Vereinbarung zur Auftrags-verarbeitung nach Art. 28 DSGVO

zwischen

Optica Abrechnungszentrum Dr. Güldener GmbH, Marienstraße 10, 70178 Stuttgart
– nachfolgend: „Auftragnehmer“ –

und

Ihnen als Partei des Vertrages über eine Anbindung an die Telematikinfrastruktur
– nachfolgend: „Auftraggeber“ –
– nachfolgend gemeinsam: „Parteien“ oder jeweils einzeln „Partei“–

Anlage 3 zu den Allgemeinen Geschäftsbedingungen für eine Anbindung an die TI
Stand: 20.10.2022

Vorbemerkung

1.1 Der Auftragnehmer bietet dem Auftraggeber in Kooperation mit Subunternehmern eine Anbindung an die Telematikinfrastruktur („**TI**“) mittels TI-Konnektoren als Software as a Service, Leistungen betreffend den Zugang zur Kommunikation im Medizinwesen („**KIM**“) sowie damit zusammenhängende Dienstleistungen wie Wartung und Support an.
Die Parteien haben dazu einen Vertrag über die Anbindung an die TI („**Hauptvertrag**“) abgeschlossen.

1.2 Die Nutzung des TI-Konnektors durch den Auftraggeber, die Zurverfügungstellung des Zugangs zu KIM sowie damit zusammenhängende Dienstleistungen können zu einer Verarbeitung personenbezogener Daten führen, insbesondere von Daten der Mitarbeiter des Auftraggebers („**Daten des Auftraggebers**“). Für diesen Fall konkretisiert die vorliegende Vereinbarung zur Auftragsverarbeitung („**Vereinbarung**“) die datenschutzrechtlichen Verpflichtungen der Parteien. Sie findet Anwendung auf sämtliche Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers in dessen Auftrag verarbeiten.

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten des Auftraggebers im Zusammenhang mit der Bereitstellung des TI-Konnektors und des Zugangs zu KIM sowie ggf. damit zusammenhängende Dienstleistungen in dessen Auftrag und nach dessen Weisung. Der Auftragnehmer gewährt dem Auftraggeber die Nutzung des TI-Konnektors, den Zugang zu KIM sowie ggf. damit zusammenhängende Dienstleistungen auf der Grundlage des Hauptvertrags. Die im Hauptvertrag vereinbarten Leistungen des

Auftragnehmers beschränken sich auf die Bereitstellung des TI-Konnektors, den Zugang zu KIM sowie ggf. damit zusammenhängende Dienstleistungen nach Maßgabe der Regelungen des Hauptvertrags.

1.2 Im Rahmen der Leistungserbringung hat der Auftragnehmer Zugriff auf personenbezogene Daten der Mitarbeiter des Auftraggebers. In diesem Fall finden die nachfolgenden Bestimmungen Anwendung.

1.3 Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieser Vereinbarung. Eine isolierte Kündigung dieser Vereinbarung ist ausgeschlossen.

2. Konkretisierung des Auftragsinhalts

2.1 Art der Daten und Kreis der Betroffenen
Zur Erbringung der Leistungen nach den Vorgaben des Hauptvertrags verarbeitet der Auftragnehmer folgende Daten des Auftraggebers:

2.1.1 Konnektor as a Service:

Stammdaten Mitarbeiter des Auftraggebers (soweit vorhanden):
Name, Vorname, Titel, Firma/Organisation, Institutskennzeichen (IK), Telematik-ID, IP-Adresse, Optica-Kundennummer, Kundenpasswort für VPN-Profil, Anschrift (Straße, Hausnummer, PLZ und Ort).

Daten von Empfangspersonen:
Name, Vorname, E-Mailadresse, Telefonnummer.

