Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

[Abrufende Stelle (Bedarfsträger oder MD-IT GmbH) gemäß der Leistungsbeschreibung des jeweiligen Fachloses]
[Anschrift]

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

[Auftragnehmer]
[Anschrift]

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem zwischen Auftraggeber und Auftragnehmer auf Grundlage der Rahmenvereinbarung „[Bezeichnung der Ausschreibung/Rahmenvereinbarung]“ geschlossenen Einzelvertrag einschließlich der für das jeweils in Anspruch genommene Fachlos geltenden Leistungsbeschreibung einschließlich ihrer Anlagen. Einzelvertrag und Leistungsbeschreibung werden nachfolgend gemeinsam als „Leistungsvereinbarung“ bezeichnet.

Die Leistungsvereinbarung konkretisiert den Gegenstand der beauftragten Leistung sowie Art und Zweck der konkreten Verarbeitung, soweit diese Angaben nicht bereits in diesem Vertrag enthalten sind. Bei Widersprüchen zwischen diesem Vertrag und der Leistungsvereinbarung gehen die Regelungen dieses Vertrages vor. Strengere oder konkretisierende Anforderungen der Leistungsvereinbarung, insbesondere zu Melde-, Reaktions-, Lösch- und Unterstützungsfristen sowie zu technischen und organisatorischen Anforderungen, bleiben unberührt.

Auf dieser Grundlage erbringt der Auftragnehmer die beauftragten Leistungen gegenüber dem Auftraggeber. Dieser Vertrag regelt die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DS-GVO. Soweit die konkrete Verarbeitung Sozialdaten umfasst und § 80 SGB X auf den Auftraggeber und die Verarbeitung Anwendung findet, gelten ergänzend die sozialdatenschutzrechtlichen Anforderungen.

(1a) Begriffe und Rolle der MD-IT GmbH

„Auftraggeber“ im Sinne dieses Vertrages ist der vorstehend genannte Verantwortliche, also die abrufende Stelle, die den Einzelvertrag geschlossen hat; ruft die MD-IT GmbH Leistungen für sich selbst ab, insbesondere die Grundleistung des Fachloses 3, ist sie Auftraggeber im Sinne dieses Vertrages. In der Leistungsvereinbarung bezeichnet „Auftraggeber“ dagegen die MD-IT GmbH als Auftraggeberin der Rahmenvereinbarung. Soweit die Leistungsvereinbarung der MD-IT GmbH in dieser Rolle Rechte einräumt, insbesondere Prüf- und Auditrechte, die Entgegennahme von Anzeigen über Änderungen und neue Unterauftragnehmer sowie das Recht, die Übernahme einer Änderung abzulehnen oder aufzuschieben, bestehen diese Rechte neben den Rechten des Auftraggebers nach diesem Vertrag; die Vorrangregel nach Absatz (1) steht dem nicht entgegen. Personenbezogene Daten erhält die MD-IT GmbH auf dieser Grundlage nicht. Sollen bedarfsträgerübergreifende Auswertungen, die die MD-IT GmbH nach der Leistungsvereinbarung im Auftrag der Bedarfsträger durchführt, personenbezogene Daten umfassen, schließen die MD-IT GmbH und der jeweilige Verantwortliche hierüber vor deren Beginn eine eigene Vereinbarung nach Art. 28 DS-GVO.

(2) Dauer

Die Dauer dieses Auftrags entspricht der Laufzeit der vertraglichen und leistungsbezogenen Grundlagen, auf denen die Leistungserbringung des Auftragnehmers gegenüber dem Auftraggeber beruht.

Der Auftragsverarbeitungsvertrag endet spätestens mit dem Zeitpunkt, zu dem die rechtliche Grundlage für die Leistungserbringung des Auftragnehmers gegenüber dem Auftraggeber entfällt, ohne dass es einer gesonderten Kündigung dieses Vertrages bedarf.

Gesetzliche Aufbewahrungs-, Nachweis- und Dokumentationspflichten bleiben hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck

Art und Zweck der Verarbeitung personenbezogener Daten sowie, soweit einschlägig, Sozialdaten und Betriebs- und Geschäftsgeheimnisse durch den Auftragnehmer für den Auftraggeber bestimmen sich nach der Leistungsvereinbarung.

