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

(1) Diese Datenschutzbestimmungen sind Bestandteil der vereinbarten Leistungen entsprechend des

Vertrages vom 25.06.2007 über die Bearbeitung von Dokumentationsdaten gemäß Disease-Management-Verträge

- im Folgenden Datenstellenvertrag genannt - und somit Grundlage für die Abwicklung der zwischen dem Verantwortlichen und dem Auftragsverarbeiter 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) Der Auftragsverarbeiter verarbeitet zum Zwecke der Erbringung der nach dem Datenstellenvertrag geschuldeten Leistungen Sozialdaten, personenbezogene Daten und/oder Betriebs- und Geschäftsgeheimnisse (nachfolgend Daten genannt) im Auftrag des Verantwortlichen.

§ 2

Grundsätze

(1) Geschäftsgrundlage des Rechtsverhältnisses zwischen Auftragsverarbeiter und Verantwortlichem ist, dass der Datenschutz beim Auftragsverarbeiter nach der Art der zu verarbeitenden Daten den Anforderungen genügt, die für den Verantwortlichen gelten. Der Verantwortliche verarbeitet in der Regel Daten einer hohen bis sehr hohen Schutzbedarfskategorie nach den Klassifikationen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

(2) Der Verantwortliche, die für ihn zuständigen Aufsichtsbehörden oder von ihm beauftragte externe Prüfeinrichtungen sind berechtigt, sich vor Beginn der Auftragsverarbeitung und anschließend regelmäßig von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, vgl. § 9 (Kontrollrechte des Verantwortlichen).

§ 3

Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten werden im Datenstellenvertrag, sowie vor allem in dessen Anlage 1, konkret beschrieben. Gegenstand der Datenverarbeitung sind Sozialdaten gemäß § 67 Abs.2 SGB X.

(2) Die betroffenen personenbezogenen Daten sind in **Anhang G** definiert.

(3) Die zur Anzeige nach § 80 SGB X verpflichteten Körperschaften haben auch bezüglich der o. g. Punkte die Rechtmäßigkeit der Datenverarbeitung durch Auftragsverarbeiter zu prüfen.

(4) Der Auftragsverarbeiter darf keine Verarbeitung von personenbezogene Daten für eigene Zwecke vornehmen, sondern ausschließlich solche Datenverarbeitungsvorgänge durchführen, die ihm im Rahmen der jeweiligen Vereinbarung erlaubt werden. Der Auftraggeber ist auch nicht befugt die personenbezogenen Daten zu anonymisieren, um danach eine Verarbeitung für eigene oder andere Zwecke vorzunehmen.

§ 4

Allgemeine Pflichten des Auftragsverarbeiters

(1) Dem Auftragsverarbeiter ist die Verarbeitung von Daten nur zum Zwecke der Erfüllung des Datenstellenvertrages sowie im Rahmen der schriftlichen Weisungen des Verantwortlichen und nach den datenschutzrechtlichen Vorschriften unter Beachtung der technischen und organisatorischen Maßnahmen gem. § 5 dieser Bestimmungen gestattet. Der Auftragsverarbeiter verwendet die Daten und die daraus erzielten Verarbeitungsergebnisse ausschließlich für die Erfüllung des Datenstellenvertrages. 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 solange auf, wie es für die Erfüllung der genannten Leistungen erforderlich ist. Er gibt sie nicht an Dritte weiter.

(2) Der Auftragsverarbeiter verpflichtet sich, dass die Daten des Verantwortlichen von Daten anderer Verantwortlicher streng getrennt werden. Er verpflichtet sich, keine Kopien oder Duplikate der Datenbestände bzw. Datenbanken ohne Wissen des Verantwortlichen zu erstellen oder die Daten für andere Zwecke zu nutzen. 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.

(3) Der vom Auftragsverarbeiter bestellte Datenschutzbeauftragte (vgl. Art. 37 Abs. 4 DSGVO i.V.m. § 81 Abs. 4 SGB X) wird zum Zweck der direkten Kontaktaufnahme in Anhang A mit Anschrift und telefonischer und elektronischer Erreichbarkeit mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Verantwortlichen unverzüglich mitgeteilt.

(4) Der Auftragsverarbeiter hat den für die Verarbeitung der Daten des Verantwortlichen im Rahmen des Auftragsverhältnisses vorgesehenen Standort/Standorte seiner Geschäftsräume dem Verantwortlichen vor Vertragsschluss in Anhang B schriftlich zu benennen. Eine Veränderung der Standorte oder Räumlichkeiten, in denen Daten des Verantwortlichen verarbeitet werden, oder ein Verlagern der Auftragsdurchführung an eine andere Örtlichkeit als die mit dem Verantwortlichen vereinbarte, bedarf der vorherigen schriftlichen oder elektronischen (Textform) Zustimmung des Verantwortlichen.