Logging-Daten/Betriebs-Logs des Konnektors:
Vorgänge (Versenden, Registrierung, De-Registrierung, Entsperrung, Anmeldung, Abruf von Informationen) samt Zeitstempel, Informationsobjekt und Ergebnis (kein Fehler, interner Fehler, remote Fehler)

2.1.2 Kommunikation im Medizinwesen

Daten von Kommunikationsteilnehmern:
Name, Vorname, Titel, Organisation, Profession, öffentliche Mailadresse, KIM- Mailadresse & Passwort, Telematik-ID, HBA-Zertifikate, SMC-B-Zertifikate, KIM-Mailadressen von Absendern und Empfängern, Logging-Daten

2.1.3 Wartung und Support:

Name, Vorname, E-Mail-Adresse, Telefonnummer und sonst an den Support jeweils im Einzelfall herangetragene personenbezogene Daten sowie für den Support im Falle von Fernwartungszugriffen einsehbare personenbezogene Daten.

2.1.4 Zu den Betroffenen zählen:

Mitarbeiter des Auftraggebers; Kommunikationsteilnehmer

2.2 Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Daten werden grundsätzlich zur Bereitstellung des TI-Konnektors as a Service, zur Zurverfügungstellung des Zugangs zu KIM sowie unterstützender Wartungs- und Supportleistungen verarbeitet. Umfang, Art und Zweck der Verarbeitung der Daten durch den Auftragnehmer sind im Hauptvertrag und dessen Anlagen konkret beschrieben.

2.3 Ort der Leistungserbringung

Die Verarbeitung der Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Daten unter Einhaltung der Bestimmung dieses Vertrags auch außerhalb der Europäischen Union oder des EWR zu verarbeiten, soweit der Auftragnehmer den Auftraggeber über den Ort der Datenverarbeitung informiert (insbesondere in den Angaben zu Unterauftragnehmern in Anhang 2 dieser Vereinbarung) und die Voraussetzung der Art. 44 ff. DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

3. Weisungsbefugnis des Auftraggebers

3.1 Der Auftragnehmer verarbeitet die Daten ausschließlich in Übereinstimmung mit den getroffenen Vereinbarungen und den Weisungen des Auftraggebers hinsichtlich Art, Umfang, Zweck und Verfahren der Datenverarbeitung.

3.2 Einzelweisungen des Auftraggebers, die von dem im Hauptvertrag geregelten Leistungsumfang wesentlich abweichen und an die Leistungserbringung zusätzliche Anforderungen stellen, die zu finanziellen Mehraufwendungen bei dem Auftragnehmer führen, werden als Antrag auf Leistungsänderung behandelt. Ein Anspruch des Auftraggebers auf Durchführung der Weisung besteht erst nach Zusicherung des Auftraggebers, dem Auftragnehmer den Mehraufwand für die Durchführung seiner Weisung zu erstatten.

3.3 Mündliche Weisungen sind vom Auftraggeber unverzüglich schriftlich zu bestätigen. Der Auftragnehmer dokumentiert Datum, Uhrzeit und Person, welche die mündliche Weisung erteilt hat.

3.4 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche oder sonst einschlägige gesetzliche Vorgaben. Maßgeblich ist hierbei die subjektive Einschätzung des Auftragnehmers, der nicht zu einer Rechtmäßigkeitskontrolle verpflichtet ist. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

4. Technische und organisatorische Maßnahmen

4.1 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass er den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer wird gemäß Art. 28 Abs. 3 lit. c und Art. 32 DSGVO technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den einschlägigen gesetzlichen Anforderungen genügen. Der Auftragnehmer hat Maßnahmen zu treffen, welche die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung dauerhaft sicherstellen. 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 DSGVO zu berücksichtigen.

4.2 Der Auftragnehmer hat die Umsetzung der technischen und organisatorischen Maßnahmen hinsichtlich der Auftragsdurchführung in Anhang 1 dokumentiert. Die technischen und organisatorischen Maßnahmen gelten mit Vertragsschluss als vom Auftraggeber genehmigt. Der Anhang 1 ist Grundlage und Bestandteil dieser Vereinbarung und gilt als Maßstab bei eventuellen Prüfhandlungen des Auftraggebers.

