Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag (Art. 28 DSGVO i. V. m. § 80 SGB X)

– Datenschutzbestimmungen –

§ 1

Gegenstand der Datenschutzbestimmungen

Diese Datenschutzbestimmungen sind Bestandteil der vereinbarten Leistungen entsprechend der

„Rahmenvereinbarung zur strategischen Beratung und IT-Dienstleistungen“ der AOK NordWest <Vergabenummer: 21258>

- im Folgenden Hauptvertrag genannt - und somit Grundlage für die Abwicklung der zwischen dem Verantwortlichen und dem Auftragnehmer vertraglich vereinbarten Leistungen. Diese Datenschutzbestimmungen regeln den Schutz von Daten bei der Datenverarbeitung im Auftrag unter besonderer Berücksichtigung des Art. 28 DSGVO und des § 80 SGB X.

§ 2

Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten werden im Hauptvertag konkret beschrieben.

(2) Die betroffenen personenbezogenen Daten/Sozialdaten sind in **Anhang F** definiert.

(3) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn

a) die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, sofern personenbezogene Daten verarbeitet werden, die keine Sozialdaten sind (es gilt ausschließlich Art. 28 DSGVO) oder
b) sofern Sozialdaten verarbeitet werden, ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt (Art. 28 DSGVO i. V. m. § 80 SGB X).

Ein Zugriff auf personenbezogene Daten durch Staaten, für die kein solcher Angemessenheitsbeschluss vorliegt, ist dem Auftragnehmer unverzüglich mitzuteilen. In **Anhang B** sind die Standorte, bei denen Sozialdaten / personenbezogene Daten des Auftraggebers verarbeitet werden, einzutragen und ggf. Feststellungen zum angemessenen Schutzniveau in den betreffenden Drittländern zu treffen. 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 Zustimmung des Auftraggebers schriftlich oder in Textform. Soweit der Auftraggeber eine Daten-übermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

§ 3

Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen oder Maßnahmen vergleichbarer Art und Güte vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung schriftlich oder in Textform zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben (Anhang C). Bei Akzeptanz der Maßnahmen vergleichbarer Art und Güte durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser 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 (Einzelheiten in Anhang C).

(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 revisionssicher zu dokumentieren.

(4) Sämtliche Dokumentationen zu den technischen und organisatorischen Maßnahmen, Dokumentationen von Regelungen zum Datenschutz und zur Informationssicherheit und Audit- bzw. Prüfberichte müssen in deutscher Sprache verfasst bzw. in deutscher Übersetzung bereitgehalten werden.

§ 4

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:

(1) Die schriftliche Bestellung eines Datenschutzbeauftragten (vgl. Art. 37 Abs. 4 DSGVO i. V. m. § 81 Abs. 4 SGB X), der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme in **Anhang A** mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

(2) Die Wahrung der Vertraulichkeit und des Daten- sowie Sozialgeheimnisses (sofern Sozialdaten verarbeitet werden) gemäß Art. 28 Abs. 3 Satz 2 lit. b, 29, 32 Abs. 4 DSGVO, § 35 SGB I. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit und zur Geheimhaltung unter Hinweis auf die rechtlichen Folgen einer Pflichtverletzung, insbesondere nach § 203 Abs. 4 StGB, 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 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) Dem Auftragnehmer ist die Verarbeitung von Daten nur zum Zwecke der Erfüllung des Hauptvertrages sowie im Rahmen der schriftlichen Weisungen des Verantwortlichen und nach den datenschutzrechtlichen Vorschriften unter Beachtung der technischen und organisatorischen Maßnahmen gem. § 3 dieser Bestimmungen gestattet. Der Auftragnehmer verwendet die Daten und die daraus erzielten Verarbeitungsergebnisse ausschließlich für die Erfüllung des Hauptvertrages. Insbesondere ist die Anonymisierung zu eigenen Zwecken, z. B. für eigene (Daten-Analysen ausgeschlossen. Er bewahrt die Daten unter Verschluss bzw. unter Einsatz entsprechender technischer Mittel vor unbefugtem Zugriff gesichert nur so lange auf, wie es für die Erfüllung der genannten Leistungen erforderlich ist. Er gibt sie nicht an Dritte weiter.

(4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörden, 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 bzw. Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer oder Unterauftragnehmern ermittelt.

(6) Sollte eine Verarbeitung von Daten des Verantwortlichen unter Nutzung mobiler Arbeitsplätze/ Heim- oder Telearbeitsplätze stattfinden, ist sicherzustellen, dass dies unter Beachtung der technischen und organisatorischen Maßnahmen gemäß § 3 dieser Datenschutzbestimmungen erfolgt.

