



# Vereinbarung

zwischen der

**Kassenärztlichen Vereinigung Westfalen-Lippe**

**Körperschaft des öffentlichen Rechts,**

gesetzlich vertreten durch den

Vorstand

Dr. med. Dirk Spelmeyer

Anke Richter-Scheer

Robert-Schimrigk-Str. 4-6, 44141 Dortmund

- Verantwortlicher - nachstehend Auftraggeber genannt –

und

**<Name und ggf. Rechtsform des Auftragsverarbeiters>,**

gesetzlich vertreten durch

**<Name(n) der Geschäftsvertretung>**

**<Anschrift des Auftragsverarbeiters>**

– im Folgenden Auftragnehmer –



## 1. Gegenstand und Dauer der Vereinbarung sowie Zwecke der Verarbeitung

(1) Diese Vereinbarung zum Datenschutz ist Bestandteil des Vertrages über die Bereitstellung eines Buchungsportals für Dienstreisen inkl. Support (SaaS) vom **<Vertragsdatum>** (im Folgenden: Hauptvertrag) und regelt den Schutz personenbezogener Daten bei der Datenverarbeitung im Auftrag.

(2) Diese Vereinbarung beginnt und endet mit Gültigkeit des Hauptvertrags. Im Übrigen gilt diese Vereinbarung so lange, bis der Auftragnehmer im Auftrag des Auftraggebers alle personenbezogenen Daten unwiderruflich und vollständig gelöscht hat (einschließlich Backups), es sei denn die Daten müssen nach dem für ihn geltenden Recht aufbewahrt werden.

(3) Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Hauptvertrag in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Subunternehmer mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

(4) Der Auftraggeber überträgt dem Auftragnehmer die Durchführung folgender Aufgaben: Bereitstellung eines Buchungsportals für Dienstreisen inkl. Support (SaaS). Der Auftraggeber verfolgt damit das Ziel, erheblich Kosten zu sparen, indem er die Dienstleistungen des Auftragnehmers als eines auf diesem Gebiet spezialisierten Unternehmens in Anspruch nimmt. Davon verspricht sich der Auftraggeber ferner eine hohe Qualität, die immer auf dem neuesten Stand von Recht und Technik gehalten wird. Dabei wird sich der Auftraggeber auf sein Kerngeschäft, fokussieren.

(5) Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten durch den Auftragnehmer sind folgende Datenarten/-kategorien:

☐ Stammdaten Leistungserbringer

☐ Daten elektronische Gesundheitskarte

☐ Honorardaten

☐ Behandlungsdaten

☐ Verordnungsdaten

☐ Personaldaten



☒ Sonstige Daten: Vor- und Nachname, Titel, dienstliche E-Mail-Adresse, dienstliche Telefonnummer, dienstliche oder private Handy-Nummer, Daten der BahnCard, Kostenstelle

(6) Bei den Betroffenen der unter Ziff. 1 (5) aufgelisteten Daten handelt es sich um:

☐ Mitglieder des Auftraggebers (zugelassene Ärzte und Psychotherapeuten)

☐ Patienten/ Versicherte

☒ Mitarbeiter des Auftraggebers

☐ Sonstige:

(7) Die Inhalte dieser Vereinbarung gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(8) Die Auftragsverarbeitung durch den Auftragnehmer wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Auftragsverarbeitung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen des §§ 80 Abs. 2, 35 Abs. 7 SGB X und der Art. 44 ff. DSGVO erfüllt sind.

(9) Grundlage dieser Vereinbarung bilden insbesondere Art. 28 DS-GVO und § 80 SGB X.

## 2. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.



(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen 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, die Implementierungskosten und die Art, der Umfang und die 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 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 2].

(3) Die in der Anlage 2 beschriebenen technisch-organisatorischen Maßnahmen werden regelmäßig hinsichtlich ihrer Wirksamkeit überprüft, bewertet und evaluiert.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber unaufgefordert vorzulegen.

(5) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen schriftlich zur Vertraulichkeit und Wahrung des Sozialgeheimnisses im Sinne des § 35 SGB I unter Hinweis auf die rechtlichen Folgen einer Pflichtverletzung verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

### 3. Berichtigung, Einschränkung und Löschung von Daten

(1) 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 diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

### 4. Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des



- Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. Dies gilt auch für Übermittlungen personenbezogener Daten in ein Drittland.
- b) Soweit ein Datenschutzbeauftragter gemäß den rechtlichen Vorgaben zu benennen ist, werden dessen Kontaktdaten dem Auftraggeber zur Verfügung gestellt (siehe Anlage 1).
  - c) Andernfalls ist ein Ansprechpartner für den Datenschutz beim Auftragnehmer zu benennen. Dessen Kontaktdaten werden dem Auftraggeber zur Verfügung gestellt (siehe Anlage 1).
  - d) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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 Auftraggeber und jede dem Auftragnehmer 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, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
  - e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 2].
  - f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
  - g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
  - h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
  - i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
  - j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 6 dieses Vertrages.



