

**Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 der EU-Datenschutz-  
Grundverordnung**

zwischen

Ihnen, als Versicherungsvermittler/Vermittlungsunternehmen und Nutzer des Stuttgarter  
BeratungsNavigators

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

Stuttgarter Lebensversicherung a.G.  
Rotebühlstr. 120  
70197 Stuttgart

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

## **§ 1**

### **Gegenstand und Dauer des Auftrags**

#### **(1) Gegenstand**

Gegenstand des Auftrags zur Datenverarbeitung ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- Bereitstellung der Angebotssoftware Stuttgarter BeratungsNavigator bis zur Einreichung eines Versicherungsantrags

#### **(2) Dauer**

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von einem Monat gekündigt werden.

Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

Nach Beendigung des Auftrags kann keine weitere Nutzung des Stuttgarter BeratungsNavigators durch den Auftraggeber erfolgen.

## **§ 2**

### **Konkretisierung des Auftragsinhalts**

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

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

- Bereitstellung der Angebotssoftware Stuttgarter BeratungsNavigator, die der Auftraggeber zur Verwaltung von Kunden, Berechnung und Speicherung von Versicherungsangeboten, Einreichung von Versicherungsanträgen nutzen kann. Bis zum Zeitpunkt der Übergabe/Einreichung eines Versicherungsantrags beim Auftragnehmer, besteht bezüglich der verarbeiteten Daten ein Auftragsverhältnis im Sinne der DSGVO.
- Bis zum Zeitpunkt der Übergabe/Einreichung von Versicherungsanträgen nimmt der Auftragnehmer außer zur Fehleranalyse und zur Optimierung der Online-Angebote grundsätzlich keinen lesenden Zugriff auf Daten, die im Speicherbereich des Auftraggebers auf den Servern des Auftragnehmers

liegen. Kommt es zur Übergabe/Einreichung eines Versicherungsantrags, kann der Auftragnehmer die zum zugehörigen Antrag gehörenden personenbezogenen Daten, in sein Bestandssystem übernehmen.

## (2) Erbringungsort der Datenverarbeitung

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

## (3) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

Personenstammdaten (z. B. Name, Anschrift, Geburtsdatum);

Kommunikationsdaten (z. B. Telefon, E-Mail);

Antragsdaten;

Akquisedaten;

Vertragsdaten (z. B. Laufzeit, Beitrag);

Abrechnungs- und Zahlungsdaten (z. B. Bankverbindung, Zahlweise, SEPA);

Gesundheitsdaten;

Steuerdaten (z.B. Steuernummer, Lohnsteuerdaten);

Sozialversicherungsdaten;

Daten zu Beruf und Arbeitsverhältnis;

Geschlecht;

Staatsangehörigkeit;

Geldwäschegesetzrelevante Daten (z.B. Identifizierungsdaten)

## (4) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Kunden / Versicherungsnehmer;

(mit)versicherte Personen;

Bezugsberechtigte;

Interessenten;  
Beitragszahler;  
Ehegatte/Kinder des Versicherungsnehmers  
Wirtschaftlich Berechtigte  
Trägerunternehmen  
Ärzte

### **§ 3**

#### **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 oder ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- (2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO, insbesondere i. V. m. Art. 5 DS-GVO, herzustellen. Insgesamt handelt es sich bei den zu treffenden Vorkehrungen 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 dazu sind in der Anlage "Technische und organisatorische Maßnahmen" aufgeführt.
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Daher ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das festgelegte

Sicherheitsniveau nicht unterschritten werden. Wesentliche Änderungen sind vorab mit dem Auftraggeber abzustimmen und anschließend zu dokumentieren.

## **§ 4**

### **Weisungsbefugnis des Auftraggebers**

- (1) Der Auftraggeber ist jederzeit berechtigt, dem Auftragnehmer im Zusammenhang mit der vorgesehenen Verarbeitung von Daten Weisungen zu erteilen. Der Auftragnehmer hat diese Weisungen zu beachten. Das Weisungsrecht des Auftraggebers umfasst neben der Weisung im Einzelfall auch das Recht, allgemeine Leitlinien und generelle Anweisungen für die vorgesehene Verarbeitung von Daten zu erlassen, die vom Auftragnehmer auch an eventuelle Unterauftragnehmer weiterzugeben sind. Mündlich erteilte Weisungen bestätigt der Auftraggeber unverzüglich in Textform (§ 126b BGB).
- (2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist in diesem Fall berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## **§ 5**

### **Berichtigung, Einschränkung und Löschung von Daten**

- (1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach 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. Es wird vereinbart, dass Versicherungsangebote 12 Monate nach der letzten Bearbeitung gelöscht werden.
- (2) Das Löschkonzept sowie das Recht auf Vergessenwerden, Berichtigung,

Datenportabilität und Auskunft sind nach Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

- (3) Der Auftragnehmer hat den Auftraggeber bei der Erfüllung aller bestehenden Pflichten in Bezug auf die Betroffenenrechte nach Kapitel III der DS-GVO zu unterstützen.

