

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO (i.V.m. § 80 SGB X)

zwischen

ITSCare – IT-Services für den Gesundheitsmarkt GbR
Saonestraße 3 A
60528 Frankfurt am Main

- Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO, nachstehend **Auftraggeber**
genannt -

und

- Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DS-GVO, nachstehend
Auftragnehmer genannt -

Präambel

- (1) Diese Vereinbarung zur Auftragsverarbeitung regelt die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus

Bezeichnung des Vertrages (z.B. Leistungsvereinbarung, konkrete Beauftragung, OnlineVertrag)	Lieferung von Standard-Software (ggf. mit Pflege)
Vertrags-/Auftragsnummer	IC-GB1-065
Abschlussdatum	

(nachfolgend „Hauptvertrag“) ergeben.

- (2) Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Der Auftragnehmer wird für den Auftraggeber personenbezogene Daten ausschließlich im Rahmen dieser Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO bzw. § 80 SGB X verarbeiten.
- (3) Der Auftraggeber ist eine Arbeitsgemeinschaft gesetzlicher Krankenkassen gemäß § 94 Abs. 1a SGB X in der Rechtsform der GbR und damit eine öffentliche Stelle i.S.d. § 81 Abs. 3 SGB X. Bei der Erfüllung der Leistungsvereinbarung erhebt, verarbeitet und nutzt der Auftragnehmer Sozialdaten und weitere personenbezogene Daten im Auftrag des Auftraggebers auf der Grundlage von § 80 SGB X. Dem Auftragnehmer ist bekannt, dass der Auftraggeber regelmäßig Daten verarbeitet, die einem hohen bis sehr hohem Schutzbedarf nach den Klassifikationen der IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unterliegen.
- (4) Wird im Folgenden der Begriff „personenbezogene Daten“ verwendet, so umfasst dies stets auch Sozialdaten (§ 67 Abs. 1 SGB X i.V.m. § 35 SGB I).

1. Gegenstand, Art und Zweck sowie und Dauer des Auftrages

1.1 Gegenstand

- (1) Der Gegenstand sowie Art und Zweck des Auftrages ergeben sich aus dem Hauptvertrag.
- (2) Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien und/oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungsfristen erforderlich sind.

1.2 Dauer

- (1) Die Gültigkeit dieser Vereinbarung zur Auftragsverarbeitung (Laufzeit) entspricht der Laufzeit des Hauptvertrages bis zur vollständigen Erfüllung und Abwicklung der vereinbarten Leistungen aus der Leistungsbeschreibung.
- (2) Der Auftragnehmer ist nur während der Laufzeit dieser Vereinbarung zur Auftragsverarbeitung und nur soweit es zur Erbringung der vereinbarten Leistung erforderlich ist, zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für den Auftraggeber berechtigt. Jede darüberhinausgehende Verarbeitung dieser personenbezogenen Daten ist nicht gestattet.
- (3) Der Auftraggeber kann den Auftrag jederzeit ohne Einhaltung einer Frist aus wichtigem Grund kündigen. Ein wichtiger Grund liegt insbesondere vor, wenn
 - a. der Auftragnehmer gesetzliche und/oder vertragliche Datenschutzbestimmungen verletzt, oder
 - b. der Auftragnehmer eine gesetzeskonforme Weisung des Auftraggebers nicht ausführen kann oder will, oder
 - c. der Auftragnehmer den Zutritt der durch den Auftraggeber beauftragten Person(en) oder der zuständigen Aufsichtsbehörde zu seinen Geschäftsbereichen ohne wichtigen Grund verweigert, oder
 - d. wenn sich die Grundlage der Vertragserfüllung wesentlich verändert oder ganz entfällt aufgrund einer Änderung der Rechts- oder Gesetzeslage oder wegen aufsichtsrechtlicher Maßnahmen.

2. Konkretisierung des Auftragsinhalts

2.1 Ort der Datenverarbeitung

- (1) 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. Die Übermittlung personenbezogener Daten an Stellen, die weder in einem Mitgliedsstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum ansässig sind (sog. Drittstaat), ist unzulässig.
- (2) In **Anlage 3 (Standortverzeichnis der Geschäftsräume des Auftragnehmers)** sind die Standorte, an denen personenbezogene Daten des Auftraggebers verarbeitet werden, einzutragen. Eine Veränderung der Standorte oder Räumlichkeiten, in denen Daten des Auftraggebers verarbeitet werden, oder ein Verlagern der Auftragsdurchführung an eine andere Örtlichkeit als die mit dem Auftraggeber vereinbarte, bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.