Die konkrete Leistungsvereinbarung betrifft folgendes Fachlos (Zutreffendes ankreuzen):

☐ Fachlos 1 – KI-gestützte Lösung zur fallbezogenen Zusammenfassung als vom Auftragnehmer betriebener Dienst einschließlich Anbindung, Einführung, Schulung, Support und Pflege

☐ Fachlos 2 – Compliance, Informationssicherheit, Penetrationstests und KI-Governance einschließlich Unterstützungsleistungen beim Aufbau und Betrieb eines Managementsystems

☐ Fachlos 3 – Softwarelösung zur Führung von Managementsystemen als vom Auftragnehmer betriebener Dienst einschließlich Hosting, Administration, Support, Pflege und Weiterentwicklung sowie produktbezogener Beratung und Entwicklungsleistungen zur Anpassung der Standardkonfigurationen

Bei Fachlos 2 wird dieser Vertrag nur geschlossen, soweit die konkrete Leistungsvereinbarung eine Verarbeitung personenbezogener Daten im Auftrag umfasst. Soweit Sozialdaten im Auftrag verarbeitet werden und § 80 SGB X einschlägig ist, erfolgt die Verarbeitung nach Maßgabe dieser Vorschrift.

Eine Verarbeitung personenbezogener Daten zu eigenen Zwecken des Auftragnehmers ist ausgeschlossen.

(2) Art der Daten

Gegenstand der Verarbeitung sind die für den jeweiligen Einzelauftrag erforderlichen personenbezogenen Daten. Sozialdaten im Sinne des § 67 SGB X sowie besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO sind nur umfasst, soweit dies für den jeweiligen Einzelauftrag vorgesehen und rechtlich zulässig ist.

Folgende Datenarten/-kategorien sind Gegenstand der Verarbeitung (Zutreffendes ankreuzen; Mehrfachauswahl möglich):

☐ Sozialdaten im Sinne des § 67 SGB X

☐ Gesundheitsdaten und sonstige besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO

☐ Personenstammdaten

☐ Kommunikationsdaten (z. B. Telefon-, E-Mail- und vergleichbare Kommunikationsdaten)

☐ Daten im Zusammenhang mit Leistungs-, Abrechnungs- und Begutachtungsverfahren

☐ Beschäftigtendaten

☐ Nutzer-, Rollen- und Berechtigungsdaten

☐ Protokoll- und technische Nutzungsdaten

☐ Freie Nutzereingaben und Dialogverläufe

☐ Echtdaten in Test-, Fehleranalyse- und Validierungsumgebungen, beschränkt auf den Nachweis eines konkreten Fehlers oder die technische Validierung, nur auf dokumentierte Weisung des Auftraggebers und mit anschließender Löschung

☐ Inhalte und Nachweise aus Managementsystemen, soweit diese personenbezogene Daten enthalten

☐ Im Rahmen der Auftragsverarbeitung erzeugte Zwischen- und Ergebnisdaten

☐ Sonstige personenbezogene Daten: _____

Betriebs- und Geschäftsgeheimnisse, die im Zusammenhang mit den ausgewählten Daten oder der jeweiligen Leistung verarbeitet werden, sind vom Schutzumfang dieses Vertrages mit umfasst.

(3) Kategorien betroffener Personen

Folgende Kategorien betroffener Personen sind Gegenstand der Verarbeitung (Zutreffendes ankreuzen; Mehrfachauswahl möglich):

☐ Versicherte sowie deren vertretungsberechtigte Personen

☐ An- und Zugehörige von Versicherten

☐ Leistungserbringer sowie deren Beschäftigte

☐ Beschäftigte und Ansprechpartner der Auftraggeber der Medizinischen Dienste

☐ Beschäftigte des jeweiligen Auftraggebers

☐ Nutzerinnen und Nutzer der jeweiligen Softwarelösung

☐ Externe Gutachterinnen und Gutachter

☐ Beschäftigte und Ansprechpartner von Dienstleistern oder sonstigen beteiligten Organisationen