4.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer ist berechtigt, alternative adäquate Maßnahmen umzusetzen, sofern sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

5. Betroffenenrechte

5.1 Der Auftragnehmer hat personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, nur nach dokumentierter Weisung des Auftraggebers zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken. Wendet sich ein Betroffener mit der Forderung nach Berichtigung, Löschung, Einschränkung der Verarbeitung, Auskunft und/oder Datenportabilität unmittelbar an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen. Der Auftragnehmer leitet hierzu den Antrag des Betroffenen unverzüglich an den Auftraggeber weiter und wird diesen auf Weisung im Rahmen seiner Möglichkeiten bei der Bearbeitung des Anliegens des Betroffenen unterstützen.

5.2 Der Auftragnehmer haftet nicht, wenn das Ersuchen des Betroffenen vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird. Die Umsetzung des Löschkonzepts des Auftraggebers sowie der Betroffenenrechte auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft ist nur insoweit durch den Auftragnehmer unmittelbar sicherzustellen, als dies vom vertraglich vereinbarten Leistungsumfang im Hauptvertrag umfasst ist.

6. Weitere Pflichten des Auftragnehmers

6.1 Der Auftragnehmer verarbeitet die Daten des Auftraggebers – vorbehaltlich abweichender Vereinbarungen – nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers, es sei denn das Recht der Europäischen Union oder der Bundesrepublik Deutschland verpflichtet den Auftragnehmer hierzu.

6.2 Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

6.3 Der Auftragnehmer verpflichtet sich, seinen gesetzlichen Kontrollpflichten nachzukommen. Der Auftragnehmer wird insbesondere regelmäßig kontrollieren, ob die Verarbeitung der personenbezogenen Daten des Auftraggebers in Übereinstimmung mit den vertraglichen Vereinbarungen und den Weisungen des Auftraggebers erfolgt sowie ob die Einhaltung, Nachweisbarkeit und Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sichergestellt ist.

6.4 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen sowie unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten des Auftraggebers nach Art. 32 bis 36 DSGVO. Hierzu zählen

6.4.1 die Sicherstellung des vereinbarten Schutzniveaus durch technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, 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,

6.4.2 die Meldepflicht bei Datenschutzverletzungen gemäß Art. 33 DSGVO, soweit diese im Zusammenhang mit der Erfüllung dieser Vereinbarung geschehen,

6.4.3 die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber den von einer Datenschutzverletzung Betroffenen gemäß Art. 34 DSGVO zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen,

6.4.4 die Unterstützung des Auftraggebers bei dessen Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO sowie im Rahmen vorheriger Konsultationen gemäß Art. 36 DSGVO.

6.5 Der Auftragnehmer wird den Auftraggeber über Kontrollhandlungen und Maßnahmen der Datenschutzaufsichtsbehörden informieren, sofern diese Handlungen und Maßnahmen die Verarbeitung von personenbezogenen Daten des Auftraggebers durch den Auftragnehmer zum Gegenstand haben.

7. Verantwortlichkeit und Pflichten des Auftraggebers

7.1 Für die Einhaltung der einschlägigen datenschutzrechtlichen Bestimmungen im Rahmen dieses Vertrages, insbesondere für die Rechtmäßigkeit der Datenübermittlung an den Auftragnehmer, die Rechtmäßigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen im Rahmen dieser Vereinbarung ist allein der Auftraggeber verantwortlich („Verantwortlicher“ im Sinne von Art. 4 Nr. 7 DSGVO). Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtmäßig erbringen kann. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Daten nach Maßgabe dieser Vereinbarung Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen Ansprüchen auf erstes Anfordern freistellen.

7.2 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Ergebnisse der Auftragsleistung feststellt.

