Auftragsverarbeitungsvereinbarung (AVV) nach § 80 SGB X und Art. 28 Datenschutzgrundverordnung

Bereitstellung von Arbeitsplatzlösungen

der

BARMER

Inhaltsverzeichnis

Präambel

Die folgenden Abschnitte regeln die Maßnahmen zum Schutz personenbezogener Daten bei der Verarbeitung im Auftrag unter Berücksichtigung des Art. 28 DSGVO und soweit Sozialdaten verarbeitet werden, unter Berücksichtigung des § 80 SGB X. Sie ergänzen insoweit die Leistungsbeschreibung und ihre Anlagen.

§ 1 Konkretisierung der Vereinbarung

Der Gegenstand des Auftrags ergibt sich aus dem Anhang 1. Art und Zweck der Verarbeitung personenbezogener Daten bzw. Sozialdaten, die Art der personenbezogenen Daten bzw. Sozialdaten und die Kategorien der durch den Umgang mit ihren personenbezogenen Daten bzw. Sozialdaten im Rahmen dieses Auftrags Betroffenen sind ebenfalls im Anhang 1 beschrieben.

Die Dauer des Auftrags (Laufzeit) entspricht der Laufzeit des Vertrages. Die Laufzeit der Datenverarbeitung umfasst die vollständige Erfüllung und Abwicklung der vereinbarten Dienstleistungen aus der Leistungsbeschreibung und ihrer Anlagen. Die Geheimhaltungspflicht gilt darüber hinaus unbegrenzt.

§ 2 Außerordentliches Kündigungsrecht

Unabhängig von den in den Vergabeunterlagen enthaltenen außerordentlichen Kündigungsgründen kann der Auftraggeber den gesamten Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn

a. ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen des Vertrages vorliegt oder
b. der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers (in Bezug auf den Datenschutz) nicht ausführen kann oder will oder
c. der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert oder
d. die Grundlage der Vertragserfüllung (im Hinblick auf die Datenverarbeitung) wesentlich verändert wird oder ganz entfällt aufgrund einer Änderung der Rechts- oder Gesetzeslage oder wegen aufsichtsrechtlicher Maßnahmen und zwischen den Parteien eine Einigung zur rechtmäßigen Anpassung der Leistungserbringung an diese Änderungen aufgrund Unmöglichkeit nicht erzielt werden konnte, oder
e. Daten entgegen der Regelung in § 3 dieser Vereinbarung durch den Auftragnehmer an ein Drittland übermittelt werden.

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

§ 3 Ort der Datenverarbeitung

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. Sofern Sozialdaten verarbeitet werden, darf die Datenverarbeitung zusätzlich neben den vorgenannten Staaten auch in der Schweiz erfolgen. 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 bzw. Sozialdaten durch Drittstaaten ist dem Auftraggeber unverzüglich mitzuteilen. In **02-09-04 AVV Anhang (3-5)**, Ziffer 3 sind die Standorte, bei denen personenbezogene Daten bzw. Sozialdaten 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 schriftlichen Zustimmung des Auftraggebers. Bei einer Verlagerung der Standorte bzw. Räumlichkeiten mit vergleichbarem Sicherheitsniveau innerhalb der EU / EWR genügt eine rechtzeitige Information über die Maßnahme. Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

§ 4 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 schriftlich oder in Textform 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 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) Es werden die in **02-09-03 AVV TOMs Informationssicherheit** aufgeführten technischen und organisatorischen Maßnahmen verbindlich festgelegt.

(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 der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind revisionssicher zu dokumentieren.

(5) 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.

§ 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:

a. Die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck

der direkten Kontaktaufnahme in **02-09-04 AVV Anhang (3-5)**, Ziffer 5 mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

b. 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 der Auftragnehmer nachweisbar schriftlich auf die Vertraulichkeit und zur Geheimhaltung unter Hinweis auf die rechtlichen Folgen einer Pflichtverletzung, insbesondere nach § 203 Abs. 4 StGB, verpflichtet und vor der Übermittlung mit den für sie relevanten Pflichten und Bestimmungen zum (Sozial-) Datenschutz vertraut gemacht hat. 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 bzw. 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. Auf diese Weisungs- und Zweckgebundenheit hinsichtlich der Verarbeitung ist jede dem Auftragnehmer unterstellte Person vor der Übermittlung schriftlich hinzuweisen.
c. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c, 32 DSGVO (Einzelheiten in **02-09-03 AVV TOMs Informationssicherheit**).
d. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e. 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 bzw. Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
f. 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.
g. 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.
h. Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieser Vereinbarung.
i. 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.
j. Personenbezogene Daten bzw. Sozialdaten des Auftraggebers dürfen nicht im öffentlichen Raum (z.B. Flughafen, Bahn etc.) verarbeitet werden. Die Verarbeitung der perso-

nenbezogenen Daten bzw. 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 § 4 sind zu beachten.