2.2 Art der Daten

- ☐ Gegenstand der Verarbeitung personenbezogener Daten sind im Hauptvertrag konkret beschrieben unter _____.
- ☒ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

(Beispiele: Vor- und Nachname, Anschrift, Kontaktdaten, Bankverbindung, Gehaltsdaten, Steuerdaten, Geburtsdaten)

Alle Arten von personenbezogenen Daten (Beispiel: Vor- und Nachname, Anschrift, Kontaktdaten, Telefondaten, Geburtsdaten etc.) von Mitarbeitern und Kunden des Auftraggebers

2.3 Kategorien betroffener Personen

- ☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind im Hauptvertrag konkret beschrieben unter _____.
- ☒ Die Kategorien der durch die Verarbeitung betroffener Personen umfassen:

(Beispiele: Mitarbeiter des Auftraggebers, Kunden des Auftraggebers)

Mitarbeiter des Auftraggebers, Kunden des Auftraggebers

3. Technisch-organisatorische Maßnahmen

- (1) Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes jederzeit gerecht wird. Der Auftragnehmer ist verpflichtet, durch technische und organisatorische Maßnahmen nach Maßgabe von Art. 28 Abs. 3 lit. c, 32 DS-GVO, i.V.m. Art. 5 Abs. 1, Abs. 2 DS-GVO ein angemessenes Schutzniveau sicherzustellen. Hierbei hat der Auftragnehmer den Stand der Technik, die Umstände und Zwecke der Verarbeitung, die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken, sowie die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen zu ermöglichen. Einzelheiten sind in **Anlage 1 (technisch-organisatorische Maßnahmen)** dieser Vereinbarung beschrieben.
- (2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei dürfen die jeweils aktuellen datenschutzrechtlichen Bestimmungen sowie der jeweils aktuelle Stand der Technik nicht unterschritten werden. Der Auftragnehmer ist verpflichtet, die Dokumentation seiner technischen und organisatorischen Maßnahmen auf dem jeweils aktuellen Stand zu halten und dem Auftraggeber die jeweils aktuelle Version unaufgefordert zur Verfügung zu stellen.
- (3) Der Auftragnehmer kontrolliert regelmäßig seine internen Prozesse sowie seine technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich jederzeit im Einklang mit den Anforderungen dieser Vereinbarung und den einschlägigen gesetzlichen Bestimmungen erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. Der Auftragnehmer ist verpflichtet, diese Kontrollen, die Ergebnisse und ggfs. umgesetzten Maßnahmen vollständig zu protokollieren und für die Dauer von mindestens sechs (6) Jahren aufzubewahren.
- (4) Sämtliche Dokumentationen zu den technischen und organisatorischen Maßnahmen, Dokumentationen von Regelungen zum Datenschutz und zur Informationssicherheit, einschließlich Audit- bzw. Prüfberichte, müssen in deutscher Sprache verfasst bzw. in deutscher Übersetzung bereitgehalten werden.

4. Pflichten des Auftragnehmers

Der Auftragnehmer hat die Einhaltung der Regelungen dieser Vereinbarung sowie der einschlägigen gesetzlichen Pflichten jederzeit nachweisbar zu erfüllen, insbesondere:

- (1) Der Auftragnehmer wird einen Datenschutzbeauftragten, der seine Tätigkeit nach Maßgabe der einschlägigen gesetzlichen Bestimmungen ausübt, benennen. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme in **Anlage 4 (Ansprechpartner)** mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unter Angabe der Kontaktdaten des neuen Datenschutzbeauftragten unverzüglich mitgeteilt. Ist der Auftragnehmer nicht zur Benennung eines Datenschutzbeauftragten verpflichtet, benennt er an dieser Stelle einen Ansprechpartner für datenschutzrechtliche Belange.
- (2) Der Auftragnehmer ist verpflichtet, jederzeit die Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO, § 35 SGB I zu wahren. Der Auftragnehmer setzt bei der Durchführung seiner Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit und zur Geheimhaltung (einschließlich Sozialgeheimnis) unter Hinweis auf die rechtlichen Folgen einer Pflichtverletzung nachweisbar verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Dies umfasst die Verpflichtung zur Geheimhaltung auch über das bestehende Dienst- oder Beschäftigungsverhältnis hinaus. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten des Auftraggebers 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. Ferner stellt der Auftragnehmer sicher, dass das von ihm eingesetzte Personal regelmäßig im Sinne der Datenschutzvorschriften geschult wird.