7.3 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

8. Kontrollrechte des Auftraggebers

8.1 Der Auftragnehmer stellt gemäß Art. 28 Abs. 3 lit. h DSGVO sicher, dass sich der Auftraggeber von der Einhaltung der gesetzlichen Kontroll- und Prüfpflichten des Auftragnehmers auf eigene Kosten unter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen und des Datenschutzes selbst oder durch einen beruflich zur Verschwiegenheit verpflichteten Prüfer überzeugen kann. Der Auftraggeber benennt einen unabhängigen externen Prüfer in Abstimmung mit dem Auftragnehmer. Der Prüfer darf in keinem Wettbewerbsverhältnis zum Auftragnehmer und/oder dessen Unterauftragnehmer stehen.

8.2 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen mit geeigneten Mitteln nachzuweisen. Dabei kann der Nachweis nach Wahl des Auftragnehmers durch

- die Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO),
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren (Art. 42 DS-GVO),
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzauditoren, Qualitätsauditoren) und/oder
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz, ISO 27001) erbracht werden.

8.3 Weitergehende Überprüfungen, insbesondere Audits, sind nur zulässig, sofern die oben aufgezählten Nachweise nicht ausreichen, um die gesetzlichen Anforderungen an Kontrollen einzuhalten. Hierbei entstehende Kosten sind vom Auftraggeber nach Aufwand gesondert zu vergüten. Sollten im Einzelfall Überprüfungen nach Satz 1 ausnahmsweise erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufes in angemessenen Abständen durchgeführt. Der Auftragnehmer darf diese von einer vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen.

9. Unterauftragnehmer

9.1 Als Unterauftragsverhältnisse im Sinne dieser Vereinbarung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der (haupt-)vertraglich vereinbarten Leistungen beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer bei der Auftragsdurchführung in Anspruch nimmt, z. B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Hausmeister- und Sicherheitsdienste, Reinigungsdienste und Wartungs- und Benutzerservice-Dienstleistungen (letzteres soweit kein Zugriff auf personenbezogene Daten erfolgen kann). Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

9.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragnehmer) mit Zustimmung des Auftraggebers nach Maßgabe der folgenden Regelungen beauftragen:

9.2.1 Der Auftraggeber erklärt hiermit seine Zustimmung (allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 DSGVO), dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen Unterauftragnehmer zur Leistungserfüllung heranzieht bzw. mit (Teil-)Leistungen unterbeauftragt.

9.2.2 Eine Auflistung sämtlicher zum Zeitpunkt des Vertragsschlusses hinzugezogener und vom Auftragnehmer genehmigter Unterauftragnehmer ergibt sich aus Anhang 2.

9.2.3 Der Auftragnehmer wird den Auftraggeber über beabsichtige Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Unterauftragnehmer informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 4 Wochen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diese Vereinbarung mit einer Frist von 3 Monaten zu kündigen.

9.3 In Fällen des betrieblichen Notstands, wie z. B. Serverausfällen mit massiven Auswirkungen auf die Aufrechterhaltung des Geschäftsbetriebs, ist der Auftragnehmer für die Dauer des Bestehens des betrieblichen Notstandes berechtigt, mit ihm verbundene Unternehmen im Sinne des § 15 AktG mit Sitz in der EU oder andere in der EU und dem EWR oder in einem Staat, für den ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO besteht, niedergelassene Unterauftragnehmer ohne Einhaltung des Verfahrens zur Möglichkeit des Einspruchs als Unterauftragnehmer einzusetzen.

9.4 Der Auftragnehmer muss weiteren Unterauftragnehmer gleiche Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieser Vereinbarung obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn dem weiteren Unterauftragnehmer die in Art. 28 Abs. 3 DSGVO festgelegten Mindestpflichten auferlegt sind.

10. Löschung und Rückgabe von Datenträgern

10.1 Der Auftragnehmer ist verpflichtet, nach Abschluss der vertraglich vereinbarten Leistungen oder früher, sofern der Auftraggeber dies anweist und dies vom Weisungsrecht erfasst ist, spätestens aber mit Beendigung des Hauptvertrags, sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzkonform zu löschen bzw. zu vernichten. Gleiches gilt für Test- und Ausschussmaterial sowie ggf. angefertigte Sicherungskopien.