(5) Der Auftragsverarbeiter stellt sicher, dass ein Zugriff auf die Daten des Verantwortlichen von Betriebsstätten/Geschäftsräumen und anderen Orten außerhalb der in Anhang B angegebenen Standorte des Auftragsverarbeiters grundsätzlich ausgeschlossen ist.

(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 § 5 dieser Datenschutzbestimmungen erfolgt.

(7) Der Auftrag zur Verarbeitung von Daten darf nur erteilt werden, wenn die Verarbeitung im Inland, in einem anderen Mitgliedstaat der Europäischen Union, in einem diesem

nach § 35 Absatz 7 des Ersten Buches gleichgestellten Staat, oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat oder in einer internationalen Organisation erfolgt. Der Auftragsverarbeiter stellt sicher, dass – sowohl bei gegenwärtigen Verträgen als auch bei künftigen Verträgen – die tatsächliche Datenverarbeitung nach Maßgabe des § 80 Abs. 2 SGB X erfolgt und es zu keiner Datenverarbeitung außerhalb Deutschlands oder des EU-Raumes kommt, soweit für das Drittland kein Angemessenheitsbeschluss besteht.

(8) Sofern wider Erwarten ein Zugriff auf Sozialdaten beim Auftragsverarbeiter durch Dritte, wie z. B. Behörden eines Drittstaates ohne Geltung der DSGVO oder eines Angemessenheitsbeschlusses, erfolgt, ist jeder Zugriff dem Auftraggeber unverzüglich mitzuteilen. Der Auftragsverarbeiter stellt sicher, dass kein Zugriff auf Sozialdaten durch Dritte, wie z. B. Behörden eines Drittstaates ohne Geltung der DSGVO oder eines Angemessenheitsbeschlusses (Beispiel: Zugriff von US-Behörden), erfolgt und das die Daten, die Gegenstand der Geschäftsbeziehung zwischen dem Verantwortlichen und dem Auftragsverarbeiter sind, nicht an Dritte im vorbezeichneten Sinne herausgegeben werden. Dies wird insbesondere auch sichergestellt, wenn sich die Beteiligungsverhältnisse eines in Deutschland oder Europa ansässigen Auftragsverarbeiters in der Weise ändern, dass sich auf der Seite des Auftragsverarbeiters die Beteiligungsverhältnisse (unmittelbar oder mittelbar) ändern.

(9) Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen zu informieren, wenn Aufsichtsbehörden nach § 40 BDSG tätig werden oder eine zuständige Behörde beim Auftragsverarbeiter oder seinen Unterauftragnehmern ermittelt. Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens gemäß § 41 ff. BDSG in Bezug auf die Verarbeitung von Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt. Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen bei dessen nach Artikel 35 DSGVO entstehenden Pflichten bei der Erstellung einer Datenschutz-Folgenabschätzung zu unterstützen.

(10) Sollte das Eigentum des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (z.B. durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren) oder durch sonstige Ereignisse gefährdet werden, hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren. Der Auftragsverarbeiter ist verpflichtet alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber zu unterrichten, dass es sich um Daten des Verantwortlichen handelt, über die er keinerlei Verfügungs- oder sonstige Bestimmungsgewalt oder Eigentumsrechte hat.

§ 5

Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter 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 Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Hierzu ist die Umsetzung von individuell geeigneten technischen und organisatorischen Maßnahmen

notwendig, die ein angemessenes Schutzniveau in Bezug auf tatsächliche oder mögliche Risiken gewährleisten. Die Risiken und daraus resultierenden Maßnahmen sind mindestens für die folgenden Schutzziele zu bewerten: Vertraulichkeit, Integrität, Verfügbarkeit sowie der Belastbarkeit der Systeme und Dienste. Bei der Bewertung sind insbesondere der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die jeweils unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen immer dem technischen Fortschritt und der Weiterentwicklung und sind entsprechend dieser fortlaufend zu gewährleisten, Änderungen sind grundsätzlich 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. auf Anforderung des Verantwortlichen in deutscher Übersetzung in angemessener Zeit zur Verfügung gestellt werden.

(5) Der Auftragsverarbeiter 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.

(6) Erfolgt eine Verarbeitung von Daten des Verantwortlichen unter Nutzung mobiler Arbeitsplätze/ Heim- oder Telearbeitsplätze darf dies nicht im öffentlichen Raum (z.B. Flughafen, Bahn etc.) erfolgen und grundsätzlich 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. Näheres regelt die interne Verfahrensbeschreibung der Datenstelle „Homeoffice in der DMP-Datenstelle“ in der aktuell gültigen Version.

§ 6

Sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der vertraglichen Regelungen die Bestimmungen gemäß Art. 28 bis 33 DSGVO sicherzustellen.