k. 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 § 4 sind zu beachten.

l. 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 und/oder Gesundheitsdaten 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, insbesondere dessen Abs. 2, bezüglich der räumlichen Beschränkungen der Verarbeitung eingehalten werden.

m. Der Auftragnehmer darf ausschließlich solche Datenverarbeitungsvorgänge durchführen, die ihm innerhalb des Auftragsverhältnisses gemäß Art. 28 DSGVO und sofern Sozialdaten verarbeitet werden, i.V.m. § 80 SGB X vorgegeben werden. Insbesondere ist die Anonymisierung zu eigenen Zwecken, z.B. für eigene (Daten-) Analysen, ausgeschlossen.

n. Analysen des Nutzungsverhaltens und das Erfassen, Sammeln und Verarbeiten personenbezogener Telemetrie- und Diagnosedaten durch den Anbieter des eingesetzten Dienstes zu eigenen Zwecken (z. B. zur Optimierung der eigenen Produkte, Dienste und Geräte per Fernmessung) sind ausgeschlossen. Es dürfen nur die zur Bereitstellung des Dienstes zwingend erforderlichen technischen und sonstigen Informationen verarbeitet werden, sofern dies durch eine gesetzliche Befugnis gerechtfertigt ist.

o. 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.

p. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (z.B. durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren) oder durch sonstige Ereignisse 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.

§ 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 bzw. Sozialdaten nicht ausgeschlossen werden kann.

(2) Der Auftragnehmer darf Unterauftragnehmer (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, die zudem die in diesem Vertrag vereinbarte Rechte und Pflichten berücksichtigt, geschlossen hat.
Der Auftraggeber stimmt der Beauftragung der im **02-09-04 AVV Anhang (3-5)**, Ziffer 4 aufgeführten Unterauftragnehmer zu, soweit jeweils eine vertragliche Vereinbarung nach Maßgabe von Satz 1 geschlossen wurde.

(3) Sollen vom Auftragnehmer während der Vertragslaufzeit andere als im **02-09-04 AVV Anhang (3-5)**, Ziffer 4 benannte Unterauftragnehmer beauftragt oder Standorte von Unterauftragnehmern verlegt/erweitert werden, sind dem Auftraggeber rechtzeitig vor der geplanten Veränderung folgende Unterlagen in Textform zur Zustimmung vorzulegen:
   a. Beschreibung der Arbeiten, die der Unterauftragnehmer ausführen soll,
   b. Bericht der letzten Prüfung (nicht älter als 12 Monate),
   c. Kopie der geplanten vertraglichen datenschutzrelevanten Regelungen (einschließlich der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit sowie ggf. nach § 393 SGB V erforderlicher Unterlagen) mit dem Unterauftragnehmer.

Die Änderung ist nur zulässig, wenn der Auftraggeber dem ausdrücklich zustimmt. Der Auftraggeber wird die Unterlagen binnen 4 Wochen ab Zugang der Änderungsmitteilung und aller vollständigen Unterlagen prüfen. Er wird zustimmen, wenn der Änderung kein sachlicher Grund entgegensteht. Ein sachlicher Grund im Sinne dieser Regelung liegt insbesondere vor, wenn der Unterauftragnehmer-Einsatz gegen die räumlichen Beschränkungen aus § 80 Abs. 2 SGB X verstößt oder der Unterauftragnehmer-Einsatz den Vorgaben aus § 393 SGB V nicht entspricht.