(7) 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. Die Kontrollen, die Ergebnisse und ggf. umgesetzte Maßnahmen sind zu protokollieren und für mindestens 6 Jahre aufzubewahren.

(8) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber erfolgt im Rahmen seiner Kontrollbefugnisse nach § 6 dieser Datenschutzbestimmungen.

(9) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Diese Verpflichtung besteht über das Ende des Vertragsverhältnisses hinaus.

(10) Personenbezogene Daten/Sozialdaten des Auftraggebers dürfen nicht im öffentlichen Raum (z. B. Flughafen, Bahn etc.) verarbeitet werden. Die Verarbeitung der personenbezogenen Daten/Sozialdaten des Auftraggebers außerhalb der Geschäftsräume des Auftragnehmers ist nur im nichtöffentlichen Raum zulässig und nur mit gesicherten firmeneigenen Geräten des Auftragnehmers. Es muss sich dabei um verschlüsselte Festplatten, geschützte Verbindungen und fortschrittliche Sicherheitsvorkehrungen (jeweils aktuell) wie z. B. Firewall handeln, sowie aktuelle Signaturen von Viren- und Malwarescannern. Die Bestimmungen zu den technisch-organisatorischen Maßnahmen nach § 3 dieser Datenschutzbestimmungen sind zu beachten.

(11) Die Verwendung privater IT-Geräte wie PCs, Tablets, Notebooks, Smartphones etc. bzw. die private Nutzung der firmeneigenen IT-Geräte ist grundsätzlich nicht gestattet. Ausnahmen bedürfen der vorherigen ausdrücklichen Zustimmung (schriftlich oder in Textform) des Auftraggebers und stehen unter dem Vorbehalt, dass sich der Auftraggeber von einer hinreichenden Endgerätesicherheit des Auftragnehmers überzeugen kann. Der Auftragnehmer hat dem Auftraggeber hierzu geeignet nachzuweisen, dass er bei der Verwendung privater IT-Geräte dem Schutzbedarf der Daten und dem jeweiligen Stand der Technik entsprechende Maßnahmen umgesetzt hat. Die Bestimmungen zu den technisch-organisatorischen Maßnahmen nach § 3 dieser Datenschutzbestimmungen sind zu beachten.

(12) Die Nutzung von Cloudcomputing durch den Auftragnehmer ist nur zulässig, wenn dieser mit dem jeweiligen Anbieter eine Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO abschließt und – soweit Sozialdaten verarbeitet werden – die Vorgaben des § 393 Abs. 2 bis 4 SGB V und bei der Verarbeitung von Sozialdaten zusätzlich die Anforderungen des § 80 SGB X, bezüglich der räumlichen Beschränkungen der Verarbeitung eingehalten werden. Die Umsetzung der Anforderungen ist in **Anhang C** zu dokumentieren.

(13) Der Auftragnehmer verpflichtet sich, dass die Daten des Auftraggebers von Daten anderer Auftraggeber streng getrennt werden. 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.

(14) Zur Einhaltung der Vorgaben gemäß § 392 Abs. 6 SGB V und § 103a Abs. 6 SGB XI verpflichtet sich der Auftragnehmer gegenüber dem Auftraggeber zur Einhaltung des branchenspezifischen Sicherheitsstandards B3S-GKV/PV in der jeweils gültigen Fassung. Ferner verpflichtet sich der Auftragnehmer gegenüber dem Auftraggeber die durch ihn beauftragten Unterauftragnehmer ebenso zur Einhaltung des branchenspezifischen Sicherheitsstandard B3S-GKV/PV in der jeweils gültigen Fassung, zumindest für alle Dienstleistungen im Zusammenhang mit der beauftragten Leistung zu verpflichten, soweit die beauftragten Unterauftragnehmer IT-Dienstleistungen erbringen.

(15) Technische Überprüfungen (z. B. Penetrationstests) sollen jährlich mit jeweils wechselnden Schwerpunkten durchgeführt werden. Für den Fall, dass die technische Überprüfung Sicherheitslücken und /oder Einschränkungen aufführt, sind diese unverzüglich zu beheben.

