unterschritten wird.

2 Pseudonymisierung

Bei Datenanalysen werden die Daten pseudonymisiert und anonym verarbeitet.

3 Verschlüsselung

Regelungsgegenstand:

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbefugte Offenlegung von bzw. unbefugten Zugang zu den im Auftrag verarbeiteten Daten ist zu reduzieren.

Technische und organisatorische Maßnahmen:

Die einzelnen Datenbanken sind verschlüsselt. Der Datenaustausch zwischen den Datenbanken und den Backend-Diensten findet ausschließlich über eine verschlüsselte Kommunikation statt.

Die Arbeitsplatz-Rechner der Mitarbeiter und Datenträger sind standardisiert durch entsprechende Betriebssystemwerkzeuge, jeweils mit dem Verschlüsselungsstandard AES (Advanced Encryption Standard) verschlüsselt.

Das Firmennetzwerk ist durch ein Unified Threat Management System abgesichert. Dieses vereint Firewall, Network Protection, Web Protection, Email Protection und Wireless Protection.

4 Vertraulichkeit

4.1 Physikalische Sicherheit

Regelungsgegenstand:

Unbefugten ist der Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten im Auftrag verarbeitet werden, zu verwehren. Der Grad der Schutzmaßnahmen richtet sich dabei nach dem Grad der Schutzbedürftigkeit der Daten

Technische und organisatorische Maßnahmen:

Die Eingangstür zu den Büroräumen der SPENDIT AG ist mit einer digitalen Schließanlage und einem automatischen Zuzieher ausgestattet. Die Tür ist während der Geschäftszeiten außer zum Betreten und Verlassen geschlossen. Außerhalb der Geschäftszeiten ist die Türe abgesperrt. Die Fenster sind in allen Lagen außerhalb der Geschäftszeiten geschlossen.

Es besteht eine Zugangsbeschränkung für Büro- und Geschäftsräume. Es existiert ein geregelter Ablauf zur Genehmigung, Verwaltung und Löschung von Zutrittsberechtigungen. Die Zutrittsmittel für Mitarbeiter werden ausschließlich an berechtigte Mitarbeiter gegen Nachweis ausgegeben und sofort entzogen, wenn die Berechtigung erlischt. Beim Verlust eines Transponders erfolgt die Deaktivierung des jeweiligen Transponders. Zu- und Abgänge von betriebsfremden Personen werden durch Besucherlisten festgestellt und protokolliert. Betriebsfremden Personen ist der Aufenthalt in allen Büroräumen der SPENDIT AG nur in Anwesenheit und in Begleitung von Mitarbeitern gestattet.

Für das Rechenzentrum gelten die IT-Sicherheitsrichtlinien des jeweiligen Betreibers.

4.2 Authentifizierung

Regelungsgegenstand:

Es muss verhindert werden, dass Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten) von unbefugten Dritten genutzt werden können.

Technische und organisatorische Maßnahmen:

Alle Rechner verfügen über ein Zugangskontrollsystem (UserID (Benutzername), Passwort). Ein Passwortsystem für den Zugriff auf die Datenverarbeitungssysteme ist eingerichtet. Jeder Berechtigte erhält eine individuelle Benutzerkennung und ein persönliches, geheim zu haltendes Passwort, das nicht an Dritte weitergegeben werden darf. Berechtigungen werden regelmäßig kontrolliert. Der Zugriff wird sofort gesperrt, falls die Berechtigung erlischt. Über alle Aktivitäten auf den Datenverarbeitungssystemen werden Protokolle erstellt.

Bildschirmarbeitsplätze sperren sich bei Inaktivität automatisch.

Interne Netze werden nach dem Stand der Technik gegen Zugriffe von außen durch Firewalls und durch Verschlüsselung abgeschottet. Bestimmungsgemäße Zugriffe von außen werden durch Virtual Private Network (VPN) abgesichert.

Daten / Festplatten von mobilen Endgeräten werden verschlüsselt. Private Speichermedien sind durch Organisationsanweisung verboten. Es besteht eine Organisationsanweisung zum Download von Apps auf dienstliche Endgeräte.

Es sind definierte organisatorische und technische Verfahren und Methoden zum Incident-Management umgesetzt.

