Vereinbarung zur Auftragsverarbeitung gem. Art. 28, 29 DSGVO und § 80 SGB X

zwischen dem

Kunden

- nachstehend Auftraggeber genannt -

und der

medicomp

Gesellschaft für neue Medien und Computer mbH

Hoheloogstr. 14
67065 Ludwigshafen

- nachstehend Auftragnehmer genannt -

Präambel

Diese Vereinbarung ergänzt und konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der MIP-Nutzervereinbarung und aus der KIBnet-Nutzervereinbarung - nachfolgend Hauptvertrag genannt - in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben.

Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen personenbezogene Daten des Auftraggebers durch Mitarbeiter des Auftragnehmers oder durch vom Auftragnehmer Beauftragte verarbeitet werden.

Diese Vereinbarung ist eine Anlage zu den Allgemeinen Geschäftsbedingungen des Auftragnehmers und gilt als Anlage zum Hauptvertrag, sofern abweichende Regelungen getroffen wurden.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand
Der Auftragnehmer als Dienstleistungsunternehmen und Systemhaus übernimmt für den Auftraggeber folgende Aufgaben:

Die Abwicklung von elektronischen Kostenvoranschlägen, Genehmigungen und Aufträgen zwischen Kostenträgern und Leistungserbringern und die Verarbeitung aller hierfür erforderlichen Daten mit Hilfe der Onlineplattform MIP-Hilfsmittel-Management.

Erfassung und Verarbeitung statistischer Daten zu leistungsbezogenen Merkmalen von Hilfeempfängern (Klienten) in pseudonymisierter Form in den KIBnet-Modulen (gemäß Art 4, Absatz 5 DSGVO) sowie Erfassung personenbezogener Daten der Hilfeempfänger (Klienten) (gemäß Art. 9 Abs. 3).

Erfassung von Mitarbeiterdaten der Leistungserbringer (Mitarbeitende in den Beratungsstellen) zwecks Zuordnung zu den erfassten Statistikdaten in den KIBnet-Modulen.

Erfassung von Kontaktdaten der Ansprechpartner des Trägers einer Beratungsstelle (für Abrechnungszwecke) in den KIBnet-Modulen.

(2) Dauer
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages und ist an diesen gekoppelt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Aus dem Hauptvertrag ergeben sich Gegenstand und Dauer des Auftrags, sowie Art und Zweck der vorgesehenen Verarbeitung von Daten.

- Der Umfang der Tätigkeiten des Auftragnehmers ergeben sich aus dem Hauptvertrag. Die gesetzliche Grundlage für die Auftragsverarbeitung ist dieser Vertrag gem. Art. 28 DSGVO und § 80 SGB X sowie der § 302 SGB V.

- Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt.

(2) Art der Daten
- Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:
    - Personenbezogene Daten gem. Art. 4 Nr. 1 DSGVO
    - Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO
    - Sozialdaten gem. § 67 Abs. 1 SGB X
    - Daten, die für eine Genehmigung von Leistungen bzw. Hilfsmitteln durch die Kostenträger erforderlich sind

(3) Kategorien betroffener Personen

- Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
    - Mitarbeiter von Leistungserbringern (Kontaktdaten)
    - Leistungserbringer (Kontaktdaten)
    - Kundendaten von Kunden (gesetzliche bzw. privat versicherte Bürger der Bundesrepublik Deutschland bzw. ausländische Staatsbürger deren Daten in der BRD registriert sind – betroffene Personen im Sinne des Art. Nr. 1 DSGVO)

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/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 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

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

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung

folgender Vorgaben:

- Schriftliche Bestellung, soweit nach DSGVO bzw. BDSG-Neu erforderlich, eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.
- Datenschutzbeauftragter des Auftragnehmers ist: Herr Joachim Kramer, Datenschutz Kramer OHG, Elsternweg 24, 42555 Velbert, info@datenschutz-kramer.de
- Ein Wechsel des Datenschutzbeauftragten wird ggf. dem Auftraggeber unverzüglich mitgeteilt.
- Dessen jeweils aktuelle Kontaktdaten sind ggf. auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit, auf das Sozialgeheimnis gemäß § 35 SGB I und für die Fälle der Einbeziehung des § 203 StGB in das Vertragsverhältnis auf die Schweigepflicht nach § 203 StGB 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.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO.
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- 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.
- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu erstehen, 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.

- 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 oder in Textform 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. 2-4 DSGVO zugrunde gelegt wird.

Zurzeit gibt es keine Untervertragsverhältnisse.

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

(4) 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.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen schriftlichen Zustimmung des Auftraggebers sowie des Hauptauftragnehmers. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte und Pflichten des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann

erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz oder DIN-ISO 27001).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Dieser darf die tatsächlich entstandenen Kosten nicht überschreiten.

(5) Der Auftraggeber hat seinen Pflichten gegenüber dem Betroffenen gemäß Art. 13 DSGVO nachzukommen und dem Betroffenen mitzuteilen, dass der Auftragnehmer in die Verarbeitung der Daten involviert ist. Ferner ist der Auftraggeber verpflichtet, bei nicht gesetzlich versicherten Betroffenen eine Einwilligungserklärung, gemäß Art. 6 Abs. 1 und Art. 7, des Betroffenen einzuholen. Diese hat er dem Auftragnehmer auf Anfrage zur Verfügung zu stellen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.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
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Schriftform.

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

10. Löschung und Rückgabe von personenbezogenen Daten

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

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ausgenommen von dieser Regel sind Daten, die der Auftragnehmer zur Wahrung der gesetzlichen Aufbewahrungsfristen nicht löschen darf.

(3) Daten, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder der Vertragserfüllung der Auftragsverarbeitung eines weiteren Auftraggebers (i.d.R. des Kostenträgers) dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen oder den vertraglichen Regelungen zur Auftragsverarbeitung des weiteren Auftraggebers (i.d.R. des Kostenträgers) über das Vertragsende hinaus aufzubewahren.

Anlage – Technisch-organisatorische Maßnahmen

Eine Dokumentation der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO ist Bestandteil dieses Auftrags und kann beim Auftragnehmer in aktueller Form angefordert werden. Bei Abschluss dieser Vereinbarung wurden die technischen und organisatorischen Maßnahmen durch den Auftraggeber oder durch eine von ihm bevollmächtigten Personen kontrolliert und für ausreichend befunden. Diese zum Datenschutz getroffenen Maßnahmen unterliegen dem technischen Fortschritt und werden somit fortlaufend aktualisiert.