Vereinbarung zur Auftragsverarbeitung

Die SPENDIT AG, Reichenbachstraße 31, 80469 München („Auftragnehmer“) betreibt die Portale https://portal.spendit.de/ und („Portale“).

Der Auftragnehmer hat mit seinem Vertragspartner („Auftraggeber“, gemeinsam mit dem Auftragnehmer „Parteien“) einen „Hauptvertrag“ geschlossen. Der Hauptvertrag beschreibt kumulativ (a) den Nutzungsvertrag, der durch die erfolgreiche Registrierung des Auftraggebers auf dem Portal https://benefitportal.spendit.de/ und Akzeptieren der „Spendit AGB“ oder auf andere Weise zustande kommen kann einschließlich etwaiger bestellter Lizenzen für Benefits im Sinne der Spendit AGB und (b) den „Spendit Portal Rahmenvertrag“ und/oder die einbezogenen „Lunchit AGB“, der durch die erfolgreiche Registrierung auf dem Portal https://portal.spendit.de/ oder auf andere Weise geschlossen werden kann.

Über die Portale kann der Auftraggeber Accounts für Beschäftigte anlegen, Lizenzen erwerben und verwalten. Der Auftragnehmer verarbeitet über die Portale personenbezogene Daten des Auftraggebers.

Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO („Vertrag“).

1. Vertragsgegenstand | Definitionen | Dauer dieses Vertrags

1.1 Der Gegenstand des Auftrags ergibt sich aus dem zwischen den Parteien geschlossenen Hauptvertrag.

1.2 Die in diesem Vertrag verwendeten Begriffe entsprechen ihrer Definition in der DSGVO.

1.3 Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers in dessen Auftrag verarbeiten. Der Auftraggeber ist insoweit Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Der

Auftragnehmer wird als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO für den Auftraggeber tätig.

1.4 Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrages.

2. Konkretisierung des Auftragsinhalts

2.1 Art, Umfang und Zweck der vorgesehenen Verarbeitung ergibt sich aus dem zwischen den Parteien geschlossenen Hauptvertrag und umfasst insbesondere die Bereitstellung der Portale, die es dem Auftraggeber ermöglichen, seinen Beschäftigten Sachleistungen und andere Vergünstigungen zuzuwenden, Accounts für User und Verwalter anzulegen. Daneben kann eine Verarbeitung zum Zwecke der Wartung und zur Erbringung von Support stattfinden.

2.2 Der Auftragnehmer darf die im Rahmen der Auftragsverarbeitung erlangten Daten zu keinen anderen als zu den von diesem Vertrag genannten Zwecken nutzen. Der Auftraggeber erteilt dem Auftragnehmer die Erlaubnis die im Rahmen dieses Vertrags verarbeiteten Daten zu anonymisieren und in dieser Weise zum Zwecke der Verbesserung der Leistungen und des Angebots des Auftragnehmers weiterzuverwenden.

2.3 Die verarbeiten Kategorien von Betroffenen und Kategorien personenbezogener Daten sind in Anhang AV 1 aufgeführt.

2.4 Der Auftraggeber ist berechtigt, die Datenverarbeitungsvorgänge zu konkretisieren und hierauf bezogene Weisungen entsprechend den Regelungen unter 3. zu erteilen.

2.5 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet entweder in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt oder in einem Drittland, soweit die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

3. Weisungsbefugnis des Auftraggebers

3.1 Der Auftragnehmer wird die Verarbeitung der Daten stets nur aufgrund der Weisungen des Auftraggebers vornehmen, es sei denn, er ist zu einer Verarbeitung nach dem EU-Recht oder dem Recht eines EU-Mitgliedsstaates verpflichtet. Die Weisungen des Auftraggebers ergeben sich aus dem Hauptvertrag und können vom Auftraggeber durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

3.2 Weisungen sind vom Auftragnehmer zu dokumentieren. Mündliche Weisungen des Auftraggebers hat dieser unverzüglich in Textform zu bestätigen.