4.3 Berechtigungskonzept

Regelungsgegenstand:

Die zur Benutzung von IT-Systemen berechtigten Personen dürfen ausschließlich auf die Daten zugreifen, auf die sie die Berechtigungen haben und die sie für die unmittelbare Ausübung ihrer Arbeit benötigen. Im Auftrag verarbeitete Daten dürfen während der Verarbeitung nicht unbefugt kopiert, verändert oder entfernt werden.

Technische und organisatorische Maßnahmen:

Die eingesetzten IT-Systeme haben ein dediziertes Rechtesystem, welche es ermöglicht, Datenzugriffe und -veränderungen auf Basis von Rollen und individuellen Berechtigungen zu vergeben.

Es existiert ein Berechtigungskonzept. Das Berechtigungskonzept umfasst die Verwaltung der Zugriffsrechte durch Systemadministratoren. Die Beantragung, Genehmigung, Vergabe und Rückgabe von Zugriffsberechtigungen ist in einer Organisationsanweisung geregelt.

Der Zugriff auf Computersysteme und Netzlaufwerke ist auf berechtigte Benutzer beschränkt. Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen. Das Erfordernis der Berechtigung wird regelmäßig geprüft.

Die persönliche Verantwortung jedes Mitarbeiters für die Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen wird durch Schulungsmaßnahmen und zentral bereitgestellte Informationen gestärkt.

In den Sicherheitsbereichen gilt ein grundsätzliches Fotografier-Verbot. Das Verbot ist für alle Mitarbeiter verbindlich geregelt, es wird von den Führungskräften überwacht.

4.4 Weitergabe von Daten

Regelungsgegenstand:

Im Auftrag verarbeitete Daten dürfen bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf den Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Technische und organisatorische Maßnahmen:

Alle Mitarbeiter und Fremdpersonal sind verpflichtet, dass Datengeheimnis zu wahren. Datenschutzschulungen für die Mitarbeiter werden regelmäßig durchgeführt.

Die Verbindung zu den Servern von SPENDIT AG findet ausschließlich über eine HTTPS-verschlüsselte Verbindung statt.

4.5 Löschen von Daten

Regelungsgegenstand:

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es der Zweck, für den sie verarbeitet werden, erforderlich ist.

Technische und organisatorische Maßnahmen:

Nicht mehr benötigte Datenträger und Fehldrucke werden datenschutzgerecht entsorgt. Datenträger werden ordnungsgemäß durch physische Zerstörung, Papier durch den Schredder vernichtet.

Die Aufbewahrungsfrist der Daten wird im Rahmen der Beauftragung durch die steuerrechtlichen Vorgaben vorgegeben.

4.6 Mandantentrennung

Regelungsgegenstand:

Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können.

Technische und organisatorische Maßnahmen:

Die Daten werden in einer Datenbank logisch voneinander getrennt. Entwicklungs-, Test- und Produktionssysteme sind getrennt.

5 Integrität

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten ist zu reduzieren.

5.1 Protokollierung

Regelungsgegenstand:

Es sind Maßnahmen zu wählen, mittels derer nachträglich überprüft und festgestellt werden kann, ob und von wem im Auftrag verarbeitete Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische und organisatorische Maßnahmen:

Die Zugriffe auf die datenverarbeitenden Systeme werden über die Logfiles und Systemlogs kontrolliert.

6 Verfügbarkeit

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Nichtverfügbarkeit von im Auftrag verarbeiteten Daten ist zu reduzieren.

Hierzu trifft die SPENDIT AG im Rechenzentrum Maßnahmen, die dazu dienen, dass im Auftrag verarbeitete Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn der Verantwortliche sie benötigt.

6.1 Sicherstellen der Verfügbarkeit

Regelungsgegenstand:

Im Auftrag verarbeitete Daten sind gegen zufällige oder mutwillig herbeigeführte Zerstörung oder Verlust zu schützen.

Technische und organisatorische Maßnahmen:

Hardwareschutz ist durch unterbrechungsfreie Stromversorgung (USV), Feuerlöschgeräte im oder unmittelbar vor dem Serverraum und die Einhaltung der einschlägigen Brandschutzvorschriften gewährleistet.

Die Ausführung arbeitsplatzfremder Software wird durch Spamfilter, Aktualisierung des Betriebssystems und Sicherheitssoftware (Updates und Patches) und Lizenzüberwachung verhindert. Die Ausführung arbeitsplatzfremder Software wird ferner durch technische Maßnahmen verhindert.