§ 5

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 Sozialdaten nicht ausgeschlossen werden kann. In **Anhang D** sind die Unterauftragnehmer jeglichen Grades anzugeben. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. dem Fernmeldegeheimnis unterliegenden Digitalen Dienste (z.B.: als Telekommunikationsdienstleister), dem Postgeheimnis unterliegende Post-/Transportdienstleistungen, sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nehmen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen. Soweit im Fall der Beauftragung/Zuschlagserteilung ein oder mehrere Unterauftragnehmer jeglichen Grades Daten des Verantwortlichen verarbeiten, müssen sowohl der Auftragnehmer als auch die

Unterauftragnehmer jeglichen Grades angeben, welches Aufgabenfeld an welchem Unternehmensstandort ausgeführt werden sollen.

(2) Der Auftragnehmer darf Unterauftragnehmer jeglichen Grades (weitere Auftragnehmer) nur nach vorheriger ausdrücklicher Zustimmung (mindestens Textform) des Auftraggebers beauftragen und soweit der Auftragnehmer mit dem Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO und sofern Sozialdaten verarbeitet werden i. V. m. § 80 SGB X, die zudem die in diesem Vertrag vereinbarte Rechte und Pflichten berücksichtigt, geschlossen hat.

Der Auftraggeber stimmt der Beauftragung der in **Anhang D** aufgeführten Unterauftragnehmer zu, soweit jeweils eine vertragliche Vereinbarung nach Maßgabe von Satz 1 geschlossen wurde.

(3) Sollen vom Auftragnehmer während der Vertragslaufzeit andere als in **Anhang D** benannte Unterauftragnehmer beauftragt oder Standorte von Unterauftragnehmern verlegt/erweitert werden, sind dem Auftraggeber rechtzeitig vor der geplanten Veränderung folgende Unterlagen zur Zustimmung vorzulegen:

a) Beschreibung der Arbeiten, die der Unterauftragnehmer ausführen soll,

b) Ort der Datenverarbeitung

c) Bericht der letzten Prüfung (nicht älter als 24 Monate),

d) Kopie der geplanten vertraglichen datenschutzrelevanten Regelungen (einschließlich der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit) mit dem Unterauftragnehmer.

(4) Erfordert abweichend von Absatz 3 dieser Datenschutzbestimmungen ein unvorhergesehenes Ereignis, wie z. B. ein IT-Sicherheitsvorfall, den Ersatz oder die Hinzuziehung neuer Unterauftragnehmer, damit die vertraglich geschuldete Leistung noch erbracht werden kann, wird der Auftraggeber unverzüglich über die Maßnahme in Textform informiert. Der Auftragnehmer darf den Unterauftragnehmer erst beauftragen, wenn der Auftragnehmer mit dem Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO und sofern Sozialdaten verarbeitet werden i. V. m. § 80 SGB X, die zudem die in diesen Datenschutzbestimmungen vereinbarten Rechte und Pflichten berücksichtigt, geschlossen hat. Die Unterlagen nach § 5 Abs. 3 von a) bis c) dieser Datenschutzbestimmungen werden vom Auftragnehmer unverzüglich zur Genehmigung durch den Auftraggeber nachgereicht. Der Auftraggeber wird die Unterlagen binnen 4 Wochen ab Zugang der Änderungsmitteilung und aller vollständigen Unterlagen prüfen. Er wird den Ersatz bzw. die Hinzuziehung des Unterauftragnehmers genehmigen, wenn kein sachlicher Grund entsprechend Abs. 3 entgegensteht. Der Auftragnehmer hat sicherzustellen, dass der neue bzw. hinzugezogene Unterauftragnehmer noch von der Leistungserbringung ausgeschlossen werden kann, wenn ein sachlicher Grund zur Versagung der Genehmigung besteht. In diesem Fall werden die Parteien unter Beachtung der Aufrechterhaltung der Leistungserbringung gemeinsam eine einvernehmliche Lösung finden.

(5) Die Weitergabe von personenbezogenen Daten/Sozialdaten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller gesetzlichen und vertraglich vereinbarten Voraussetzungen insbesondere der vorliegenden schriftlichen (mindestens Textform) Zustimmung des Auftraggebers für eine Unterbeauftragung gestattet.

(6) Erbringt der Unterauftragnehmer die vereinbarte Leistung im Sinne von Abs. 1 Satz 3 stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

(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 sind durch den Auftragnehmer nachzuweisen und rechtzeitig vor Abschluss des Vertrages vorzulegen.

(8) § 2 Abs. 3 dieser Datenschutzbestimmungen gilt für Unterauftragnehmer entsprechend.

(9) Wird beim Auftragnehmer die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen und kann dabei der Zugriff auf Sozialdaten / 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 Zuschlag bestehende Vertragsbeziehungen sind in **Anhang E** aufzuführen.