3.3 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

4. Technisch-organisatorische Maßnahmen

4.1 Auftragnehmer und Auftraggeber ergreifen die für die Auftragsdurchführung erforderlichen technischen und organisatorischen Maßnahmen zur Gewährung der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, Art, Umfang und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

4.2 Die im Einzelnen vom Auftragnehmer umzusetzenden Maßnahmen sind im Dokument *„Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 (1) DSGVO für Auftragsverarbeiter (Art. 30 (2) lit. d DSGVO)"* (Anhang AV 2) geregelt.

4.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist der Auftragnehmer berechtigt, auf eigene Kosten die Maßnahmen dem Stand der Technik anzupassen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Änderungen sind zu dokumentieren.

4.4 Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung im Auftrag im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. Das Ergebnis der Kontrollen dokumentiert der Auftragnehmer und stellt diese dem Auftraggeber auf Anforderung zur Verfügung.

5. Anfragen und Rechte von Betroffenen

5.1 Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Kapitel 3 der DSGVO (Rechte der Betroffenen).

5.2 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich insoweit unmittelbar an den Auftragnehmer wendet, wird die betroffene Person unverzüglich darauf hingewiesen, dass das Ersuchen an den Auftraggeber als Verantwortlichen zu richten ist.

6. Sonstige Pflichten des Auftragnehmers

6.1 Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede ihm unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, sie sind zu einer Verarbeitung nach dem EU-Recht oder dem Recht eines EU-Mitgliedsstaates verpflichtet.

6.2 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Die Parteien informierten sich gegenseitig über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

6.3 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 32 bis 36 der DSGVO genannten Pflichten. Hierzu gehören:

6.3.1 die Sicherstellung eines angemessenen Schutzniveaus 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;

6.3.2 die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden, sobald diese dem Auftragnehmer bekannt wird;

6.3.3 die Unterstützung des Auftraggebers bei der Benachrichtigung der betroffenen Person einer Verletzung;

6.3.4 die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;

6.3.5 die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

6.4 Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung (Art. 30 Abs. 2 DSGVO).

6.5 Der Auftragnehmer hat gegenwärtig folgenden Datenschutzbeauftragten bestellt:

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

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

7. Unterauftragnehmer/Dritte

7.1 Der Auftragnehmer stimmt der Hinzuziehung von Unterauftragnehmern zu. Ein Unterauftragnehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unterauftragnehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden. Der Auftragnehmer vereinbart vertraglich mit solchen Dritten angemessene Maßnahmen zur Gewährleistung des Schutzes und der Sicherheit personenbezogener Daten.

7.2 Der Einschaltung der im Dokument „*Liste der Subunternehmer*“ (Anhang AV 3), genannten Unterauftragnehmer stimmt der Auftraggeber bereits jetzt zu.

7.3 Der Auftragnehmer ist verpflichtet, mit eingesetzten Unterauftragnehmer vertragliche Regelungen zu vereinbaren, den Anforderungen des Art. 28 Abs. 2 bis Abs. 4 DSGVO entsprechen. Der Auftraggeber hat das Recht, sich die Einhaltung

dieser Verpflichtung nachweisen zu lassen, gegebenenfalls durch Vorlage der entsprechenden Vertragsdokumente.

7.4 Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

7.4.1 der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit aber mindestens 4 Wochen vorab in Textform anzeigt,

7.4.2 der Auftraggeber nicht binnen vier Wochen in Textform widerspricht und

7.4.3 die Vorgaben nach 7.3 gewahrt sind.