## 5. Unterauftragsverhältnisse

- (1) Subunternehmer dürfen durch den Auftragnehmer grundsätzlich nicht eingesetzt werden.
- (2) Der Auftraggeber kann schriftlich Ausnahmen im Einzelfall zulassen. Die in Anlage 3 genannten Subunternehmer gelten als genehmigt.
- (3) Vorab einer schriftlichen Genehmigung hat der Auftragnehmer dem Auftraggeber Name und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmens mitzuteilen. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung dessen technischer und organisatorischer Maßnahmen gem. Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen sind dem Auftraggeber auf Verlangen zur Verfügung zu stellen. Der Auftragnehmer hat sicherzustellen, dass dem jeweiligen Subunternehmer über eine schriftliche Vereinbarung die Pflichten dieser Vereinbarung auferlegt werden. Der Auftraggeber ist berechtigt, im Bedarfsfall Überprüfungen und Inspektionen – auch vor Ort – bei Subunternehmern selbst oder durch beauftragte Dritte durchzuführen zu lassen. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn die Voraussetzungen dieses Absatzes erfüllt sind. Der Auftragnehmer hat die technischen und organisatorischen Maßnahmen beim Subunternehmer regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren und dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

## 6. Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- (3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
  - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
  - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
  - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
  - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).



## 7. Mitteilungspflichten des Auftragnehmers

(1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder bei ihm beschäftigter Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Feststellungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten des Auftraggebers mit.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören

- a) 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
- b) die Verpflichtung, Verletzungen personenbezogener Daten gem. Art. 33 und 34 DS-GVO unverzüglich an den Auftraggeber zu melden
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung. Hierzu stellt der Auftragnehmer auf Anfrage die notwendigen Dokumentationen zur Durchführung einer Datenschutz-Folgenabschätzung bezogen auf das angebotene standardisierte Produkt zur Verfügung und unterstützt den Auftraggeber in einem angemessenen Umfang bei der weiteren Durchführung.
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

## 8. Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

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

(3) Der Auftraggeber und der Auftragnehmer benennen in Anlage 1 die jeweils Weisungsberechtigten und Weisungsempfänger.





## 9. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten 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.

(3) 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 dem Auftraggeber übergeben.

## 10. Haftung

Jede Partei haftet für den Schaden, den sie durch einen Verstoß gegen diese oder eine weitere Vereinbarung oder eines für sie anwendbaren Datenschutzgesetzes verursacht hat.

## 11. Verschiedenes

(1) Im Falle eines Konflikts zwischen dieser und anderen bestehenden oder zukünftigen Vereinbarungen, zwischen den Parteien soll diese Vereinbarung vorrangig gelten, es sei denn es wird schriftlich anderweitiges verabredet.

(2) Änderungen dieser Vereinbarung bedürfen der Schriftform und müssen zum Ausdruck bringen, dass Regelungen dieser Vereinbarung geändert werden sollen.

(3) Sollte eine Datenschutz-Aufsichtsbehörde, eine Fachaufsicht oder ein Gericht der Meinung sein, dass Regelungen dieser Vereinbarung oder technisch-organisatorische Maßnahmen bzw. deren Fehlens einen Verstoß gegen anwendbare Datenschutzgesetze darstellen, werden die Parteien einvernehmlich Änderungen an dieser Vereinbarung oder den Verarbeitungsaktivitäten vornehmen.

(4) Sollten die Parteien zu keiner einvernehmlichen Änderung dieser Vereinbarung, der technisch-organisatorischen Maßnahmen oder der Datenverarbeitungsaktivitäten in angemessener Zeit (spätestens nach 3 Monaten) gelangen, hat jede Partei das Recht, diese Vereinbarung sowie den zugehörigen Hauptvertrag zu kündigen. Dieses Recht steht dem Auftraggeber auch zu, wenn der Auftragnehmer nicht gewillt ist bzw. es ihm unmöglich ist, Hinweise oder Empfehlungen der Datenschutz-Aufsichtsbehörden oder Fachaufsicht umzusetzen. Keine Partei soll im Falle einer





Kündigung nach diesem Absatz zum Schadenersatz berechtigt sein (z.B. wegen eines entgangenen Gewinns).

(5) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(6) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(7) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

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

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

\_\_\_\_\_  
Unterschrift Auftraggeber

\_\_\_\_\_  
Unterschrift Auftragnehmer



## Anlage 1 – Auflistung Datenschutzbeauftragter und Ansprechpartner

### Datenschutzbeauftragte

Datenschutzbeauftragter des Auftraggebers	Name und Sitz der Firma	Kontaktdaten
Jan Morgenstern	MORGENSTERN consecom GmbH Große Himmels-gasse 1 67346 Speyer	<a href="mailto:datenschutz@kvwl.de">datenschutz@kvwl.de</a> Tel.: 0231 9432-1600

Datenschutzbeauftragte(r) des Auftragnehmers	Name und Sitz der Firma	Kontaktdaten
Bitte angeben.		

### Weisungsberechtigte und Weisungsempfänger

Weisungsberechtigte des Auftraggebers	Name und Sitz der Firma	Kontaktdaten
GB Infrastruktur – Zentrale Beschaffung	KVWL Robert-Schimrigk-Str. 4-6 44141 Dortmund	<a href="mailto:einkauf@kvwl.de">einkauf@kvwl.de</a>

Weisungsempfänger beim Auftragnehmer	Name und Sitz der Firma	Kontaktdaten
Bitte angeben.		



## Anlage 2 – Technisch-organisatorische Maßnahmen

Bitte die TOMs des Auftragnehmers einfügen oder anhängen.



## Anlage 3 – Auflistung der Subunternehmer

Name und Sitz des Subunternehmers	Tätigkeit	Kontaktdaten
Bitte angeben.		