- (3) Der Auftragnehmer unterstützt den Auftraggeber nach besten Kräften bei der Einhaltung der in den Artikeln 30 bis 36 DS-GVO und §§ 82 bis 84 SGB X genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen.
- (4) Der Auftragnehmer ist verpflichtet, die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen nach Maßgabe von § 3 (Technisch-organisatorische Maßnahmen) dieser Vereinbarung umzusetzen.
- (5) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Soweit der Auftraggeber 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.
- (6) Die Verarbeitung der personenbezogenen Daten des Auftraggebers außerhalb der Geschäftsräume des Auftragnehmers ist nur im nichtöffentlichen Raum und nur mit gesicherten firmeneigenen Geräten des Auftragnehmers zulässig. Es muss sich dabei um jeweils aktuelle verschlüsselte Festplatten, geschützte Verbindungen und fortschrittliche Sicherheitsvorkehrungen, wie z.B. Firewall, handeln, sowie aktuelle Signaturen von Viren- und Malwarescannern. Die Bestimmungen zu den technisch-organisatorischen Maßnahmen nach § 3 (Technisch-organisatorische Maßnahmen) dieser Vereinbarung sind zu beachten.
- (7) Der Auftragnehmer ist nicht berechtigt, an den für den Auftraggeber erhobenen, verarbeiteten und genutzten personenbezogenen Daten oder an den diesbezüglichen Datenträgern ein Zurückbehaltungsrecht gegenüber dem Auftraggeber geltend zu machen.
- (8) Sollte das Eigentum des Auftraggebers beim Auftragnehmer, z.B. durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer ist verpflichtet, alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber zu unterrichten, dass es sich um Daten des Auftraggebers handelt, über die er keinerlei Verfügungs- oder sonstige Bestimmungsgewalt oder Eigentumsrechte hat.
- (9) Der Auftragnehmer verpflichtet sich, dass die Daten des Auftraggebers von Daten anderer Auftraggeber streng getrennt werden. Die Daten des Auftraggebers können mit den Daten anderer Auftraggeber in der gleichen Datenbank gespeichert werden, aber es ist durch logische Trennung und durch entsprechende Applikationslogik sicherzustellen, dass ein anderer Auftraggeber niemals auf Daten des Auftraggebers zugreifen kann.
- (10) 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.
- (11) Der Auftragnehmer führt gemäß Art. 30 Abs. 2 DS-GVO ein Tätigkeitsverzeichnis und stellt dieses dem Auftraggeber auf dessen Aufforderung hin unverzüglich zur Verfügung.

5. Mitteilungs- und Informationspflichten des Auftragnehmers

- (1) Der Auftragnehmer teilt dem Auftraggeber sämtliche Verletzungen des Schutzes personenbezogener Daten, einschließlich des begründeten Verdachts von Datenschutzverletzungen des Auftragnehmers oder der bei ihm Beschäftigten oder von ihm beauftragten Personen gegen Bestimmungen dieser Vereinbarung, gegen einschlägige gesetzliche bestimmungendatenschutzrechtliche Bestimmungen oder gegen die im Auftrag getroffenen Festlegungen unverzüglich mit. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers gegenüber betroffenen Personen oder Aufsichtsbehörden.
- (2) Der Auftragnehmer wird den Auftraggeber über sämtliche Auskunftersuchen von betroffenen Personen oder Dritten, das zugrundeliegende Auftragsverhältnis betreffend, unverzüglich informieren. Der Auftragnehmer selbst darf in diesen Fällen nur nach vorheriger schriftlicher Zustimmung des Auftraggebers Auskunft erteilen, es sei denn, er ist gesetzlich zur Auskunft verpflichtet. Er stellt sicher, dass die Daten von betroffenen Personen bei Bedarf auf Anweisung des Auftraggebers unverzüglich berichtigt, gelöscht oder gesperrt werden können.
- (3) Der Auftragnehmer wird den Auftraggeber über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, unverzüglich 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. Unterauftragsverhältnisse

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen, und bei denen ein Zugriff auf personenbezogene Daten des Auftraggebers nicht ausgeschlossen werden kann. Nicht hierzu gehören Leistungen, die der Auftragnehmer als Nebenleistung zur Hauptleistung beauftragt (sog. ausgelagerte Nebenleistung), wie z.B. Personal-, Post- und Versanddienstleistungen, Telekommunikationsleistungen, Dienstleistungen von Reinigungskräften oder Prüfern. Gleiches gilt für Lieferanten, soweit diese Hardware- oder Standard-Softwareprodukte an den Auftragnehmer bzw. den Unterauftragnehmer ausliefern, ohne diese zu warten (zur Klarstellung: Wartungsleistungen sind Unterauftragnehmerleistungen im Sinne dieser Vorschrift). Der Auftragnehmer ist 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 bzw. darauf hinzuwirken, dass der jeweilige Unterauftragnehmer angemessene und gesetzeskonforme vertragliche Vereinbarungen trifft sowie Kontrollmaßnahmen ergreift.
- (2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragnehmer) mit der Verarbeitung personenbezogener Daten des Auftraggebers nur nach vorheriger schriftlicher Zustimmung des Auftraggebers beauftragen und soweit der Auftragnehmer mit dem Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO, die zudem die in dieser Vereinbarung vereinbarten Rechte und Pflichten berücksichtigt, geschlossen hat.
Wird die Zustimmung ohne datenschutzrechtlich oder sozialrechtlich wesentlicher Grund verweigert, kann der Auftragnehmer die betroffene Leistung kündigen. Kann der Auftragnehmer bei berechtigter Zustimmungsverweigerung trotz angemessener Bemühungen keinen anderen vergleichbaren Unterauftragnehmer einsetzen und die Leistungen nicht ohne die Nutzung des Unterauftragnehmers anbieten, so kann jede Partei die betroffene Leistung kündigen.