(10) Beauftragt der Auftragnehmer für den Datentransport einen Transportunternehmer, so hat er vertraglich sicherzustellen und dem Auftraggeber auf Verlangen nachzuweisen, dass der Transportunternehmer den Datenschutzbestimmungen Genüge tut. Werden Unterlagen des Auftraggebers abgeholt, stattet der Auftragnehmer den Transportunternehmer mit einem schriftlichen Berechtigungsausweis für die Entgegennahme der Unterlagen aus.

§ 6

Kontrollrechte des Auftraggebers und dessen Aufsichtsbehörden

(1) Der Auftraggeber, dessen zuständige Aufsichtsbehörden bzw. ein von ihm beauftragter neutraler Dienstleister, der in keinem Wettbewerbsverhältnis zum Auftragnehmer stehen darf und zuvor schriftlich vom Auftraggeber auf die Vertraulichkeit und Wahrung der Geschäftsgeheimnisse zu verpflichten ist, haben das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Sie haben das Recht, sich durch Stichprobenkontrollen von der Einhaltung dieser Datenschutzbestimmungen 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) Das Prüfrecht umfasst insbesondere die Besichtigung von Grundstücken und Geschäftsräumen, Auskünfte zur Vertragsausführung, Einsicht in Papierunterlagen und auch die Einsichtnahme in die beim Auftragnehmer gespeicherten personenbezogenen Daten / Sozialdaten des Auftraggebers, soweit dies im Rahmen des Auftrags zur Überwachung von Datenschutz und Datensicherheit erforderlich ist. Dies gilt insbesondere für den Nachweis der Umsetzung der technischen und organisatorischen Maßnahmen.

(4) Der Nachweis technischer und organisatorischer Maßnahmen kann erfolgen durch

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001 oder BSI-Standards).

(5) Der Auftragnehmer sichert zu, dass er die notwendige personelle und sachliche Unterstützung bei den Prüfungen zur Verfügung stellt.

(6) 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.

§ 7

Mitwirkungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den §§ 83a bis 84 SGB X (soweit Sozialdaten verarbeitet werden) und den Art. 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen der Aufsichtsbehörde. Hierzu gehören u. a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

b) die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden. In diesem Falle hat der Auftragnehmer sofort alle erforderlichen Maßnahmen zur Sicherung der Sozialdaten zu treffen und weitere Anweisungen durch den Auftraggeber abzuwarten,

c) 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,

d) die Unterstützung des Auftraggebers bei der Beantwortung und Umsetzung von Betroffenenrechten mit geeigneten technischen und organisatorischen Maßnahmen (§§ 3 und 9 dieser Datenschutzbestimmungen bleiben hiervon unberührt)

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung,

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

§ 8

Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber hat das Recht, erforderlichenfalls Weisungen (mindestens Textform) im Rahmen der Art. 28, 32 DSGVO zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit 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 Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 9

Berichtigung, Einschränkung, Löschung und Rückgabe der vertragsgegenständlichen Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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, ist das Löschkonzept, das Recht auf Vergessenwerden, die Berichtigung von personenbezogenen Daten / Sozialdaten, die Datenportabilität (soweit einschlägig) und Auskünfte nach Weisung (mindestens Textform) 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 den jeweiligen Vereinbarungen im Einzelfall bzw. nach Abschluss der vertraglichen Arbeiten dem Auftraggeber auszuhändigen bzw. zu übermitteln.

(4) Auf Verlangen des Auftraggebers hat der Auftragnehmer in seinem Besitz befindliche Daten bzw. Datenbestände (z.B. physische Datenträger, elektronische Dateien oder Datenbanken in seinen Datenverarbeitungs-Systemen) nichtreproduzierbar zu löschen bzw. physisch zu vernichten. Die Vernichtung hat in Abhängigkeit von den verarbeiteten personenbezogenen Daten / Sozialdaten nach DIN 66399 Teile 1 bis 3 mindestens mit der Schutzklasse 3 mindestens mit Sicherheitsstufe 4 in der jeweils einschlägigen Materialklasse zu erfolgen. Die Datenlöschung hat nach anerkanntem Standard des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder anderweitiger adäquater Regelungen für vertrauliche Daten in der jeweils aktuellen Fassung zu erfolgen. Dies gilt auch für Test- und Zwischenergebnisse. 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 Löschung und Vernichtung hat der Auftragnehmer in geeigneter Weise zu protokollieren. Im Zweifelsfall sind geeignete Maßnahmen mit dem Auftraggeber abzustimmen. Hinsichtlich sämtlicher Löschvorgänge hat der Auftragnehmer dem Auftraggeber Löschprotokolle auf Verlangen zu übergeben.

