[Anlage zum Hauptvertrag] Stand: 10.07.2026

Vereinbarung nach § 80 SGB X, Art. 28 Datenschutz-Grundverordnung (DS-GVO)

zwischen dem/der
BMW BKK
Mengkofener Str. 6
84130 Dingolfing
vertreten durch den Vorstand Jens Gerhardt

– Verantwortlicher –
nachstehend Auftraggeber genannt

und dem/der
…
…
…
…

– Auftragsverarbeiter –
nachstehend auch Auftragnehmer genannt

Präambel

Die Vertragsparteien haben mit Zuschlag vom _____ (Vergabe-Nummer: CXP4YMTMV3M) einen Vertrag über den zentralen Druckoutput der BMW BKK geschlossen.]

Diese Vereinbarung regelt die Maßnahmen zum Schutz des Sozialgeheimnisses und der Sozialdaten im Sinne des § 35 SGB I oder anderer personenbezogener Daten bei der Datenverarbeitung im Auftrag unter Berücksichtigung des § 80 SGB X, soweit Sozialdaten verarbeitet werden, sowie des Art. 28 DS-GVO.

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag vom _____, auf den hier verwiesen wird (im Folgenden auch Leistungsvereinbarung).

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages bis zur vollständigen Erfüllung und Abwicklung der vereinbarten Leistungen aus der Leistungsbeschreibung. Die Geheimhaltungspflicht gilt darüber hinaus unbegrenzt.

Der Auftraggeber kann den Hauptvertrag 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 Weisung des Auftraggebers nicht ausführen kann oder will oder

c) der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert oder

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

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 oder die Schweiz sind oder für die kein Angemessenheitsbeschluss nach Art. 45 DS-GVO vorliegt.

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

§ 2 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten / Sozialdaten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom 24.09.2026.

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 personenbezogenen 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 Auftraggeber unverzüglich mitzuteilen. In Anhang 2 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 schriftlichen Zustimmung des Auftraggebers. Soweit der Auftraggeber eine Daten-übermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

(2) Art der Daten

Die Art der verwendeten personenbezogenen Daten / Sozialdaten ist in der Leistungsvereinbarung und den Vergabeunterlagen beschrieben

(3) Kategorien betroffener Personen

Die Kategorien der durch den Umgang mit ihren personenbezogenen (Sozial-)Daten im Rahmen dieses Auftrags Betroffenen sind im Hauptvertrag konkret beschrieben unter: § 19

§ 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 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 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen (Einzelheiten in Anhang 1).

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestat-

tet, 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 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme in Anhang 4 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 DS-GVO, § 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 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.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c, 32 DS-GVO (Einzelheiten in Anhang 1).

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 § 6 dieses Vertrages.

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 personenbezogenen 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 § 3 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 § 3 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 DS-GVO 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 DS-GVO 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.

Optional bei der Beauftragung von IT-Dienstleistungen

q) Soweit die Voraussetzungen des § 392 Abs. 6 SGB V oder des § 103a Abs. 6 SGB XI erfüllt sind, verpflichtet sich der Auftragnehmer gegenüber dem Auftraggeber zur Einhaltung des nach § 392 Abs. 3 SGB V einschlägigen branchenspezifischen Sicherheitsstandards in der jeweils gültigen Fassung. Ergänzend verpflichtet sich der Auftragnehmer gegenüber dem Auftraggeber zur Einhaltung der Verpflichtungen zum § 393 SGB V, soweit die Voraussetzungen des § 393 Abs. 1 SGB V erfüllt sind.

r) Technische Überprüfungen (z. B. Penetrationstests) sollen jährlich mit jeweils wechselnden Schwerpunkten durchgeführt werden. Für den Fall, dass die technische Überprüfung bzw. der Penetrationstest-Bericht 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 bzw. personenbezogene Daten nicht ausgeschlossen werden kann. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsdienstleister, dem Postgeheimnis unterliegende Post-/Transportdienstleistungen, Gebäudereinigung sowie sonstige

Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(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 DS-GVO 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 3 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 3** benannte Unterauftragnehmer beauftragt oder Standorte von Unterauftragnehmern verlegt/erweitert werden, sind dem Auftraggeber rechtzeitig vor der geplanten Veränderung geeignete Unterlagen mindestens in Textform zur Zustimmung vorzulegen, insbesondere:

a) Beschreibung der Arbeiten, die der Unterauftragnehmer ausführen soll,
b) Ort der Datenverarbeitung
c) Bericht der letzten Prüfung der technischen und organisatorischen Maßnahmen (möglichst nicht älter als 24 Monate),
d) Kopie der geplanten vertraglichen datenschutzrelevanten Regelungen (einschließlich der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit sowie ggf. nach § 393 SGB V) mit dem Unterauftragnehmer.

Die Änderung der vorlegten Unterlagen in dieser Hinsicht 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 bei der Verarbeitung von Sozialdaten seinen Sitz nicht in einem Land hat, das Mitglied der EU/des EWR ist oder zu dem die Kommission einen Angemessenheitsbeschluss nach Art. 45 DSGVO erlassen hat oder der Unterauftragnehmereinsatz nicht den Vorgaben des § 393 SGB V entsprechen würde.

(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 und - sofern Sozialdaten verarbeitet werden - i.V.m. § 80 SGB X, die zudem die in diesem Vertrag vereinbarten Rechte und Pflichten berücksichtigt, geschlossen hat. Die Unterlagen nach § 5 Abs. 3 von a) bis d) 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) Erbringt der Unterauftragnehmer die vereinbarte Leistung im Sinne von Abs. 1 Satz 2, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

(7) 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.

(8) Die vertraglichen Vereinbarungen zwischen Auftragnehmer und Unterauftragnehmer sind so zu gestalten, dass sie den Bestimmungen des Vertragsverhältnisses zwischen Auftraggeber und Auftragnehmer entsprechen. Dies gilt insbesondere im Hinblick auf die Zweckbindung und die Vertraulichkeit der Datenvereinbarung im Sinne des § 4 dieses Vertrages. Die entsprechenden vertraglichen Vereinbarungen sind durch den Auftragnehmer nachzuweisen und rechtzeitig vor Abschluss des Vertrages vorzulegen.

(9) 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.

(10) Der Auftragnehmer stellt die datenschutzrechtliche Zulässigkeit bei der Erbringung von Leistungen durch Unterauftragnehmer durch entsprechende Maßnahmen sicher. Das Verhalten eines Unterauftragsnehmers ist dem Auftragnehmer wie eigenes Verhalten zuzurechnen.

Optional für Wartungsaufträge etc.:

(11) 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 Wartungsar-

beiten einschließlich der damit Beauftragten mitzuteilen. Sind Störungen im Betriebsablauf zu erwarten oder bereits eingetreten, ist der Vorgang dem Auftraggeber unverzüglich mitzuteilen.

§ 6 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 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.

(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 solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, 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. Kosten, die dem Auftraggeber im Zuge der Prüfung entstehen, trägt dieser selbst. 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 Artikeln 32 bis 36 der DS-GVO 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 und erfolgreichen Cyberangriffen 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, 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) nach Möglichkeit die Unterstützung des Auftraggebers bei der Beantwortung und Umsetzung von Betroffenenrechten mit geeigneten technischen und organisatorischen Maßnahmen (§ 3 und 9 bleiben hiervon unberührt),

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

f) 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 DS-GVO 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 2 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 und keine 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 Ansprechpartner

Ansprechpartner des Auftraggebers ergeben sich aus Anhang 4.

§ 11 Haftung

(1) Der Auftragnehmer haftet gegenüber dem Auftraggeber im Rahmen der gesetzlichen Bestimmungen für Schäden, die infolge schuldhaften Verhaltens gegen Datenschutzbestimmungen und gegen diese Datenschutzvereinbarung entstehen. Ebenso haftet er für schuldhaftes Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer.