- (3) Der Auftraggeber stimmt der Beauftragung der vom Auftragnehmer in **Anlage 2 (Übersicht Unterauftragnehmer)** dieser Vereinbarung aufgeführten Unterauftragnehmer zu, soweit jeweils eine vertragliche Vereinbarung nach Maßgabe von § 6 Absatz 2 dieser Vereinbarung geschlossen wurde. Der Auftragnehmer ist zusätzlich verpflichtet, anzugeben, welche Leistungen die Unterauftragnehmer an welchen Standorten jeweils erbringen.
- (4) Die Beauftragung weiterer Unterauftragnehmer bzw. der Wechsel bestehender Unterauftragnehmer ist zulässig, soweit
 - a) der Auftragnehmer eine solche geplante Unterbeauftragung dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
 - b) der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Unterbeauftragung erhebt und
 - c) eine vertragliche Vereinbarung zwischen dem Auftragnehmer und dem Unterauftragnehmer nach Maßgabe von § 6 Absatz 2 dieser Vereinbarung geschlossen wurde.
- (5) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller gesetzlichen und vertraglichen Voraussetzungen für eine Unterbeauftragung gestattet.
- (6) Eine weitere Auslagerung durch einen Unterauftragnehmer bedarf der vorherigen ausdrücklichen Zustimmung des Auftraggebers mindestens in Textform. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch den weiteren Unterauftragnehmer aufzuerlegen.
- (7) Die vertraglichen Vereinbarungen zwischen Auftragnehmer und Unterauftragnehmer sind so zu gestalten, dass sie den Bestimmungen des Vertragsverhältnisses zwischen Auftraggeber und Auftragnehmer entsprechen. Die vertraglichen Vereinbarungen sowie die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers sind durch den Auftragnehmer nachzuweisen und rechtzeitig vor Abschluss des Vertrages unaufgefordert vorzulegen.
- (8) Wird beim Auftragnehmer die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen und kann dabei der Zugriff auf personenbezogene Daten oder deren Kenntnisnahme durch diese Stellen nicht ausgeschlossen werden, sind dem Auftraggeber rechtzeitig vor der Auftragserteilung die Verträge über Wartungsarbeiten einschließlich der damit Beauftragten mitzuteilen. Sind Störungen im Betriebsablauf zu erwarten oder bereits eingetreten, ist der Vorgang dem Auftraggeber unverzüglich mitzuteilen. Bereits bei Vertragsabschluss bestehende Vertragsbeziehungen sind ebenfalls in **Anlage 2 (Übersicht Unterauftragnehmer)** aufzuführen.
- (9) Beauftragt der Auftragnehmer für den Datentransport ein Transportunternehmen, so hat er vertraglich sicherzustellen und dem Auftraggeber auf Verlangen nachzuweisen, dass der Transportunternehmer die Datenschutzbestimmungen erfüllt und die erforderlichen technischen und organisatorischen Maßnahmen umsetzt. Werden Unterlagen des Auftraggebers abgeholt, stattet der Auftragnehmer den Transportunternehmer mit einem schriftlichen Berechtigungsausweis für die Entgegennahme der Unterlagen aus.
- (10) Der Auftragnehmer wird die Einhaltung der datenschutzrechtlichen Anforderungen beim Unterauftragnehmer regelmäßig überprüfen. Er ist verpflichtet, die Überprüfung zu protokollieren und die entsprechenden Unterlagen mindestens sechs (6) Jahre aufzubewahren.
- (11) Das Verhalten eines Unterauftragnehmers ist dem Auftragnehmer wie eigenes Verhalten zuzurechnen.