## **§ 6**

### **Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

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

- (1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- (2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO ist vom Auftragnehmer sicherzustellen. 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 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.
- (3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen (siehe Anlage) gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO ist von Auftragnehmer zu gewährleisten.
- (4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der

Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

- (5) Der Auftragnehmer hat den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, zu informieren. 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.
- (6) 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.
- (7) Die getroffenen technischen und organisatorischen Maßnahmen sind vom Auftragnehmer gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nachzuweisen.
- (8) Der Auftragnehmer führt ein Verzeichnis von Verarbeitungstätigkeiten, die er im Auftrag des Auftraggebers durchführt. Das Verzeichnis enthält alle in Art. 30 Abs. 2 DS-GVO vorgeschriebenen Angaben. Der Auftragnehmer stellt dem Auftraggeber das Verzeichnis auf Anfrage zur Verfügung.

## **§ 7**

### **Unterauftragsverhältnisse**

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software

von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

- (2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 4 DS-GVO:

| Firma<br>Unterauftragnehmer                                                                                      | Anschrift/Land                                                                                               | Leistung                                                                            |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Stuttgarter Versicherung<br>Holding AG                                                                           | wie<br>Auftragnehmer                                                                                         | Bereitstellung Soft- und<br>Hardware                                                |
| Kyndryl Deutschland<br>GmbH                                                                                      | IBM-Allee 1,<br>71139<br>Ehningen                                                                            | Betrieb Rechenzentrum und<br>Wartungsdienstleistung                                 |
| Microsoft Ireland<br>Operations Limited                                                                          | One Microsoft<br>Place, South<br>County<br>Business Park,<br>Leopardstown,<br>Dublin 18, D18<br>P521, Irland | Email-Server                                                                        |
| Datagroup Stuttgart<br>GmbH                                                                                      | Wilhelm-<br>Schickard-<br>Straße 7,<br>72124<br>Pliezhausen                                                  | Betrieb und<br>Betriebsunterstützung<br>Microsoft Arbeitsplatz<br>und Microsoft 365 |
| Institut für Vorsorge und<br>Finanzplanung GmbH /<br>Software für Vorsorge<br>und Finanzplanung<br>GmbH & Co. KG | Auf der Haide<br>1, 92665<br>Altenstadt a.d.<br>Waldnaab                                                     | Beratungstools                                                                      |
| Versdiagnose GmbH /<br>Franke und Bornberg<br>Research GmbH                                                      | Prinzenstr. 16,<br>30159<br>Hannover                                                                         | Risikoprüfungstool                                                                  |

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



- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich, in Textform oder über den Stuttgarter BeratungsNavigator anzeigt und
  - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
  - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 4 DS-GVO zugrunde gelegt wird.
- (3) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
- (4) Die Weitergabe von personenbezogenen Daten von Kunden oder Mitarbeitern des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

## **§ 8**

### **Kontrollrechte des Auftraggebers**

- (1) Der Auftraggeber hat das Recht, 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

- a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).

## **§ 9**

### **Mitteilung bei Verstößen des Auftragnehmers**

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

- 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 unverzüglich an den Auftraggeber zu melden, insbesondere auch bei Verdacht auf solche Verletzungen;
- c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber der betroffenen Person zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
- d) die Unterstützung des Auftraggebers bei dessen Datenschutz-Folgenabschätzung;
- e) die Unterstützung des Auftraggebers im Rahmen von Konsultationen der Aufsichtsbehörde.

## **§ 10**

### **Löschung und Rückgabe von personenbezogenen Daten**

- (1) Kopien oder Duplikate der Daten werden vom Auftragnehmer 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 Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und Datenträger, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, entsprechend seinem Löschkonzept datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.
- (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.

## **§ 11**

### **Haftung**

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

## **§ 12**

### **Salvatorische Klausel**

Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam sein oder nicht durchgeführt werden können, so wird hierdurch die Wirksamkeit der übrigen Bestimmungen nicht beeinträchtigt. Die Vertragspartner werden in diesem Fall eine der unwirksamen oder undurchführbaren Bestimmung wirtschaftlich

möglichst nahe kommende rechtswirksame Ersatzregelung treffen. Wird keine Ersatzregelung getroffen, tritt an die Stelle der unwirksamen oder undurchführbaren Bestimmung diejenige, die die Parteien bei angemessener Abwägung ihrer Interessen nach Treu und Glauben als redliche Vertragspartner vereinbart hätten, wenn sie Unwirksamkeit oder Undurchführbarkeit der Bestimmung bedacht hätten. Gleiches gilt bei Vorliegen einer Regelungslücke, wenn diese nicht durch Heranziehung des dispositiven Rechts sachgerecht geschlossen werden kann.