(2) Der Auftragnehmer bestätigt, sich gegen die Inanspruchnahme wegen Verletzung von Datenschutzvorschriften hinreichend versichert zu haben und diesen Versicherungsschutz für die gesamte Laufzeit des Hauptvertrages in vollem Umfang aufrechtzuerhalten. Auf Nachfrage des Auftraggebers ist dies durch Vorlage geeigneter Dokumente nachzuweisen.

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

§ 12 Sonstiges

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

(2) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der personenbezogenen Daten/Sozialdaten und der zugehörigen Datenträger ausgeschlossen.

(3) Sämtliche Kommunikation zwischen dem Auftragnehmer und dem Auftraggeber sowie zwischen dem Auftragnehmer und den Aufsichten/Prüfdiensten haben in deutscher Sprache zu erfolgen.

§ 13 Inkrafttreten

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

(2) Es gilt die Gerichtsstandvereinbarung des Hauptvertrages.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Stempel/Unterschrift Auftragnehmer	Stempel/Unterschrift Auftraggeber

Anhang 1.1 zur Vereinbarung über die Einhaltung datenschutzrechtlicher Bestimmungen
Sicherheitskonzept des Auftragnehmers

Angaben zu den umgesetzten technisch-organisatorischen Maßnahmen nach dem Datenschutzkonzept des Auftragnehmers und ihre Dokumentation
Es wird eine detaillierte und prüffähige Beschreibung der umgesetzten technischen und organisatorischen Maßnahmen (TOM) im Datenschutzkonzept gefordert.

Der Auftragnehmer hat spätestens mit dem finalen Angebot eine detaillierte, prüffähige Beschreibung der umgesetzten technischen und organisatorischen Maßnahmen (TOM) vorzulegen, die den Anforderungen des Art. 32 DSGVO genügt.

Die TOM-Dokumentation muss dabei mindestens die folgenden Gewährleistungsziele vollständig adressieren und die jeweils umgesetzten Maßnahmen konkret und nachvollziehbar beschreiben:

a) Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO),
b) Integrität (Art. 32 Abs. 1 lit. b DSGVO),
c) Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO),
d) Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO),
e) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO),
f) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO).

Die Dokumentation muss sich an einem anerkannten Rahmenwerk orientieren. Als geeignete Grundlagen gelten insbesondere:

- ISO/IEC 27001 (Statement of Applicability / Anwendbarkeitserklärung, Risikobehandlungsplan),
- BSI IT-Grundschutz (Sicherheitskonzept nach BSI-Standards 200-1 bis 200-3),
- Standard-Datenschutzmodell (SDM) der Datenschutzkonferenz (Gewährleistungsziele und Referenzmaßnahmenkatalog),
- BSI-Baustein CON.2 Datenschutz (Datenschutzkonzept).

Die bloße Aufzählung von Maßnahmenkategorien oder generischer Beispielmaßnahmen genügt nicht. Die TOM-Dokumentation muss je adressiertem Gewährleistungsziel mindestens enthalten:

- die konkret umgesetzten Maßnahmen mit Bezug zur Auftragsverarbeitung,
- den Geltungsbereich der Maßnahme (Standorte, Systeme, Prozesse),
- die Zuordnung zu den verarbeiteten Datenkategorien und Verarbeitungstätigkeiten dieses Auftrags, soweit auftragsspezifische Maßnahmen erforderlich sind,
- den Umsetzungsstatus und das Datum der letzten Überprüfung.

Liegt eine gültige Zertifizierung oder ein geeigneter Nachweis vor, kann die TOM-Dokumentation durch Verweis auf den zugehörigen Prüfbericht oder das Sicherheitskonzept erfolgen, sofern die oben genannten Gewährleistungsziele daraus nachvollziehbar hervorgehen und der Bezug zur konkreten Auftragsverarbeitung hergestellt wird.