7. Kontrollrechte des Auftraggebers

- (1) 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. Der Auftraggeber, bzw. ein von ihm beauftragter Dienstleister, hat das Recht, nach vorheriger Ankündigung (mindestens 14 Tage vorher) zu den üblichen Geschäftszeiten, Überprüfungen durchzuführen. Dies beinhaltet das Recht, sich durch Stichprobenkontrollen, Auskünften zur Vertragsausführung, Einsichtnahmen in die beim Auftragnehmer gespeicherten personenbezogenen Daten des Auftraggebers sowie Einsichtnahmen in die relevanten Datenverarbeitungsprogramme, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- (2) Der Auftragnehmer ist zur Duldung und Unterstützung des Auftraggebers bei dessen Überprüfung verpflichtet. Der Auftragnehmer sichert zu, dass er die notwendige personelle und sachliche Unterstützung bei den Prüfungen zur Verfügung stellt.
- (3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann zudem 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); oder
 - d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz).Die Kontrollrechte des Auftraggebers gemäß § 7 Abs. 1 und 2 dieser Vereinbarung bleiben davon unberührt.
- (4) Aufwände und Kosten, die beim Auftragnehmer im Zuge der Prüfung durch den Auftraggeber entstehen, trägt allein der Auftragnehmer. Eine Kostenverrechnung und -weitergabe an den Auftraggeber oder an vom Auftraggeber zur Durchführung der Prüfung beauftragte Dritte ist ausgeschlossen.
- (5) Die Kontrollrechte des Auftraggebers gelten für sämtliche gegenüber dem Auftraggeber zur Überprüfung berechnete Dritte (z.B. Aufsichtsbehörde) entsprechend. Ggfs. weitergehende Rechte dieser Dritten gegenüber dem Auftragnehmer bleiben unberührt.

8. Weisungsbefugnis des Auftraggebers

- (1) Der Auftraggeber ist berechtigt, dem Auftragnehmer Weisungen im Rahmen der Auftragsverarbeitung zu erteilen.
- (2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. in Textform).
- (3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen einschlägige gesetzliche Bestimmungen. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Wird die Weisung durch den Auftraggeber trotz der durch den Auftragnehmer geäußerten Bedenken bestätigt, ist der Auftragnehmer verpflichtet, diese Weisung unverzüglich umzusetzen.

9. Berichtigung, Einschränkung, Löschung und Rückgabe von Daten

- (1) Der Auftragnehmer darf die Daten, die im Auftrag des Auftraggebers 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 das Löschkonzept, das Recht auf Vergessenwerden, die Berichtigung von personenbezogenen Daten und (soweit einschlägig) die Datenübertragbarkeit nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen und revisionssicher zu dokumentieren.
- (3) Sämtliche Daten und Unterlagen sowie Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit den im Hauptvertrag genannten Leistungen dieser Datenschutzbestimmungen in die Verfügungsgewalt des Auftragnehmers gelangt sind, hat dieser entsprechend der jeweiligen Vereinbarung im Einzelfall bzw. nach Abschluss der vertraglichen Arbeiten dem Auftraggeber auszuhändigen bzw. zu übermitteln.
- (4) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, je nach Weisung des Auftraggebers, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzkonform zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Die Vernichtung von Datenträgern und Unterlagen mit personenbezogenen Daten erfolgt nach Maßgabe der jeweils einschlägigen Schutzklassen und Sicherheitsstufen gemäß ISO/IEC 21964 Teile 1 bis 3 in der jeweils anwendbaren Fassung.
Soweit Nachweise, Zertifizierungen oder Prozessbeschreibungen noch auf die frühere DIN 66399 Bezug nehmen, gelten diese als gleichwertig, sofern sie den Anforderungen der ISO/IEC 21964 entsprechen und ein dem Schutzbedarf angemessenes Vernichtungsverfahren sicherstellen.
Die Vernichtung hat mindestens mit

	Schutzklasse 2 (hoher Schutzbedarf für vertrauliche Daten)
	Schutzklasse 3 (sehr hoher Schutzbedarf für besonders vertrauliche und geheime Daten)

und mindestens Sicherheitsstufe 4 (Datenträger mit besonders sensiblen und vertraulichen Daten) in der jeweils einschlägigen Materialklasse gemäß ISO/IEC 21964 zu erfolgen. Ist eine Löschung auf Sicherungskopien wegen der besonderen Art der Speicherung nur mit einem unverhältnismäßig hohen Aufwand möglich, sind die Daten nach Abstimmung mit dem Auftraggeber für jede weitere Verarbeitung einzuschränken.

- (5) Die datenschutzkonforme Löschung und Vernichtung hat der Auftragnehmer in geeigneter Weise zu protokollieren und dem Auftraggeber unaufgefordert vorzulegen. Im Zweifelsfall sind geeignete Maßnahmen mit dem Auftraggeber abzustimmen. Hinsichtlich sämtlicher Löschvorgänge hat der Auftragnehmer dem Auftraggeber Löschprotokolle zu übergeben.
- (6) Es sind folgende Mindestinhalte für ein Löschprotokoll zu berücksichtigen:
 - a) Datum und Uhrzeit der Löschung,
 - b) das gültige Löschkonzept (Version, Datum),
 - c) die Methode der Datenlöschung (Verfahren),
 - d) das betroffene Verfahren (Beschreibung der zu löschenden Daten),
 - e) die angewandte Löschregel,
 - f) die für die Löschung verantwortliche Person,
 - g) die ausführenden Personen,
 - h) die Anzahl der zu löschenden Daten (Summenprotokolle, Zählreport) und
 - i) die Anzahl der gelöschten Daten (Summenprotokolle, Zählreport, Löschlaufreport).