7.5 Im Falle eines Widerspruchs nach 7.4.2, der nicht auf einem legitimen Interesse des Kunden beruht, hat der Auftraggeber die Folgen (z.B. subjektive Unmöglichkeit der Leistungserbringung) und die ggfls. resultierenden Mehrkosten zu tragen, die sich daraus ergeben, dass der Unterauftragnehmer nicht hinzugezogen werden kann. Wenn der Auftragnehmer die im Hauptvertrag geschuldete Leistung aufgrund des Einspruchs nicht oder nur noch mit wirtschaftlich unzumutbarem Aufwand erbringen kann, steht dem Auftragnehmer ein außerordentliches Kündigungsrecht zu.

7.6 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

7.7 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Soweit die Zulässigkeit des Datentransfers von der Durchführung eines *Transfer Impact Assessments (TIA)* abhängt, stellt der Auftragnehmer dem Auftraggeber das Ergebnis der Prüfung zur Verfügung. Jegliche Verlagerung der Verarbeitung durch einen Unterauftragnehmer in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers.

7.8 Eine weitere Auslagerung durch den Unterauftragnehmer ist nur im Rahmen der gesetzlichen Bestimmungen zulässig.

8. Kontrollrechte des Auftraggebers

8.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder von im Einzelfall zu benennenden Prüfern durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die mindestens vier Wochen zuvor schriftlich anzumelden sind, von der Einhaltung dieses Vertrags im Geschäftsbetrieb zu überzeugen.

8.2 Der Auftragnehmer stellt auf Anforderung die erforderlichen Informationen zum Nachweis der in Art. 28 DSGVO niedergelegten Pflichten dem Auftraggeber zur Verfügung und weist die Umsetzung der technischen und organisatorischen Maßnahmen nach. Zum Nachweis können unter anderem dienen, ohne dass die Vorlage der im Folgenden genannten Dokumente für den Auftragnehmer verpflichtend ist:

8.2.1 die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;

8.2.2 die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

8.2.3 aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

8.2.4 eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

8.3 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer eine angemessene Vergütung verlangen, soweit ein nicht nur unerheblicher Aufwand beim Auftragnehmer entsteht.

9. Mitteilungspflichten

9.1 Der Auftragnehmer ist verpflichtet, Verletzungen personenbezogener Daten und Verstöße gegen diesen Vertrag unverzüglich an den Auftraggeber zu melden. Mündliche Meldungen werden in Textform bestätigt. Die Meldung sollte, soweit bekannt, folgende Punkte enthalten:

9.1.1 Den Gegenstand des Verstoßes, sofern möglich über die Kategorien und die Zahl der betroffenen Daten,

9.1.2 die möglichen Folgen des Verstoßes,

9.1.3 die ergriffenen Maßnahmen, mit denen der Verstoß abgestellt werden soll, einschließlich der Maßnahmen zur Schadensminderung und möglichen Maßnahmen.

9.2 Der Auftraggeber verpflichtet sich, den Auftragnehmer unverzüglich über etwaige von ihm erkannte Verstöße gegen die in diesem Vertrag geregelte Auftragsbearbeitung oder gegen sonstige datenschutzrechtliche Vorschriften in Kenntnis setzen.

9.3 Sollten die 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 darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegen.

10. Löschung und Rückgabe von personenbezogenen Daten

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien und notwendige Vervielfältigungen, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Beendigung der vertraglich vereinbarten Auftragsverarbeitung und nach Ablauf der im Hauptvertrag vereinbarten Bereitstellungsfrist hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen und/oder zu vernichten. Der Auftraggeber hat die Möglichkeit, bis Ablauf der Bereitstellungsfrist auf

seine Daten zuzugreifen und diese herunterzuladen. Personenbezogene Daten, die in Backups des Auftragnehmers gespeichert sind und deren Löschung nur mit nicht unerheblichem Aufwand möglich ist, werden im Rahmen der allgemeinen Löschroutine für Backups gelöscht.

10.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben oder nach Ankündigung und Ablauf einer angemessenen Frist löschen.

11. Haftung

11.1 Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.