10.2 Eine Pflicht zur Löschung von Daten besteht nicht, soweit der Auftragnehmer gesetzlich, vertraglich oder satzungsmäßig zur Aufbewahrung der personenbezogenen Daten über das Vertragsende hinaus verpflichtet ist. In diesen Fällen sind die Daten erst nach Ablauf der jeweils einschlägigen Aufbewahrungsfristen datenschutzkonform zu löschen. Entsprechend sind Dokumentationen, die dem Nachweis der auftrags- oder ordnungsgemäßen Datenverarbeitung dienen, durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Der Auftragnehmer kann diese Dokumentationen zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

10.3 Trifft der Auftraggeber durch Einzelweisungen weitergehende Vorgaben betreffend der Löschung der Daten, so hat er die dem Auftragnehmer hierbei entstehenden zusätzlichen Kosten zu erstatten.

11. Haftung

Die Haftung des Auftragnehmers bemisst sich nach den Regelungen des Hauptvertrags.

12. Änderungsverfahren

12.1 Der Inhalt dieser Vereinbarung kann bei Bedarf veränderten Umständen angepasst werden. Verfahrensänderungen sind vor ihrer Durchführung gemeinsam abzustimmen. Sie dürfen nicht ohne schriftliche Einwilligung vollzogen werden. Der Verzicht auf dieses Schriftformerfordernis bedarf ebenfalls der Schriftform. Mündlich erteilte Weisungen sind nachträglich schriftlich zu bestätigen.

12.2 Bei lediglich formalen Anpassungen wie dem Wechsel in der Funktion des Datenschutzbeauftragten ist kein schriftlicher Nachtrag erforderlich. Dies gilt auch für Änderungen an den technisch-organisatorischen Maßnahmen beim Auftragnehmer. Dieser übersendet an den Auftraggeber ggf. eine aktualisierte Fassung des Anhang 1.

13. Vertraulichkeit und Geheimnisschutz

13.1 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten die Vertraulichkeit zu wahren.

13.2 Dem Auftragnehmer ist bekannt, dass der Auftraggeber als Heilberufsausübender nach § 203 Abs. 1 Nr. 1 StGB zum Geheimnisschutz verpflichtet ist und die vertrauliche Behandlung ihm anvertrauter oder bekanntgewordener fremder Geheimnisse sicherstellen muss. Die unbefugte Offenbarung von fremden Geheimnissen ist nach § 203 StGB strafbar. Personen, wie der Auftragnehmer, die an der beruflichen Tätigkeit des Auftraggebers mitwirken (sog. mitwirkende Personen), können sich ebenfalls strafbar machen,

- wenn sie unbefugt fremde Geheimnisse offenbaren, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit als mitwirkende Personen bei dem Auftraggeber bekannt geworden sind und/oder
- wenn sie sich einer weiteren mitwirkenden Person bedienen, die unbefugt ein fremdes, ihr bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen haben, dass diese weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

13.3 Der Auftragnehmer verpflichtet sich, dem Geheimnisschutz nach § 203 StGB unterliegenden Informationen vertraulich zu behandeln und nicht unbefugt zu offenbaren.

13.4 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor der Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzrechts und des Strafrechts (Verschwiegenheit) schult und für die Zeit ihrer Tätigkeit wie auch nach Beendigung zur Verschwiegenheit sowie zum Geheimnisschutz verpflichtet (Art. 28 Abs. 3 S. 2 lit. b, Art. 29 DSGVO, § 203 Abs. 4 StGB).

14. Schlussbestimmung

14.1 Änderungen, Ergänzungen und die Aufhebung dieser Vereinbarung bedürfen der Schriftform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses.

14.2 Sollten sich einzelne Bestimmungen dieser Vereinbarung als unwirksam oder undurchführbar erweisen, eine Lücke enthalten oder infolge Rechtsänderungen unwirksam werden, so bleiben die übrigen Bestimmungen dieser Vereinbarung hiervon unberührt. Auftraggeber und Auftragnehmer verpflichten sich, anstelle der unwirksamen Regelung eine solche Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den einschlägigen datenschutzrechtlichen Vorgaben genügt. Entsprechendes gilt für die Ausfüllung von Vertragslücken.