10. Fernwartung

- (1) Der Auftragnehmer wird bei der Durchführung von Fernwartungsmaßnahmen ausschließlich auf Daten zugreifen, die Gegenstand der vereinbarten Fernwartung und für deren Durchführung zwingend erforderlich sind. Er wird keine Kopien anfertigen. Der Auftragnehmer darf ferner keine eigenen Test- und Wartungsprogramme dauerhaft auf dem fernzuwartenden System ablegen. Eine Speicherung von Daten auf Rechnern außerhalb des Bereiches des Auftraggebers erfolgt nur auf dessen Weisung.
- (2) Der Auftragnehmer wird den mit der Fernwartung betrauten Personen nur die zur Durchführung der konkreten Aufgaben nötigen Berechtigungen erteilen. Der Auftraggeber kann hierfür Vorgaben definieren, die der Auftragnehmer einzuhalten hat.
- (3) Der Auftragnehmer hat die von ihm ergriffenen Fernwartungsmaßnahmen zu dokumentieren, ohne dabei Daten des Auftraggebers zu kopieren, zu speichern oder in sonstiger Form aufzuzeichnen. Auf Anforderung wird der Auftragnehmer dem Auftraggeber im Anschluss an jeden Fernwartungsvorgang die Dokumentation übersenden.
- (4) Das per Fernwartung zu wartende System wird jeweils für jeden Wartungsfall durch den Auftraggeber freigegeben. Dafür wird der Auftraggeber dem Auftragnehmer ein neu vergebenes Zugangskennwort mittels E-Mail zuverlässig verschlüsselt übermitteln. Eine Kommunikation ohne Verwendung sicherer Verschlüsselungsverfahren über ein Netzwerk oder eine Telefonleitung ist nicht gestattet.
- (5) Sofern technisch möglich, erfolgt die Fernwartung innerhalb von Testumgebungen. Eine Fernwartung auf Produktivsystemen erfolgt ausschließlich dann, wenn ein Wartungsziel anderweitig nachweislich nicht erreicht werden kann.
- (6) Wird die Verbindung mehr als zwanzig (20) Minuten vom Auftragnehmer nicht genutzt, wird sie durch den Auftraggeber unterbrochen und bei Bedarf nach dem oben beschriebenen Verfahren erneut hergestellt.
- (7) Vor einem Zugriff auf personenbezogene Daten im Rahmen der Fernwartung holt der Auftragnehmer in jedem Einzelfall die Zustimmung (Textform ausreichend) des Auftraggebers ein. Die elektronische oder die Übertragung personenbezogener Daten auf einen Datenträger an den Auftraggeber erfolgt nur auf Grund dokumentierter Weisung des Auftraggebers.
- (8) Bei der Wartung oder Fernwartung übertragene oder auf Datenträger gespeicherte Daten dürfen ohne vorherige Zustimmung des Auftraggebers nicht an Dritte weitergegeben werden und müssen datenschutzkonform gelöscht werden, sobald sie nicht mehr zur Erfüllung der vertraglich vereinbarten Wartungsarbeiten benötigt werden.
- (9) Der Auftragnehmer gewährleistet, die Fernwartung ausschließlich von Standorten innerhalb der Mitgliedsstaaten der Europäischen Union oder des Europäischen Wirtschaftsraumes aus durchzuführen.
- (10) Der Auftraggeber und der Auftragnehmer dürfen eine Fernwartungsmaßnahme bei Unklarheiten über deren rechtmäßigen Verlauf unverzüglich abbrechen.

11. Haftung

- (1) Der Auftragnehmer haftet gegenüber dem Auftraggeber im Rahmen der gesetzlichen Bestimmungen für Schäden, die infolge schuldhaften Verhaltens gegen Datenschutzbestimmungen und gegen diese Datenschutzvereinbarung entstehen. Ebenso haftet er für schuldhaftes Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer. Die im Hauptvertrag vereinbarten Haftungsregelungen bleiben unberührt.
- (2) Der Auftragnehmer bestätigt, sich gegen die Inanspruchnahme wegen Verletzung von Datenschutzvorschriften hinreichend versichert zu haben und diesen Versicherungsschutz für die gesamte Laufzeit des Hauptvertrages in vollem Umfang aufrechtzuerhalten. Auf Nachfrage des Auftraggebers ist dies durch Vorlage geeigneter Dokumente nachzuweisen.