☐ Sonstige betroffene Personen: _____

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 eine Prüfung/ein Audit einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer gewährleistet die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 Buchst. b, Art. 29, Art. 32 Abs. 4 DS-GVO und § 203 StGB. 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/Sozialdaten 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 technischen und organisatorischen Maßnahmen des Auftragnehmers orientieren sich an anerkannten Standards der Informationssicherheit und des Datenschutzes (Stand der Technik). Die jeweils aktuellen technischen und organisatorischen Maßnahmen werden vom Auftragnehmer dokumentiert und dem Auftraggeber in geeigneter Form digital zur Verfügung gestellt. Die zum Zeitpunkt des Vertragsschlusses geltende Version der technischen und organisatorischen Maßnahmen ist diesem Vertrag als Anlage beigefügt.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen

umzusetzen. Dabei darf das Sicherheitsniveau, welches im Vorfeld zwischen Auftraggeber und Auftragnehmer abgestimmt wurde, nicht unterschritten werden. Änderungen sind zu dokumentieren.

(5) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für fünf volle Kalenderjahre aufzubewahren.

4. Sicherstellung der Betroffenenrechte

(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.

(2) Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(3) Der Auftragnehmer hat im Rahmen seiner Leistung den Auftraggeber in die Lage zu versetzen, die Betroffenenrechte erfüllen zu können. Der Auftragnehmer hat bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO, im notwendigen Umfang mitzuwirken und den Auftraggeber zu unterstützen (Art. 28 Abs. 3 S. 2 Buchst. e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an die in Anlage 2 angegebenen Ansprechpartner des Auftraggebers zu übermitteln.

(4) Der Auftragnehmer ist dazu verpflichtet, die personenbezogenen Daten/Sozialdaten auf Weisung des Auftraggebers unverzüglich zu berichtigen, zu löschen oder die Verarbeitung einzuschränken. Der Auftragnehmer wird dem Auftraggeber die Löschung, Berichtigung bzw. Einschränkung der Verarbeitung auf Verlangen in Textform nachweisen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zur Einhaltung der Regelungen dieses Vertrags gesetzliche Pflichten gemäß Art. 28 bis 36 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Soweit der Auftragnehmer gesetzlich zur Benennung eines Datenschutzbeauftragten verpflichtet ist oder freiwillig einen Datenschutzbeauftragten benannt hat, übt dieser seine Tätigkeit gemäß Art. 38 und 39 DS-GVO aus. Die entsprechenden Angaben sind in Anlage 2 aufzuführen. Ein Wechsel des Datenschutzbeauftragten beim Auftragnehmer ist dem Auftraggeber unverzüglich durch Aktualisierung der Anlage 2 mitzuteilen.

b) Der Auftragnehmer unterstützt den Datenschutzbeauftragten des Auftraggebers im Rahmen der Auftragsverarbeitung und ermöglicht dessen Kontrolltätigkeit.

c) Der Auftragnehmer ermöglicht und unterstützt Kontrolltätigkeiten der für den Auftraggeber zuständigen Aufsichtsbehörden.

d) Der Auftragnehmer unterstützt den Auftraggeber bei der Beantwortung von Anfragen der Aufsichtsbehörden sowie bei Kontrollen der Aufsichtsbehörden. Gleiches gilt für Ordnungswidrigkeits- oder Strafverfahren sowie Haftungsansprüchen betroffener Personen oder Dritter oder anderer Ansprüche im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer.

e) 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.

f) Der Auftragnehmer weist die nach Absatz e) durchgeführten Kontrollen und die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber in Textform nach.

g) Der Auftragnehmer hat bei der Erfüllung der Rechte der betroffenen Personen z. B. nach Art. 12 bis 22 DS-GVO bei der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten und bei ggf.

erforderlichen Datenschutz-Folgenabschätzungen sowie zugehöriger Konsultation im notwendigen Umfang mitzuwirken und den Auftraggeber zu unterstützen (Art. 28 Abs. 3 S. 2 Buchst. e und f, i. V. m. Art. 35 und 36 DS-GVO).

h) Soweit der Auftraggeber in den Anwendungsbereich des § 393 SGB V fällt, hält der Auftragnehmer die sich daraus ergebenden Anforderungen einschließlich hinsichtlich der von ihm eingesetzten Unterauftragnehmer ein und weist deren Einhaltung auf Verlangen nach.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung gelten solche Dienstleistungen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen und bei denen die Möglichkeit besteht, dass personenbezogene Daten einschließlich Sozialdaten des Auftraggebers, soweit diese betroffen sind, verarbeitet werden oder zur Kenntnis genommen werden können.