Es sind folgende Mindestinhalte für ein Löschprotokoll zu berücksichtigen:

- Datum und Uhrzeit der Löschung,
- das gültige Löschkonzept (Version, Datum),
- die Methode der Datenlöschung (Verfahren),
- das betroffene Verfahren (Beschreibung der zu löschenden Daten),
- die angewandte Löschregel,
- die für die Löschung verantwortliche Person,
- die ausführenden Personen,
- bei automatisierter Löschung die Anzahl der zu löschenden Daten (Summenprotokolle, Zählreport) und

- bei automatisierter Löschung die Anzahl der gelöschten Daten (Summenprotokolle, Zählreport, Löschlaufreport).

Das Löschprotokoll darf darüber hinaus keine personenbezogenen Daten /Sozialdaten enthalten. Sind von der Vernichtung auch nicht elektronische Unterlagen betroffen, ist ein Vernichtungsprotokoll zu erstellen.

(6) Endet das Vertragsverhältnis, hat der Auftragnehmer gegenüber dem Auftraggeber schriftlich zu erklären, dass die nicht mehr erforderlichen Daten und Datenträger ordnungsgemäß im Sinne dieses Vertrages gelöscht bzw. vernichtet wurden und welche Daten aus gesetzlichen Gründen über das Ende des Auftragsverhältnisses hinaus aufbewahrt werden müssen.

§ 10

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.

(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 Verantwortlichen ist dies durch Vorlage geeigneter Dokumente nachzuweisen.

(3) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

§ 11

Nebenabreden

Änderungen und Nebenabreden zu diesen Datenschutzbestimmungen bedürfen der Schriftform.

§ 12

Laufzeit des Vertrages und Kündigung

(1) Beginn und Ende des Auftragsverhältnisses sind im Hauptvertrag geregelt.

(2) Der Verantwortliche kann den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn

a) ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutz-vorschriften oder diese Datenschutzbestimmungen vorliegt. Ein schwerwiegender Verstoß ist u.a. anzunehmen, wenn gegen die in § 2 Abs. 3 bzw. § 5 Abs. 8 dieser Datenschutzbestimmungen bezeichneten Vorgaben verstoßen wird oder

b) der Auftragnehmer eine Weisung des Verantwortlichen nicht ausführen kann oder will oder

c) der Auftragnehmer Kontrollrechte des Verantwortlichen vertragswidrig verweigert oder

d) die Grundlage der Vertragserfüllung aufgrund einer Änderung der Rechts- oder Gesetzeslage oder wegen aufsichtsrechtlicher Maßnahmen wesentlich verändert wird oder ganz entfällt.

e) Daten vertragswidrig durch den Auftragnehmer an Staaten übermittelt werden, die kein Mitgliedsstaat der Europäischen Union, kein anderer Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind oder für die kein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt.

Insbesondere die Nichteinhaltung der in diesen Datenschutzbestimmungen vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 13

Salvatorische Klausel

(1) Sollten einzelne Regelungen dieser Datenschutzbestimmungen ganz oder teilweise unwirksam sein oder werden oder sollten die Datenschutzbestimmungen eine Regelungslücke enthalten, bleibt die Wirksamkeit der übrigen Bestimmungen davon unberührt. Anstelle der unwirksamen oder fehlerhaften Bestimmungen treten die jeweiligen gesetzlichen Regelungen. Unwirksam gewordene Vereinbarungen werden die Vertragspartner durch wirksame Regelungen ersetzen, die dem ursprünglich verfolgten Zweck möglichst nahekommen. Diese sind bei nächster Gelegenheit als Ergänzung in diese Datenschutzbestimmungen aufzunehmen.

(2) Sollten sich gesetzliche Änderungen während der Vertragslaufzeit ergeben, die zu einer Vertragsanpassung führen müssen, verpflichten sich die Vertragspartner Vertragsverhandlungen mit dem Ziel der Einigung aufzunehmen.

§ 14

Inkrafttreten

(1) Diese Datenschutzbestimmungen treten mit Inkrafttreten des Hauptvertrages in Kraft.

(2) Es gilt die Gerichtsstands-Vereinbarung des Hauptvertrages.

Anhänge:

Anhang A	Übersicht Ansprechpartner
Anhang B	Datenverarbeitungsstandorte
Anhang C	technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit
Anhang D	Unterauftragnehmer
Anhang E	Wartung

Anhang F Datenkategorien und Personengruppen