Anhang 1:
Beschreibung der bestehenden technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Maßnahmen, durch die Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

- Lage der Gebäude ist risikoarm. Geringe Angriffswahrscheinlichkeit von außen.
- Auf- und Abschließen der Gebäude bei Arbeitsbeginn bzw. -ende. Protokollierte Schlüsselvergabe.
- Gebäude grundsätzlich mit Alarmanlagen gesichert.
- Zutritt von Mitarbeitern und registriertem Standardwartungspersonal zu Büroflächen nur mittels codierter individueller Tokens.
- Zutritt von anderen Personen (Besucher, Dienstleister etc.) nur nach vorheriger Anmeldung und grundsätzlich ausschließlich in Begleitung von Mitarbeitern.
- Server- und Technikräume nur für Administratoren/Techniker zugänglich. Betrieb der Server in speziellen Sicherheitsräumen.

1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- Zugang zu Systemen und Applikationen durch persönliche Passwörter geschützt.
- Schutz des Netzwerks gegen unerlaubten Zugriff aus dem Internet und gegen Schadsoftware durch Firewall Systeme, Proxy-Server und Antivirensoftware. Alle Zugriffsversuche, zulässige und unzulässige, werden protokolliert.
- Zentrale Datenverarbeitungskomponenten (Server, Datenbanken, Netzwerk etc.) werden grundsätzlich ausschließlich von eigenem Personal administriert.
- Zugriffe werden systemseitig oder durch Tätigkeitsnachweise dokumentiert.

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und personenbezogene Daten bei der Verarbeitung nicht unbefugt kopiert, verändert oder gelöscht werden können:

- Zugang zu Systemen und Applikationen durch persönliche Passwörter geschützt.
- Steuerung der Rechte der einzelnen Benutzer (Datenzugriffe, Funktionsumfang) durch dedizierte Rollen- und Berechtigungskonzepte.
- Systemseitige Schutzmaßnahmen gegen unbefugte Veränderung bzw. Löschung von Daten (Funktionsdeaktivierung, Protokollierung von Änderungen).

- Entsorgung von Akten und elektronischen Datenträgern ausschließlich über zertifizierte Spezialentsorger nach Sicherheitsstufe P4 (DIN 66399).
- Sperrung von Ausgabeschnittstellen.

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Logische Trennung der Daten in den Datenverarbeitungssystemen.
- Mitarbeiter sind angewiesen und geschult, Daten nur im Rahmen der Dienstleistungserbringung und zur Wahrung der Zweckbindung zu verarbeiten.

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen. Pseudonymisierungsverfahren werden insbesondere bei der Speicherung aufbewahrungspflichtiger Daten und bei statistischen Auswertungen angewendet.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Weitergabe personenbezogener Daten nur über verschlüsselte Verbindungen oder Datenträger.
- Die Verschlüsselung erfolgt entsprechend dem Stand der Technik.
- Umfangreiche systemseitige Protokollierung von Datenweitergaben.

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind:

- Umfangreiche systemseitige Protokollierung von Dateneingaben, -veränderungen und -löschungen in Verbindung mit individuellen Benutzerzugängen.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO) / Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Gebäude sind grundsätzlich mit Brandmeldeanlagen ausgestattet.
- Betrieb der Server in speziellen Sicherheitsräumen mit umfangreichem Schutzmaßnahmen (unterbrechungsfreie Stromversorgung (USV), Zutrittsschutz, Brandschottung, automatische Löschanlage, Brandmeldeanlage).
- Zwei räumlich getrennte, redundant ausgelegte Hauptrechenzentren, die im Parallelbetrieb gefahren werden.
- Permanentes, automatisches Monitoring aller wesentlichen Systeme
- Umfangreiche mehrstufige Datensicherungsmaßnahmen.
- Lagerung der Datensicherungen an unterschiedlichen Standorten in gesicherten Bereichen.
- Schutz gegen unerlaubten Zugriff aus dem Internet und gegen Schadsoftware durch doppelte Firewall, Proxy-Server, Netzwerksegmentierung, Antivirensoftware, Zugriffsprotokollierung.
- An ISO 27001 ausgerichtetes Informationssicherheitsmanagementsystem.
- Notfallmanagementsystem und Notfallpläne sind eingerichtet und werden regelmäßig getestet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 2 DSGVO)