12. Sonstiges

- (1) Im Falle von Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen die Regelungen dieser Vereinbarung vor.
- (2) Sollten sich datenschutzrechtliche Änderungen während der Vertragslaufzeit ergeben, die zu einer Vertragsanpassung führen müssen, verpflichten sich die Vertragspartner Vertragsverhandlungen mit dem Ziel der Einigung aufzunehmen.
- (3) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Vereinbarungsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit der Vereinbarung im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.
- (4) Es gilt die Gerichtsstandsvereinbarung des Hauptvertrages.
- (5) Änderungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für die Änderung dieser Schriftformklausel.

13. Anlagen

Dieser Vereinbarung zur Auftragsverarbeitung sind folgende Anlagen beigelegt:

Anlage 1 – Technisch-organisatorische Maßnahmen

Anlage 2 – Übersicht Unterauftragnehmer

Anlage 3 – Standortverzeichnis der Geschäftsräume des Auftragnehmers

Anlage 4 – Ansprechpartner

14. Unterschriften

ITSCare – IT-Services für den Gesundheitsmarkt GbR

Frankfurt am Main, den _____

Unterschrift/Firmenstempel

Unterschrift/Firmenstempel

Name in Druckbuchstaben

Name in Druckbuchstaben

Für den Auftragnehmer

_____, den _____

Unterschrift/Firmenstempel

Unterschrift/Firmenstempel

Name in Druckbuchstaben

Name in Druckbuchstaben

Anlage 1 – Technisch-organisatorische Maßnahmen

Der Auftragnehmer verpflichtet sich ein Datenschutz- und Datensicherheitskonzept vorzuhalten. Hierzu hat der Auftragnehmer die im Folgenden aufgeführten technischen und organisatorischen Maßnahmen ergriffen, die als Mindeststandard zwischen den Parteien vereinbart werden und vom Auftragnehmer auf seine Kosten durchzuführen und zu erhalten sind, vgl. Art. 32 Abs. 1 DS-GVO.

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1. Zutrittskontrolle

Im Rahmen der Zutrittskontrolle ist Unbefugten der körperliche Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

(Beispiele: Zugangskontrollsystem, Chipkarten-/Transponder-Schließsystem, Bewegungsmelder, biometrische Zugangssperren, Personenkontrolle am Empfang, Protokollierung der Besucher, sorgfältige Auswahl von Sicherheits- und Reinigungspersonal, Tragepflicht von Mitarbeiter-/Besucherausweisen, Videoüberwachung der Zugänge).

2. Zugangskontrolle

Durch die Zugangskontrolle soll die unbefugte Nutzung von Datenverarbeitungssystemen verhindert werden.

(Beispiele: Authentifizierung mit Benutzername und Passwort, Einsatz von Anti-Viren-Software, Einsatz von Firewalls, Sperrung von externen Schnittstellen, Verschlüsselung von Mobile Devices, Benutzerberechtigungsverwaltung, Passwort-Policy).

3. Zugriffskontrolle

Die Zugriffskontrolle soll gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

(Beispiele: Einsatz von Aktenvernichtern, datenschutzkonforme Vernichtung von Datenträgern, physische Löschung von Datenträgern vor deren Wiederverwendung, Beschränkung von Administratorenrechten, Berechtigungskonzept).

4. Trennungskontrolle

Durch die Trennungskontrolle soll gewährleistet werden, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden.

(Beispiele: Mandantentrennung, Trennung von Produktiv- und Testsystemen, physikalisch getrennte Speicherung).

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Pseudonymisierung soll gewährleisten, dass die Identifizierung der von der Datenverarbeitung betroffenen Person ausgeschlossen bzw. wesentlich erschwert wird.

(Beispiele: Ersetzen von Identifikationsmerkmalen (z.B. Name) durch ein Kennzeichen).

II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

1. Weitergabekontrolle

Die Weitergabekontrolle soll verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft werden kann, an welche Stellen eine Übermittlung personenbezogener Daten erfolgt.

(Beispiele: E-Mail-Verschlüsselung, sichere Transporte, Weitergabe von Daten in anonymisierter oder pseudonymisierter Form, Regelungen zur Datenvernichtung, Taschenkontrollen).

2. Eingabekontrolle

Die Eingabekontrolle soll die Nachprüfbarkeit von Datenverarbeitungsvorgängen gewährleisten, so dass nachträglich festgestellt werden kann, welche personenbezogenen Daten, zu welcher Zeit und von wem in Datenverarbeitungssysteme eingegeben, verändert, gelöscht, usw. worden sind.

(Beispiele: Protokollierung von Eingaben, Änderung und Löschung von Daten).

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1. Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle soll gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust, wie beispielsweise Wasserschäden, Feuerschäden, Stromausfall, geschützt sind.