Hierzu zählen insbesondere, jedoch nicht ausschließlich, Leistungen wie

- Wartung und Pflege von Hard- und Software
- Bereitstellung von KI-Modellen und darauf aufbauenden Diensten
- Betrieb und Support von IT-Systemen und Anwendungen
- Beratungs-, Prüf- und Unterstützungsleistungen in den Bereichen Datenschutz, Compliance, Informationssicherheit und KI-Governance
- technische Sicherheitsprüfungen und Penetrationstests, soweit hierbei ein Zugriff auf personenbezogene Daten oder deren Kenntnisnahme nicht ausgeschlossen werden kann
- Benutzer-, Service- und Supportleistungen
- Entwicklungs- und Weiterentwicklungsleistungen
- Sicherheits-, Betriebs- und Überwachungsleistungen
- Hosting-, Rechenzentrums- und Infrastrukturleistungen
- Entsorgung und Vernichtung von Datenträgern
- sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der eingesetzten IT-Systeme.

(2) Der Auftragnehmer stellt sicher, dass auch bei der Beauftragung von Unterauftragnehmern angemessene, wirksame und gesetzeskonforme Verträge zur Auftragsverarbeitung sowie geeignete Kontrollmaßnahmen zur Wahrung des Datenschutzes und der Informationssicherheit getroffen werden.

(3) Regelung zur Unterbeauftragung

a) Der Auftraggeber stimmt der Beauftragung der in Anlage 3 aufgeführten Unterauftragnehmer zu, sofern mit diesen ein Vertrag nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO abgeschlossen wird. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragnehmer sind in Anlage 3 aufgeführt. Eine fortlaufend aktualisierte Übersicht der eingesetzten Unterauftragnehmer wird vom Auftragnehmer gepflegt und den Auftraggebern in geeigneter Form digital zur Verfügung gestellt.

b) Der Auftragnehmer darf weitere Unterauftragnehmer (Auftragsverarbeiter) beauftragen oder bestehende Unterauftragnehmer wechseln, wenn er dies dem Auftraggeber und, soweit die Leistungsvereinbarung es vorsieht, der MD-IT GmbH mindestens zwanzig Werktage vor dem beabsichtigten Einsatz in Textform angezeigt hat (für Fachlos 1: Abschnitt 10.1 Absatz 2 der Leistungsbeschreibung) und der Auftraggeber dem Einsatz vorher gesondert zugestimmt hat (Art. 28 Abs. 2 Satz 1 DS-GVO); für die Zustimmung gilt Absatz 9. Der Unterauftragnehmer darf erst nach Erteilung dieser Zustimmung eingesetzt werden. Weitergehende Informations-, Änderungs- und Zustimmungsvorgaben der Leistungsvereinbarung bleiben unberührt. Eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO ist sicherzustellen.

c) Die Anzeige nach Buchstabe b) enthält mindestens folgende Angaben:

- Name und Anschrift des Unterauftragnehmers,
- Beschreibung der ausgelagerten Leistung,
- Ort oder Orte der Datenverarbeitung,
- datenschutzrechtliche Einordnung der Unterbeauftragung, einschließlich der sozialdatenschutzrechtlichen Anforderungen, soweit diese für den konkreten Auftrag einschlägig sind, sowie die vorgesehenen technischen und organisatorischen Maßnahmen des Unterauftragnehmers,
- eine Beschreibung der wesentlichen datenschutzrechtlichen Vertragsbedingungen mit dem Unterauftragnehmer sowie eine Bestätigung des Auftragnehmers, dass der Unterauftragnehmer vor Beginn seiner Tätigkeit durch Vertrag nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO verpflichtet wird. Soweit der Auftraggeber dies zur Prüfung begründet verlangt, stellt der Auftragnehmer geeignete Auszüge der vertraglichen Regelungen zur Verfügung; berechtigte Geheimhaltungsinteressen des Auftragnehmers und des Unterauftragnehmers bleiben gewahrt.

(4) Die Weitergabe von personenbezogenen Daten/Sozialdaten an Unterauftragnehmer sowie deren erstmaliges Tätigwerden sind erst zulässig, wenn die oben genannten Voraussetzungen für die Unterbeauftragung erfüllt sind.