Es besteht eine Vertretungsregelung für den Fall der Abwesenheit (Urlaub, Krankheit etc.).

6.2 Zweckbindung

Regelungsgegenstand:

Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Dies gilt insbesondere auch für die Löschung von Daten.

Technische und organisatorische Maßnahmen:

Die Verarbeitung von Auftragsdaten erfolgt ausschließlich entsprechend den produktbezogenen Leistungsvereinbarungen mit dem Auftraggeber. Weisungen zur Verarbeitung und insbesondere zur

Löschung von im Auftrag verarbeiteten Daten werden nur ausgeführt, wenn der Kunde sie in der vertraglich vorgeschriebenen Form erteilt.

7 Belastbarkeit der Systeme

Regelungsgegenstand:

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu im Auftrag verarbeiteten Daten aufgrund von Systemüberlastungen oder -abstürzen ist zu reduzieren.

Technische und organisatorische Maßnahmen:

Um Systemstabilität zu gewährleisten, werden im Rechenzentrum Maßnahmen für eine zuverlässige und zeitgerechte Verarbeitung der Daten getroffen.

Es werden laufende Überwachungen der Nutzung der Dienste und der Auslastung der Systeme durchgeführt. Speicher-, Zugriffs- und Leistungskapazitäten der Systeme und Dienste werden so ausgelegt, dass sie auch an Tagen planerischer Spitzenleistung ohne merkliche Verzögerung von Zugriffs- und Übertragungszeiten genutzt werden können.

Zusätzlich werden folgende Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Belastbarkeit der Datenverarbeitungssysteme eingesetzt:

- Kontrollen durch den Datenschutzbeauftragten
- Penetrationstests durch Dritte

8 Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder einem technischen Zwischenfall

Regelungsgegenstand:

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu diesen durch einen physischen oder technischen Zwischenfall ist zu reduzieren.

Hierzu werden für die Verarbeitung von Daten im Auftrag im Rechenzentrum Maßnahmen für die Systemstabilität getroffen, die dem Anspruch der großen Anzahl von Verantwortlichen und betroffenen Personen an zuverlässig zeitgerechte Verarbeitung ihrer Daten gerecht werden.

Technische und organisatorische Maßnahmen:

Regelmäßige Datensicherungen werden durchgeführt. Sicherungskopien werden in geeigneten zeitlichen Abständen erstellt. Der Datenbestand wird mindestens einmal täglich gesichert.

Daten im Rechenzentrum sind durch den jeweiligen Betreiber geschützt. Dazu gehören Brandschutz, unterbrechungsfreie Stromversorgung und redundante Komponenten.

9 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Regelungsgegenstand:

Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu betreiben.

Technische und organisatorische Maßnahmen:

Ein externer Datenschutzbeauftragter wurde bestellt. Die Wirksamkeit der Maßnahmen wird u. a. durch den Datenschutzbeauftragten der SPENDIT AG laufend geprüft. Der Datenschutzbeauftragte oder von ihm oder der Geschäftsleitung beauftragte Mitarbeiter führen regelmäßig interne Kontrollen der Einhaltung der technischen und organisatorischen Maßnahmen der Datensicherheit durch.

Die vorhandenen Dokumentationen der Datensicherheit werden regelmäßig auf Aktualität geprüft. Es erfolgt mindestens jährlich eine technische Überprüfung der Datenverarbeitungssysteme.

Sicherheitsvorfälle werden dokumentiert und ausgewertet. Für die Sicherheitsvorfälle besteht ein geschultes Krisenteam.

Es erfolgen regelmäßige Audits durch den Datenschutzbeauftragten.