(4) Erfordert abweichend von Absatz 3 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, die zudem die in diesem Vertrag vereinbarten Rechte und Pflichten berücksichtigt, geschlossen hat. Die Unterlagen nach § 5 Abs. 3 von a) bis c) dieser Vereinbarung 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 und 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) Eine weitere Auslagerung durch einen Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des (Haupt-)Auftraggebers mindestens in Textform. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem 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. Diese gelten insbesondere im Hinblick auf die Zweckbindung und die Vertraulichkeit der Datenverarbeitung im Sinne des § 5 dieses Vertrages. Die vertraglichen Vereinbarungen sind durch den Auftragnehmer nachzuweisen und rechtzeitig vor Abschluss des Vertrages vorzulegen.

(8) Der Auftragnehmer hat den Unterauftragnehmer bezüglich der Einhaltung der vertraglichen Pflichten regelmäßig zu prüfen. Das Ergebnis ist zu dokumentieren, mindestens 6 Jahre aufzubewahren und auf Verlangen dem Auftraggeber vorzulegen.

(9) Das Verhalten eines Unterauftragsnehmers ist dem Auftragnehmer wie eigenes Verhalten zuzurechnen.

(10) 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 bzw. Sozialdaten 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.

(11) Umfasst der Leistungsgegenstand Transportdienstleistungen und wird durch den Auftragnehmer für den Datentransport ein Transportunternehmen beauftragt, 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.

§ 7 Kontrollrechte des Auftraggebers und dessen Aufsichtsbehörden

(1) Der Auftraggeber, dessen zuständige Aufsichtsbehörden bzw. ein von ihm beauftragter sachverständiger und 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 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) 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 bzw. 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 einzelner technischer und organisatorischer Maßnahmen, die nicht nur den konkreten Auftrag betreffen, 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. Kosten, die dem Auftraggeber im Zuge der Prüfung entstehen, trägt dieser selbst.

§ 8 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 Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten bzw. Sozialdaten, 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 bzw. Sozialdaten unverzüglich an den Auftraggeber zu melden. In diesem Falle hat der Auftragnehmer sofort alle erforderlichen Maßnahmen zur Sicherung der personenbezogenen Daten bzw. Sozialdaten zu treffen und weitere Anweisungen durch den Auftraggeber abzuwarten.
c. die Verpflichtung, den 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 für dessen Datenschutz-Folgenabschätzung,
e. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

§ 9 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.

§ 10 Rechte von betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er 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, sind die Rechte auf Auskunft, Datenportabilität, Berichtigung, Löschung sowie Einschränkung der Verarbeitung nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen und revisionssicher zu dokumentieren.

§ 11 Löschung und Rückgabe der vertragsgegenständlichen Daten

(1) 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.
(2) 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 bzw. Sozialdaten nach DIN 66399 Teile 1 bis 3 mindestens mit der Schutzklasse 3 und 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.
(3) 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 und keine Sozialdaten enthalten.

Sind von der Vernichtung auch nicht elektronische Unterlagen betroffen, ist ein Vernichtungsprotokoll zu erstellen.

(4) Der Auftragnehmer hat dafür Sorge zu tragen, dass seine IT-Systeme und Verfahren die Möglichkeit bieten, die Berichtigung oder Löschung unzulässiger Daten auch im Einzelfall unverzüglich und systemübergreifend umzusetzen zu können. Der Auftragnehmer hat ein Archivierungs- und Löschkonzept vorzuhalten und dem Auftraggeber bis zur Aufnahme der Auftragsleistung in Kopie zur Verfügung zu stellen.

(5) 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.

§ 12 Ansprechpersonen

Ansprechpersonen des Auftraggebers und des Auftragnehmers ergeben sich aus **02-09-04 AVV Anhang (3-5)**, Ziffer 5.

§ 13 Haftung

(1) Der Auftragnehmer haftet gegenüber dem Auftraggeber im Rahmen der gesetzlichen Datenschutzbestimmungen. Ebenso haftet er für das Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer.

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

§ 14 Sonstiges

(1) 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.

(2) Sollten sich datenschutzrechtliche Änderungen aufgrund Gesetzesänderungen oder Rechtsprechung während der Vertragslaufzeit ergeben, die zu einer Vertragsanpassung führen müssen, verpflichten sich die Vertragspartner Vertragsverhandlungen mit dem Ziel der Einigung aufzunehmen.
(3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.
(4) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der personenbezogenen Daten bzw. Sozialdaten und der zugehörigen Datenträger ausgeschlossen.
(5) Sämtliche Kommunikation zwischen dem Auftragnehmer und dem Auftraggeber sowie zwischen dem Auftragnehmer und den Aufsichten/Prüfdiensten haben in deutscher Sprache zu erfolgen.
(6) Es gilt die Gerichtsstandsvereinbarung des Hauptvertrages.
(7) Der Anhang 1 sowie die Dokumente **02-09-03 AVV TOMs Informationssicherheit** und **02-09-04 AVV Anhang (3-5)** sind Bestandteil dieser Vereinbarung.