(5) Soweit die konkrete Verarbeitung dem § 80 SGB X unterliegt, ist die Beauftragung von Unterauftragnehmern nur zulässig, sofern die Anforderungen des § 80 Abs. 1 bis 3 SGB X einschließlich der Anzeige nach Ziffer 6a eingehalten werden.

Soweit für den jeweiligen Auftraggeber aufgrund landesrechtlicher Regelungen weitergehende oder strengere Anforderungen an die Auftragsverarbeitung gelten, sind diese für diesen Auftraggeber im jeweiligen Einzelfall zusätzlich zu berücksichtigen.

(6) Die Verarbeitung personenbezogener Daten/Sozialdaten einschließlich ihrer Speicherung sowie administrative Zugriffe auf diese Daten erfolgen ausschließlich innerhalb eines Mitgliedstaates der Europäischen Union oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum.

(7) Eine weitere Unterbeauftragung durch Unterauftragnehmer bedarf der vorherigen Zustimmung des Auftraggebers mindestens in Textform.

Der Auftragnehmer stellt sicher, dass auch in diesen Fällen die Informations- und Anzeigepflichten nach Absatz 3 und nach Ziffer 6a eingehalten werden können.

(8) Der Auftragnehmer stellt sicher, dass Unterauftragnehmer vertraglich verpflichtet werden, die für sie einschlägigen datenschutzrechtlichen Pflichten aus diesem Vertrag inhaltlich gleichwertig einzuhalten.

Der Auftragnehmer stellt sicher, dass diese Verpflichtungen entlang der gesamten Vertragskette wirksam durchgesetzt werden.

(9) Die Zustimmung des Auftraggebers zur Einbindung oder zum Wechsel von Unterauftragnehmern darf nicht ohne sachlichen Grund verweigert werden. Ein sachlicher Grund liegt insbesondere vor, wenn auf Grundlage konkreter und nachvollziehbarer Anhaltspunkte davon auszugehen ist, dass die Einbindung des Unterauftragnehmers gegen datenschutzrechtliche oder, soweit einschlägig, sozialdatenschutzrechtliche Anforderungen verstößt. Soweit die Einbindung oder der Wechsel weiterer Unterauftragnehmer durch einen bereits eingesetzten (Unter-)Auftragnehmer im Rahmen bestehender Betriebsleistungen erfolgt und für den ordnungsgemäßen Betrieb der Systeme erforderlich ist, werden die Parteien eine einvernehmliche Lösung anstreben, die den kontinuierlichen Betrieb der beauftragten Leistung sicherstellt. Das Recht der MD-IT GmbH nach der Leistungsvereinbarung, die Übernahme eines neuen Unterauftragnehmers als wesentliche Änderung abzulehnen oder aufzuschieben (für Fachlos 1: Abschnitt 10.1 Absatz 2 der Leistungsbeschreibung), bleibt nach Ziffer 1 Absatz (1a) unberührt.

6a. Anzeige nach § 80 Abs. 1 SGB X

(1) Soweit die Verarbeitung dem § 80 SGB X unterliegt, zeigt der Auftraggeber die Auftragsverarbeitung seiner Rechts- oder Fachaufsichtsbehörde rechtzeitig vor der Auftragserteilung an (§ 80 Abs. 1 SGB X). Der Auftragnehmer stellt dem Auftraggeber die hierfür erforderlichen Angaben vollständig in Textform zur Verfügung: sich selbst als Auftragsverarbeiter mit den bei ihm vorhandenen technischen und organisatorischen Maßnahmen, die vorgesehenen Unterauftragsverhältnisse (Anlage 3) sowie, soweit sie sich aus der Leistungsvereinbarung ergeben, die Art der im Auftrag zu verarbeitenden Daten, den Kreis der betroffenen Personen und die Aufgabe, zu deren Erfüllung die Verarbeitung erfolgt. Die Angaben sind mit der Erklärung auf den Abruf nach der Leistungsvereinbarung vorzulegen, spätestens zehn Kalendertage nach Eingang des Abrufs.

(2) Die Verarbeitung von Sozialdaten im Auftrag beginnt erst, wenn der Auftraggeber dem Auftragnehmer in Textform bestätigt hat, dass die Anzeige erstattet ist. Verzögert sich der Beginn, weil die Angaben nach Absatz 1 nicht rechtzeitig oder nicht vollständig vorliegen, kann sich der Auftragnehmer hierauf nicht berufen; vereinbarte Fristen zur produktiven Inbetriebnahme verlängern sich insoweit nicht. Verzögert sich der Beginn aus Gründen, die in der Sphäre des Auftraggebers oder seiner Aufsichtsbehörde liegen, gelten die Regelungen der Leistungsvereinbarung zur fehlenden Mitwirkung der abrufenden Stelle.