SPENDIT AG

Liste der Subunternehmer

Document Revision History

Datum	Version	Erstellt durch	Betrifft	Kommentar
20.01.2020	1.0	S. Kerlin		Erstellung
13.05.2020	2.0	S. Kerlin		Aktualisierung der Unternehmer
09.07.2020	2.1	S. Kerlin		Aktualisierung Serverstandorte
08.09.2020	2.2	S. Kerlin		Aktualisierung der Unternehmer für das Produkt SpenditCard
10.11.2020	3.0	S. Kerlin		Aktualisierung der Unternehmer für das Produkt SpenditCard
16.05.2023	4.0	S. Kerlin		Aktualisierung der Unternehmer für die Produkte SpenditCard und Mobility

(1) Subunternehmer

Der Auftragnehmer darf bei der Datenverarbeitung die folgenden Subunternehmer zu den jeweils genannten Leistungen einschalten:

(a) Name: Rechenzentrum Amazon-AWS
Adresse: Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855, Luxemburg
Serverstandort: Frankfurt (Deutschland)
Teilleistungen: Hosting der Applikation- und Datenserver

(b) Name: Mailjet GmbH
Adresse: 13-13 bis, rue de l'Aubrac, 75012 Paris, Frankreich,
Serverstandorte: Frankfurt (Deutschland), Saint-Ghislain (Belgien)
Teilleistungen: Übermittlung der produktbezogenen E-Mails

(c) Name: salesforce.com Germany GmbH
Adresse: Erika-Mann-Straße 31-37, 80636 München, Deutschland
Serverstandorte: Frankfurt (Deutschland), Paris (Frankreich)
Teilleistungen: CRM Leistungen im Bereich Sales Cloud, Service Cloud, Pardot

(d) Name: Microsoft Deutschland GmbH, Geschäftsstelle München
Adresse: Walter-Gropius-Straße 5, 80807 München, Deutschland
Serverstandorte: Frankfurt, Berlin (Deutschland), Wien (Österreich), Helsinki (Finnland), Paris, Marseille (Frankreich), Dublin (Irland), Amsterdam, (Niederlande)
Teilleistungen: Leistungen im Bereich Microsoft Office 365

(e) Name: domainfactory GmbH
Adresse: Oskar-Messter-Str. 33, 85737 Ismaning, Deutschland,
Serverstandort: Straßburg (Frankreich)
Teilleistungen: Domain Name System (DNS)-Webservice

(f) Name: netcup GmbH
Adresse: Daimlerstraße 25, 76185 Karlsruhe, Deutschland,
Serverstandort: Nürnberg (Deutschland)
Teilleistungen: Domain Name System (DNS)-Webservice

(g) Name: Atlassian
Adresse: Atlassian. Pty Ltd, Level 6, 341 George Street, Sydney NSW 2000, Australien
Serverstandort: Frankfurt (Deutschland)
Teilleistungen: Service Management-Tool für die Verwaltung von Störfällen, Änderungen, Problemen und Anfragen.

(2) Kooperation im Produkt SpenditCard:

In den Produkten SpenditCard und Mobility sind SPENDIT AG und Solaris SE (Adresse: Solaris SE, Cuvrystraße 53, 10997 Berlin, Deutschland) gemeinsam für die Datenverarbeitung verantwortlich und arbeiten unter einer Kooperationsvereinbarung (Joint Controllership) zusammen, bei der Solaris SE bestimmte Bankdienstleistungen und SPENDIT AG bestimmte technische und betriebliche Dienstleistungen erbringt.

Die Teilleistungen der Solaris SE umfassen insbesondere:

- Die Ausgabe von Zahlungskarten, die nur zur Verfügung über ein bei der Bank erworbenes Guthaben verwendet werden dürfen (Prepaid Cards)
- Die Ausgabe des vorausbezahlten Guthabens als elektronisches Geld (E-Geld)

(3) Zusatzleistungen in den Produkten Mobility Global und Mobility Public

(a) Name: Project Climate GmbH
Adresse: Quellenstraße 7a, 70376 Stuttgart, Deutschland,
Serverstandort: Bielefeld (Deutschland)
Teilleistungen: Kompensation der CO2-Emissionen aus den Mobilitätsaktivitäten bei der Nutzung der spendit Mobility Karten

(4) Zusatzleistungen im Produkt Mobility Deutschlandticket

(a) Name: MoPla Solutions GmbH
Adresse: Alte Landstraße 7, 86502 Laugna
Serverstandort: Frankfurt (Deutschland)
Teilleistungen: Bereitstellung einer Mobilitätsplattform, die in Form einer mobilen Anwendung zugänglich ist und die dazu dient, Angebote des öffentlichen Personennahverkehrs (ÖPNV) an die SPENDIT Nutzer zu vermitteln.