Anhang 1: Gegenstand, Art und Zweck der Datenverarbeitung, Datenkategorien und Kategorien betroffener Personen

Gegenstand der Datenverarbeitung
Der Auftragnehmer stellt dem Auftraggeber die erforderliche technische IT-Infrastruktur sowie den operativen Betrieb der Anwendungen bereit. Diese Leistungen dienen dazu, den Auftraggeber in die Lage zu versetzen, seine gesetzlichen Aufgaben und Verpflichtungen im Bereich der Kranken- und Pflegeversicherung ordnungsgemäß und effizient zu erfüllen. Dazu gehören insbesondere die Bereitstellung, Wartung und Weiterentwicklung der IT-Systeme sowie die Sicherstellung eines störungsfreien und sicheren Anwendungsbetriebs.

Art der Datenverarbeitung
Der Auftragnehmer verarbeitet auf der bereitgestellten IT-Infrastruktur personenbezogene Daten sowie Sozialdaten des Auftraggebers im Auftrag. Im Rahmen der Wartung, Pflege und Weiterentwicklung der IT-Infrastruktur sowie im Rahmen des technischen Anwendungsbetriebs kann ein Zugriff auf personenbezogene Daten und Sozialdaten des Auftraggebers durch den Auftragnehmer oder von ihm eingesetzte Unterauftragnehmer erfolgen.

Zweck der Datenverarbeitung
Der Auftraggeber beauftragt den Auftragnehmer mit der Verarbeitung personenbezogener Daten sowie Sozialdaten im Rahmen der Bereitstellung der erforderlichen technischen IT-Infrastruktur und des Betriebs unterschiedlicher IT-Lösungen im Bereich der Kranken- und Pflegeversicherung.
Der Auftragnehmer verarbeitet die personenbezogenen Daten und Sozialdaten des Auftraggebers nur für die in der Leistungsbeschreibung genannten spezifischen Zwecke, sofern keine weiteren Weisungen seitens des Auftraggebers an den Auftragnehmer erteilt werden.
Grundlegender Zweck der Verarbeitung ist:

- Die Bereitstellung, Betrieb und die Wartung operativer Systeme.
- Der Betrieb und die Unterstützung dispositiver Systeme zur Erfüllung gesetzlicher Berichtspflichten.
- Die Sicherstellung der Datenqualität und -integrität innerhalb der eingesetzten Systeme.
- Die Implementierung technischer und organisatorischer Maßnahmen zum Schutz der verarbeiteten Daten.

Kategorien der zu verarbeitenden Daten

bitte ankreuzen	Datenkategorien
☒	Stammdaten
☒	Identitätsdaten
☒	Kommunikationsdaten
☒	Technische Daten
☒	Betriebs- und Geschäftsgeheimnisse
☒	Daten zur Mitgliedschaft / zum Versicherungsverhältnis
☒	Beitragsdaten
☒	Leistungsdaten
☒	Gesundheitsdaten

bitte ankreuzen	Datenkategorien
☒	Daten von Firmenkunden
☒	Daten der Leistungserbringer
☒	Daten der Interessenten
☒	Daten der Nutzenden
☒	Daten zur Pflegeperson
☒	pseudonymisierte Daten
☒	anonymisierte Daten

Kategorien der betroffenen Personen

bitte ankreuzen	betroffene Personen
☒	Versicherte
☒	Interessenten
☒	Nutzer
☒	Firmenkunden
☒	Leistungserbringer
☒	Mitarbeiter
☒	Bewerber
☒	Externe Mitarbeiter
☒	Dienstleister
☒	Pflegepersonen
☒	Bevollmächtigte / Betreuer
☒	Schädiger / Haftungsschuldner
☒	Anspruchsteller
☒	Nicht bei der BARMER versicherte Personen
☒	Abweichende Beitragszahler
☒	Zahlstellen
☒	Geschäfts- und Kooperationspartner