(3) Ändern sich die angezeigten Angaben, insbesondere durch die Einbindung oder den Wechsel eines Unterauftragnehmers, übermittelt der Auftragnehmer die geänderten Angaben zusammen mit der Anzeige nach Ziffer 6 Absatz 3 Buchstabe b, mindestens zwanzig Werktage vor der beabsichtigten Änderung, damit der Auftraggeber die Änderung seiner Aufsichtsbehörde anzeigen kann. Die Änderung darf erst umgesetzt werden, wenn der Auftraggeber ihr nach Ziffer 6 zugestimmt hat.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Kontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Die Prüf- und Kontrollrechte stehen entsprechend auch der MD-IT GmbH, soweit ihr die Leistungsvereinbarung Prüfrechte einräumt (Ziffer 1 Absatz (1a)), dem Datenschutzbeauftragten des Auftraggebers, den für den jeweiligen Auftraggeber zuständigen Aufsichtsbehörden sowie, soweit einschlägig, den zuständigen Prüfdiensten zu. Der Auftragnehmer ermöglicht und unterstützt die Durchführung dieser Prüfungen im erforderlichen Umfang.

(2) Liegt bereits ein Verdacht auf einen Verstoß des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten/Sozialdaten oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte auch hierbei weitestgehend vermieden werden.

(3) 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. Hierzu stellt der Auftragnehmer im erforderlichen Umfang auch die zur Prüfung notwendigen Unterlagen und sonstigen Nachweise zur Verfügung. Auf Anforderung sind die Auskünfte und Nachweise an den Auftraggeber in Textform zu übermitteln.

(4) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann z.B. erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(5) Der Auftragnehmer hat sicherzustellen, dass der Auftraggeber gegenüber jedem Unterauftragnehmer seine Kontrollrechte aus diesem Vertrag in geeigneter Weise ausüben kann. Dabei unterstützt der Auftragnehmer den Auftraggeber. Das Prüf-/Kontrollrecht gilt auch für den Datenschutzbeauftragten des Auftraggebers, die zuständigen Aufsichtsbehörden sowie, soweit einschlägig, die zuständigen Prüfdienste. An jeden Unterauftragnehmer müssen die vorgenannten Prüf-/Kontrollrechte inhaltlich entsprechend schriftlich weitergegeben werden.

(6) Für die Erfüllung der in diesem Abschnitt geregelten Nachweis-, Unterstützungs- und Kontrollpflichten, einschließlich der Durchführung von Dokumentenaudits sowie der Ausübung entsprechender Kontrollrechte gegenüber Unterauftragnehmern, kann der Auftragnehmer gegenüber dem Auftraggeber keine gesonderte Vergütung oder Kostenerstattung verlangen. Der Auftragnehmer stellt sicher, dass die Ausübung der nach Abs. 5 an Unterauftragnehmer weitergegebenen Prüf- und Kontrollrechte nicht von einer gesonderten Vergütung oder Kostenerstattung durch den Auftraggeber abhängig gemacht wird.

(7) Soweit die Prüfung als Dokumentenaudit erfolgt, stellt der Auftragnehmer die angeforderten Unterlagen und Nachweise unverzüglich, grundsätzlich innerhalb von sieben Arbeitstagen, zur Verfügung. Soweit aufgrund der Dringlichkeit oder des Umfangs der Prüfung eine abweichende Frist erforderlich ist, stimmen die Parteien diese im Einzelfall ab.

8. Mitteilungspflichten des Auftragnehmers bei Störungen, Datenschutz-/Vertragsverletzungen, sicherheitsrelevanten Vorfällen sowie Kontrollhandlungen Dritter

(1) Bei Störungen bei den Verarbeitungstätigkeiten, Verdacht auf Datenschutzverletzungen, Verletzungen vertraglicher Verpflichtungen des Auftragnehmers und des Unterauftragnehmers sowie bei Verdacht auf sicherheitsrelevante Vorfälle beim Auftragnehmer und Unterauftragnehmer, bei ihnen im Rahmen dieses Vertrages beschäftigten Personen oder bei Dritten wird der Auftragnehmer den Auftraggeber unverzüglich nach Kenntniserlangung mindestens in Textform informieren.