4.1 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit).
- Schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsverarbeitungsvertrag) i. S. d. Art. 28 DSGVO.
- Alle Mitarbeiter und sonstige Personen, die Zugriff auf personenbezogene Daten haben, sind schriftlich zur Einhaltung des Datenschutzes verpflichtet.
- Separate Dienstanweisung, die umfassende Anordnungen und Vorgaben zur Wahrung der Datensicherheit und des Datenschutzes am Arbeitsplatz enthält.
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart.
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten.

4.2 Datenschutz-Management

Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

- Bestellung eines Datenschutzbeauftragten.
- An ISO 27001 ausgerichtetes Informationssicherheitsmanagementsystem.
- Regelmäßige und anlassbezogene Sensibilisierung der Mitarbeiter zum Datenschutz.
- Bewertung aller Prozesse in einem Verfahrensverzeichnis, das regelmäßig und anlassbezogen aktualisiert wird.
- Prozesse zur Behandlung und Meldung von potentiellen/tatsächlichen Datenschutzverletzungen eingerichtet und kommuniziert.

4.3 Datenschutzfreundliche Voreinstellungen

Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen Zweck erforderlich ist, verarbeitet werden.

- Zugang zu Systemen und Applikationen durch persönliche Passwörter geschützt.
- Steuerung der Rechte der einzelnen Benutzer (Datenzugriffe, Funktionsumfang) durch dedizierte Rollen- und Berechtigungskonzepte. Mitarbeiter erhalten grundsätzlich nur Zugriff zu den Daten, die für die Arbeit benötigt werden.
- Datenlöschungs- und Datensperrungskonzept.

Anhang 2:
Weitere Unterauftragnehmer

Unterauftragnehmer	Zu erbringende Lesitungen
Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH („**RISE AT**“) Concorde Business Park F 2320 Schwechat Österreich	• Bereitstellung eines TI-Konnektors als Software as a Service • Bereitstellung eines VPN-Zugangs Wartung und Support
Research Industrial Systems Engineering (RISE) Deutschland GmbH (**“RISE DE”**) Invalidenstraße 113 10115 Berlin	• Betrieb KIM-Fachdienst • Wartung und Support
Research Industrial Systems Engineering (RISE) Deutschland GmbH Invalidenstraße 113 10115 Berlin	• Bereitstellung eines TI-Konnektors als Software as a Service • Bereitstellung eines VPN-Zugangs • Betrieb KIM-Fachdienst • Wartung und Support (1st-, 2nd- und 3rd-level) (als Subunternehmer von RISE DE und RISE AT)
Arvato Systems Perdata GmbH Martin-Luther-Ring 7-9 04109 Leipzig Unterauftragnehmer der Arvato Systems Perdata GmbH, gelistet unter www.arvato-systems.de/Sub-Auftragsverarbeiter, sofern diese ihren Sitz in der EU haben.	• Betrieb KIM-Fachdienst • Wartung und Support (2nd- und 3rd-level) (als Subunternehmer von RISE DE)
MEDKONNEKT GmbH Landsberger Straße 155 80687 München	• Betrieb KIM-Fachdienst • Wartung 1st-, 2nd- und 3rd-Level-Support (als Subunternehmer von RISE DE)
ActiveCampaign LLC 1 North Dearborn St 5th Floor Chicago, IL 60602	• E-Mail-Versand im Zusammenhang mit der Ersteinrichtung