11.2 Werden im Zusammenhang mit den unter diesen Vertrag fallenden Verarbeitungsvorgängen gegenüber einer Partei Schadenersatzansprüche i.S.v. Art. 82 DSGVO, Geldbußen i.S.v. Art. 83 DSGVO und/oder andere Sanktionen i.S.v. Art. 84 DSGVO angedroht oder geltend gemacht, so informiert diese Partei die andere Partei hierüber unverzüglich in Textform. Die Parteien verpflichten sich, sich bei der Abwehr solcher Ansprüche zu unterstützen.

11.3 Sollten Bußgelder verhängt werden sind die Parteien, sofern nicht abweichend im Einzelfall vereinbart, zur Ausschöpfung sämtlicher Rechtsbehelfe verpflichtet. Entspricht die gegen eine Partei verhängte Geldbuße nicht ihrem internen Anteil an der Verantwortung für den Verstoß, stellt die andere Partei diese Partei hinsichtlich des übersteigenden Anteils von der Geldbuße frei.

12. Kosten

Der Auftragnehmer kann eine angemessene Vergütung für solche Tätigkeiten unter diesen Vertrag zu verlangen, die über die üblichen Leistungen zur Gewährleistung der technischen und organisatorischen Maßnahmen hinausgehen,

einen unverhältnismäßigen Aufwand erfordern und nicht durch den Auftragnehmer verschuldet wurden (etwa Kosten durch Gesetzesänderungen, Behördenanfragen beim Auftragnehmer, Unterstützungsleistungen nach 6.3.4 oder 6.3.5 oder Unterstützungsleistungen aufgrund auftraggeberseitiger und über die Anforderungen hinausgehender Compliance-Anforderungen).

13. Schlussbestimmungen

13.1 Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

13.2 Der Auftragnehmer ist berechtigt, dem Auftraggeber Änderungen dieser Vereinbarung vier 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. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Bei etwaigen Widersprüchen gehen die Regelungen dieses Vertrages den Regelungen des Hauptvertrages vor.

13.3 Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht. Die unwirksame oder undurchführbare Bestimmung gilt als durch eine angemessene und billige Regelung ersetzt, die, soweit gesetzlich zulässig, dem wirtschaftlichen Sinn und Zweck der unwirksamen oder undurchführbaren Bestimmung möglichst nahekommt. Gleiches gilt für den Fall einer ungewollten Lücke.

13.4 Der Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist München.

Anhang AV 1

Kategorien von Betroffenen und Kategorien personenbezogener Daten

Anhang AV 2

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

Anhang AV 3

Liste der Subunternehmer

Kategorien von Betroffenen und Kategorien personenbezogener Daten

Zur Nutzung der Spendit- und Spendit- Partnerprodukte werden im Rahmen dieser Auftragsverarbeitung die folgenden Kategorien von Betroffenen und Kategorien personenbezogener Daten verarbeitet:

- **Auftraggeber:**
  Vor- und Nachname des Hauptansprechpartners und Admins („Account-Verwalter"), Adress- und Kommunikationsdaten, Geschäfts- und Vertragsdaten, Abrechnungsdaten, geschäftliche Bankdaten

- **Beschäftigte des Auftraggebers**
  und sonstige Inhaber von „User-Accounts" oder „Verwaltungs-Accounts":

  Grundlegend für alle Spendit Produkte:
  Vor- und Nachname, geschäftliche E-Mail-Adresse, Personalnummer,
  Postleitzahl, (IT-)Nutzungsdaten, Geschäftsstelle (optional);
  Art des Benefitproduktes (z.B. Lunchit, SpenditCard) und Höhe des Zuschusses

  Zusätzliche Daten zu einzelnen Benefitprodukten:

  Lunchit: Fotografien von Essensbelegen

  SpenditCard: Nummerische Daten persönlicher Anlässe, die vom Auftraggeber festgelegt werden können und zu denen steuerfrei Zuwendungen gewährt werden können (z.B. Geburtstag)