(Beispiele: Feuerlöschgeräte und Klimaanlage in den Serverräumen, Feuer- und Rauchmeldeanlagen, unterbrechungsfreie Stromversorgung (USV), Notstromaggregate, Aufbewahrung von Datensicherungen an einem sicheren ausgelagerten Ort).

2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Nach einem eingetretenen Datenverlust muss eine rasche Wiederherstellbarkeit der Daten gewährleistet werden.

(Beispiele: Backup- und Recoverykonzept, Notfall- und Katastrophenplan, Durchführung von regelmäßigen Wiederherstellungstests).

IV. Datenschutz-Management

1. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Zur Gewährleistung der Sicherheit der Datenverarbeitung muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der ergriffenen technischen und organisatorischen Maßnahmen implementiert sein.

(Beispiele: interne Kontrollsysteme, externe Prüfungen; Zertifizierungsverfahren, Prüfpläne)

2. Incident-Response-Management; Meldeweg

Es muss gewährleistet sein, dass bei Datenschutzverstößen bzw. bei Verdacht von Datenschutzverstößen der Auftragnehmer unverzüglich den Auftraggeber informiert.

(Beispiele: Darstellung des Meldewegs bei Datenschutzverstößen auf Seiten des Auftragnehmers bzw. Subunternehmers).

3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Durch datenschutzfreundliche Voreinstellungen ist zu gewährleisten, dass nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

(Beispiele: Begrenzung des Verarbeitungsumfangs, Definition von Speicherfristen, Begrenzung der Zugänglichkeit).

4. Auftragskontrolle

Die Auftragskontrolle dient der Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, ausschließlich entsprechend den Weisungen des Auftraggebers verarbeitet werden.

(Beispiele: Vereinbarung von Kontrollrechten beim Auftragnehmer, laufende Kontrollen von Auftragnehmern, sorgfältige Auswahl von Auftragnehmern, Sicherstellung der Einhaltung und Gewährleistung der Datenschutzbestimmungen bei den Auftragnehmern).

Anlage 2 – Übersicht Unterauftragnehmer

Aus dieser Übersicht sollen alle Unterauftragnehmer des Auftragnehmers hervorgehen, welche mit der Verarbeitung der personenbezogenen Daten des Auftraggebers sowie der in diesem Zusammenhang erforderlichen Wartung der eingesetzten automatisierten Verfahren und Datenverarbeitungsanlagen betraut sind.

Unterauftragnehmer	
Firma	
Anschrift	
Ort der Datenverarbeitung	
Leistungsgegenstand	

Unterauftragnehmer	
Firma	
Anschrift	
Ort der Datenverarbeitung	
Leistungsgegenstand	

Unterauftragnehmer	
Firma	
Anschrift	
Ort der Datenverarbeitung	
Leistungsgegenstand	

Unterauftragnehmer	
Firma	
Anschrift	
Ort der Datenverarbeitung	
Leistungsgegenstand	

Unterauftragnehmer	
Firma	
Anschrift	
Ort der Datenverarbeitung	
Leistungsgegenstand	

Unterauftragnehmer	
Firma	
Anschrift	
Ort der Datenverarbeitung	
Leistungsgegenstand	

Unterauftragnehmer	
Firma	
Anschrift	
Ort der Datenverarbeitung	
Leistungsgegenstand	

Ort/Datum

Unterschrift/Firmenstempel des Auftragnehmers

Anlage 3 - Standortverzeichnis der Geschäftsräume des Auftragnehmers

Aus dieser Übersicht sollen alle Standorte der Geschäftsräume des Auftragnehmers hervorgehen, welche für die Verarbeitung von personenbezogenen Daten des Auftraggebers im Rahmen des vereinbarten Auftragsverhältnisses genutzt werden.

Nr.	Bezeichnung Standort	Anschrift	Kontaktdaten

Ort/Datum

Unterschrift/Firmenstempel des Auftragnehmers

Anlage 4 – Ansprechpartner

1. Ansprechpartner des Auftraggebers

Datenschutzbeauftragte(r) (bzw. Verantwortliche(r) für den Datenschutz, soweit die Benennung eines Datenschutzbeauftragten gemäß Art. 37 DS-GVO nicht erforderlich ist):	
Name	Markus Peschko
Kontaktdaten	datenschutz@itscare.de

2. Ansprechpartner des Auftragnehmers

Fachliche(r) Ansprechpartner(in)	
Name	
Funktionsbezeichnung	
Kontaktdaten	

Datenschutzbeauftragte(r) (bzw. Verantwortliche(r) für den Datenschutz, soweit die Benennung eines Datenschutzbeauftragten gemäß Art. 37 DS-GVO nicht erforderlich ist):	
Name	
Kontaktdaten	