(2) Gleiches gilt, wenn bei einer Prüfung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen festgestellt werden.

(3) Gleiches gilt für Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen und auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten/Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(4) Der Auftragnehmer ist verpflichtet, den Auftraggeber im Rahmen von dessen Informationspflichten gegenüber den Aufsichtsbehörden und den Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen. Außerdem hat der Auftragnehmer den Auftraggeber im Rahmen weitergehender Kommunikation mit den Aufsichtsbehörden zu unterstützen. Auf Anforderung des Auftraggebers hat der Auftragnehmer die Informationen nach Wahl des Auftraggebers schriftlich oder in Textform zur Verfügung zu stellen.

(5) Die Information des Auftragnehmers an den Auftraggeber über eine Verletzung des Schutzes personenbezogener Daten enthält, soweit möglich, folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung,

c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Soweit die Informationen nach a) bis c) nicht möglich sind, ist dies zu begründen.

(6) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der betroffenen Daten und zur Minderung möglicher nachteiliger Folgen für die betroffene(n) Person(en), informiert hierüber den Auftraggeber, ersucht ihn um weitere Weisungen und erteilt dem Auftraggeber jederzeit weitere Auskünfte, soweit dessen Daten von einer Verletzung nach Abs. 1 betroffen sind.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer darf personenbezogene Daten/Sozialdaten nur auf dokumentierte Weisung des Auftraggebers verarbeiten.

(2) Der Auftraggeber erteilt Weisungen in der Regel mindestens in Textform.

(3) Mündliche Weisungen wird der Auftraggeber unverzüglich mindestens in Textform bestätigen.

(4) Der Auftragnehmer notiert sich Datum, Uhrzeit und Person, welche die mündliche Weisung erteilte, sowie den Grund, warum keine Beauftragung in Textform erfolgen konnte.

(5) Weisungen sind vom Auftragnehmer zu dokumentieren und durch den Auftragnehmer für fünf Jahre ab Beendigung des Vertrages aufzubewahren.

(6) Die Ansprechpartner sowie die weisungsberechtigten Personen des Auftraggebers werden dem Auftragnehmer, mindestens in Textform, mitgeteilt und sind in Anlage 2 aufgeführt. Entsprechendes gilt für die Änderung dieser Ansprechpartner. Gleiches gilt für die Ansprechpartner und die weisungsberechtigten Personen des Auftragnehmers.

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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten/Sozialdaten und Vernichtung von Datenträgern

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien oder technisch bedingte Redundanzen, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind und nach Maßgabe der Leistungsvereinbarung zulässig 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 Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung (mindestens in Textform) datenschutzgerecht zu löschen bzw. den/die Datenträger zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Nachweis der Löschung/Vernichtung ist dem Auftraggeber vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Fernzugriff bei Prüfung/Wartung eines Systems oder anderen Dienstleistungen über Fernzugriffe

(1) Fernzugriffe auf Systeme des Auftraggebers oder auf Datenverarbeitungsanlagen, bei denen ein Zugriff auf personenbezogene Daten/Sozialdaten nicht ausgeschlossen werden kann, erfolgen

ausschließlich auf Grundlage der beim Auftragnehmer geltenden und vom Auftraggeber freigegebenen technischen und organisatorischen Maßnahmen.

(2) Diese Maßnahmen regeln insbesondere die Zugriffskontrolle, Authentifizierung, Protokollierung sowie geeignete Verschlüsselungs- und Sicherheitsmechanismen.

(3) Der Auftragnehmer stellt sicher, dass Fernzugriffe nur im erforderlichen Umfang und ausschließlich zum Zweck der ordnungsgemäßen Durchführung der beauftragten Leistungen erfolgen.

12. Zurückbehaltungsrecht

(1) Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

(2) Sollten das Eigentum oder die zu verarbeitenden personenbezogenen Daten/Sozialdaten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer, sofern gesetzlich zulässig, den Auftraggeber unverzüglich zu verständigen. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber liegt.

13. Haftung

(1) Die Haftung der Parteien richtet sich nach Art. 82 DS-GVO.