SPENDIT AG

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

Stand Januar 2025, gültig ab 25.05.2018

Document Revision History

Datum	**Version**	**Erstellt durch**	**Betrifft**	**Kommentar**
13.05.2020	1.0	S. Kerlin	Gesamt	Erstellung
21.01.2025	1.1.	A. Lehmann C. Henrichs	Gesamt 1 Hinweis	Überprüfung auf Aktualität Aktualisierung

Inhaltsverzeichnis

1 Hinweise 3

2 Pseudonymisierung 3

3 Verschlüsselung 3

4 Vertraulichkeit 4

4.1 Physikalische Sicherheit 4

4.2 Authentifizierung 5

4.3 Berechtigungskonzept 5

4.4 Weitergabe von Daten 6

4.5 Löschen von Daten 7

4.6 Mandantentrennung 7

5 Integrität 8

5.1 Protokollierung 8

6 Verfügbarkeit 8

6.1 Sicherstellen der Verfügbarkeit 9

6.2 Zweckbindung 9

7 Belastbarkeit der Systeme 10

8 Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder einem technischen Zwischenfall 11

9 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen 11

1 Hinweise

Diese Darstellung der technischen und organisatorischen Maßnahmen kann 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 Sys- temstabilität 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	Gesamt	Erstellung
13.05.2020	2.0	S. Kerlin	1	Aktualisierung der Subunternehmer
09.07.2020	2.1	S. Kerlin	1	Aktualisierung Serverstandorte
08.09.2020	2.2	S. Kerlin	2	Aktualisierung der Subunternehmer für das Produkt SpenditCard
10.11.2020	3.0	S. Kerlin	2	Aktualisierung der Subunternehmer für das Produkt SpenditCard
16.05.2023	4.0	S. Kerlin	1	Erweiterung um die Subunternehmer für die Produkte SpenditCard und Mobility
08.08.2023	5.0	A. Kraus	1	Erweiterung um den Subunternehmer FTAPI Software GmbH
29.07.2025	6.0	C. Henrichs	Gesamt	Änderung der Dokumentenklassifizierung, 1 (a+c) Namensänderung; Entfernen der Subunternehmer domainfactory GmbH, netcup GmbH; Entfernung von Produkt Mobility Global und Mobility Public; Erweiterung um die Subunternehmer QlikTech GmbH, Chargbee Inc., Concentrix Management Holding GmbH

(1) Subunternehmer

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

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

(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, Salesforce Marketing Cloud Account Engagement

(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: 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.

(f) Name: FTAPI Software GmbH
Adresse: Steinstr. 15f, 81369 München, Deutschland
Serverstandort: Frankfurt (Deutschland)
Teilleistungen: Sicherer Daten- und Dateitransfer

(g) Name: Chargebee Inc.
Adresse: 211 South Gulph Road Suite 500, King of Prussia, PA 19406, USA
Serverstandort: Frankfurt (Deutschland)
Teilleistungen: Bereitstellung und Betrieb eines cloudbasierten Subscription-Management-Systems zur Verwaltung von Abonnements, Rechnungen und Zahlungsabwicklungen

(h) Name: QlikTech GmbH
Adresse: Kaistraße 5, 40221 Düsseldorf, Deutschland
Serverstandort: Frankfurt (Deutschland)
Teilleistungen: Bereitstellung von Business-Intelligence-Software zur Datenanalyse und Prozessoptimierung

(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 im Produkt Mobility Deutschlandticket

(a) Name: MoPla Solutions GmbH

Adresse: Alte Landstraße 7, 86502 Laugna, Deutschland

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.

(4) Zusatzleistungen im Produkt Lunchit

(a) Name: Concentrix Management Holding B.V. & Co. KG

Adresse: Rheiner Landstr. 195, 49078 Osnabrück, Deutschland

Serverstandort: Osnabrück (Deutschland)

Teilleistungen: Externe Belegprüfung