Optional: Anhang 1.2 Angaben zu geeigneten Nachweisen im Kontext Informationssicherheit und Datenschutz

Zertifikate und sonstige geeignete Nachweise	Beschreibung
[Freifeld – Nachweistyp]	[Freifeld]
	Gültigkeit Nachweis Von: [Datum] Bis: [Datum]
	Sind alle Standorte aus Anhang 2 – Geschäftsstandorte zertifiziert? [ja / nein] Wird Zugang zum Zertifizierungs-/Prüfbericht gewährt? Klicken oder tippen Sie hier, um Text einzugeben. [ja / nein]
	Sonstige Anmerkungen, insofern der Nachweis nicht alle Datenverarbeitungsstandorte abdeckt: [Freifeld]
[Freifeld – Nachweistyp]	[Freifeld]
	Gültigkeit Nachweis Von: [Datum] Bis: [Datum]
	Sind alle Standorte aus Anhang 2 – Geschäftsstandorte zertifiziert? [ja / nein] Wird Zugang zum Zertifizierungs-/Prüfbericht gewährt? [ja / nein]
	Sonstige Anmerkungen, insofern der Nachweis nicht alle Datenverarbeitungsstandorte abdeckt: **[Freifeld]**
…	…

Anhang 2 zur Vereinbarung über die Einhaltung datenschutzrechtlicher Bestimmungen

Verzeichnis zu Standorten der Geschäftsräume des Auftragnehmers

Aus der Übersicht sollen alle Standorte über die Geschäftsräume des Auftragnehmers hervorgehen, welche für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten / Sozialdaten des Auftraggebers im Rahmen des vereinbarten Auftragsverhältnisses genutzt werden.

Standorte	postalische Anschrift	Telefonnummer/ Fax-Nr./ E-Mail-Adresse

---

Ort/Datum

Unterschrift/Firmenstempel
des Auftragnehmers

Anhang 3 zur Vereinbarung über die Einhaltung datenschutzrechtlicher Bestimmungen

Aus der Übersicht sollen alle Unterauftragnehmer des Auftragnehmers hervorgehen, welche für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten / Sozialdaten des Auftraggebers und der hierzu für die Wartung der eingesetzten automatisierten Verfahren und Datenverarbeitungsanlagen im Rahmen des vereinbarten Auftragsverhältnisses eingesetzt werden.

Name des Unterauftragnehmers	
Anschrift:	
Aufgabenfeld:	
Zeitraum:	Beginn:_____ Ende_____

Name des Unterauftragnehmers	
Anschrift:	
Aufgabenfeld:	
Zeitraum:	Beginn:_____ Ende_____

Name des Unterauftragnehmers	
Anschrift:	
Aufgabenfeld:	
Zeitraum:	Beginn:_____ Ende_____

Name des Unterauftragnehmers	
Anschrift:	
Aufgabenfeld:	
Zeitraum:	Beginn:_____ Ende_____

_____ _____

Ort/Datum

Unterschrift/Firmenstempel
des Auftragnehmers

Anhang 4:

(1) Ansprechpartner des Auftraggebers ist/sind:

Fachliche Zuständigkeit:	
Name, Vorname:	
Funktionsbezeichnung:	
Erreichbarkeit:	

Datenschutzbeauftragter:	
Name, Vorname:	Arntzen, Christoph
Funktionsbezeichnung:	Datenschutzbeauftragter
Erreichbarkeit:	datenschutzbeauftragter@bmwbkk.de Tel.: 089-382-11164

Ansprechpartner für Datenschutzverletzungen:	
Name, Vorname:	Arntzen, Christoph
Funktionsbezeichnung:	Datenschutzbeauftragter
Erreichbarkeit:	datenschutzbeauftragter@bmwbkk.de Tel.: 089-382-11164

(2) Ansprechpartner des Auftragnehmers[1] ist/sind:

Fachliche Zuständigkeit:	
Name, Vorname:	
Funktionsbezeichnung:	
Erreichbarkeit:	

[1] E-Mail-Kontakte möglichst mit Funktionspostfach

Datenschutzbeauftragter:	
Name, Vorname:	
Funktionsbezeichnung:	
Erreichbarkeit:	

Ansprechpartner für Datenschutzverletzungen:	
Name, Vorname:	
Funktionsbezeichnung:	
Erreichbarkeit:	