(2) Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag oder weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt. Ebenso bleibt die Haftung des Auftragnehmers für seine Unterauftragnehmer sowie deren Unterauftragnehmer unberührt.

14. Schriftformklausel

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform (§ 126 BGB) und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung oder Ergänzung dieses Vertrages handelt.

(2) Dies gilt auch für den Verzicht auf dieses Schriftformerfordernis.

(3) Änderungen und Ergänzungen der Anlagen zu diesem Vertrag sind vom vorstehenden Schriftformerfordernis ausgenommen und bedürfen der Textform (§ 126b BGB). Die Führung und Aktualisierung der Anlagen kann in einem von den Parteien gemeinsam genutzten elektronischen Dokumentationssystem erfolgen, sofern die jeweilige Änderung dokumentiert und für beide Parteien dauerhaft nachvollziehbar ist.

15. Salvatorische Klausel

(1) Sollten sich einzelne Bestimmungen dieses Vertrages ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge von Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

(2) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(3) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

(4) Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter Abs. 2 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den

Schutz der personenbezogenen Daten/Sozialdaten im Sinne dieses Vertrages am besten gewährleistet.

16. Rechtswahl, Gerichtsstand, Inkrafttreten

(1) Es gilt deutsches Recht.

(2) Gerichtsstand ist der Sitz des Auftraggebers.

(3) Dieser Vertrag wird durch beiderseitige Unterzeichnung abgeschlossen, tritt mit Abschluss in Kraft und löst ältere Versionen dieses Vertrages ab.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Auftragnehmer	Auftraggeber

Anlage 1 Technisch-organisatorische Maßnahmen des Auftragnehmers

Die vom Auftragnehmer im Vergabeverfahren bzw. vor Beginn der Verarbeitung vorgelegten und vom Auftraggeber akzeptierten technischen und organisatorischen Maßnahmen werden Bestandteil dieses Vertrages. Sie sind in ihrer jeweils für das ausgewählte Fachlos und den konkreten Einzelauftrag maßgeblichen Fassung beizufügen bzw. in der vereinbarten elektronischen Dokumentation eindeutig zu referenzieren.

Die Dokumentation umfasst mindestens die nach Art. 32 DS-GVO erforderlichen Maßnahmen, insbesondere:

- organisatorische Maßnahmen und Datenschutzorganisation
- Gewährleistung der Vertraulichkeit, insbesondere Zutritts-, Zugangs-, Zugriffs-, Weitergabe- und Trennungskontrolle
- Gewährleistung der Integrität der Systeme und Dienste
- Gewährleistung der Verfügbarkeit, Belastbarkeit und raschen Wiederherstellung
- Auftragskontrolle einschließlich Berechtigungs-, Protokollierungs- und Löschkonzept
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen
- Verfahren zum Umgang mit Informationssicherheits- und Datenschutzvorfällen

[Vom Auftragnehmer einzureichende TOM-Dokumentation / Fundstelle]

Anlage 2 Ansprechpartner des Auftraggebers und des Auftragnehmers

1. Auftraggeber

Weisungsberechtigte Person(en)

Weisungsberechtigte Person(en):	
Name, Vorname:	
Funktionsbezeichnung:	
E-Mail/Telefonnummer:	

Datenschutz- und Informationssicherheitsbeauftragte

Datenschutzbeauftragter:	
Name, Vorname:	
Funktionsbezeichnung:	
E-Mail/Telefonnummer:	
Informationssicherheitsbeauftragter:	
Name, Vorname:	
Funktionsbezeichnung:	
E-Mail/Telefonnummer:	

2. Auftragnehmer

Weisungsempfangende Person(en)

Weisungsempfangende Person(en):	
Name, Vorname:	
Funktionsbezeichnung:	
E-Mail/Telefonnummer:	

Datenschutz- und Informationssicherheitsbeauftragte

Datenschutzbeauftragter:	
Name, Vorname:	
Funktionsbezeichnung:	
E-Mail/Telefonnummer:	
Informationssicherheitsbeauftragter:	
Name, Vorname:	
Funktionsbezeichnung:	
E-Mail/Telefonnummer:	

Anlage 3 zum AV-Vertrag: Unterauftragsverhältnisse beim Auftragnehmer

Lfd. Nr.	Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung	Datum des Vertragsabschlusses
1				
2				
3				
4				
5				
6				