Insofern sind insbesondere folgende Anforderungen zu gewährleisten:

a. Der Auftragsverarbeiter ist verpflichtet, zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2b, 29, 32 Abs. 4 DSGVO für die Erfüllung der vertraglich vereinbarten Leistungen nur Personen einzusetzen, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden sowie regelmäßig informiert und angewiesen werden (Datengeheimnis). Die vorgenannte Verpflichtung hat inhaltlich mindestens dem als Anhang D beigefügten Muster der Verpflichtungserklärung zur Wahrung der Vertraulichkeit zu entsprechen.

b. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Einsicht in Daten nehmen kann, darf diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass der Auftragsverarbeiter gesetzlich zur Verarbeitung verpflichtet ist.

c. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Dies gilt auch, soweit der Verantwortliche 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 Auftragsverarbeiter ausgesetzt ist.

§ 7

Unterauftragnehmer

(1) Unterauftragnehmer jeglichen Grades, die für den Auftragsverarbeiter Daten des Verantwortlichen verarbeiten, dürfen vom Auftragsverarbeiter nur mit vorheriger, schriftlicher Zustimmung des Verantwortlichen eingeschaltet werden. Dies gilt auch für Konzerntöchter. In Anhang E sind die Unterauftragnehmer jeglichen Grades anzugeben. Für bereits bei Zuschlag benannte Unterauftragnehmer jeglichen Grades gilt die Zustimmung als erteilt.

(2) Soweit im Fall der Beauftragung/Zuschlagserteilung ein oder mehrere Unterauftragnehmer jeglichen Grades Daten des Verantwortlichen verarbeiten, müssen sowohl der Auftragsverarbeiter als auch die Unterauftragnehmer jeglichen Grades angeben, welches Aufgabenfeld an welchem Unternehmensstandort ausgeführt werden sollen.

(3) Die vertraglichen Vereinbarungen nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zwischen Auftragsverarbeiter und Unterauftragnehmer jeglichen Grades sind so zu gestalten, dass sie den Bestimmungen des Vertragsverhältnisses zwischen Verantwortlichem und Auftragsverarbeiter in vollem Umfang entsprechen. Dies gilt auch hinsichtlich der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit sowie der Prüf- und Kontrollrechte.

(4) Der Unterauftrag zur Verarbeitung von Daten darf nur erteilt werden, wenn die Verarbeitung im Inland, in einem anderen Mitgliedstaat der Europäischen Union, in einem diesem nach § 35 Absatz 7 des Ersten Buches gleichgestellten Staat, oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat oder in einer internationalen Organisation erfolgt. Der Unterauftragsverarbeiter stellt sicher, dass – sowohl bei gegenwärtigen Verträgen als auch bei künftigen Verträgen – die tatsächliche Datenverarbeitung nach Maßgabe des § 80 Abs. 2 SGB X erfolgt und es zu keiner Datenverarbeitung außerhalb Deutschlands oder des EU-Raumes kommt, soweit für das Drittland kein Angemessenheitsbeschluss besteht. Dies gilt ausdrücklich auch für alle Unterauftragnehmer jeglichen Grades.

(5) Sofern wider Erwarten ein Zugriff auf Sozialdaten beim Unterauftragnehmer durch Dritte, wie z. B. Behörden eines Drittstaates ohne Geltung der DSGVO oder eines Angemessenheitsbeschlusses, erfolgt, ist jeder Zugriff dem Auftraggeber unverzüglich mitzuteilen. Der Unterauftragsverarbeiter stellt sicher, dass kein Zugriff auf Sozialdaten durch Dritte, wie z. B. Behörden eines Drittstaates ohne Geltung der DSGVO oder eines Angemessenheitsbeschlusses (Beispiel: Zugriff von US-Behörden), erfolgt und das die Daten, die Gegenstand der Geschäftsbeziehung zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter sind, nicht an Dritte im vorbezeichneten Sinne herausgegeben werden. Dies wird insbesondere auch sichergestellt, wenn sich die Beteiligungsverhältnisse eines in Deutschland oder Europa ansässigen Unterauftragsverarbeiters in der Weise ändern, dass sich auf der Seite des Unterauftragsverarbeiters die Beteiligungsverhältnisse (unmittelbar oder mittelbar) ändern. Dies gilt ausdrücklich auch für alle Unterauftragnehmer jeglichen Grades.

(6) Der Auftragsverarbeiter hat sich regelmäßig von der Einhaltung der bei den Unterauftragnehmern jeglichen Grades getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren, mindestens 6 Jahre aufzubewahren und auf Verlangen dem Verantwortlichen vorzulegen.

(7) Der Auftragsverarbeiter hat im Vertrag mit den Unterauftragnehmern jeglichen Grades den Auftrag, den Arbeitsablauf und die an den jeweiligen Unterauftragnehmer zum Zwecke der auftragsgemäßen Verarbeitung oder Nutzung gelangenden Daten der Art nach zu bezeichnen sowie die Betriebsstätten/ Geschäftsräume und Standorte in denen die Daten des Verantwortlichen verarbeitet werden, zu benennen.

(8) Die vom Auftragsverarbeiter mit seinen Unterauftragnehmern geschlossenen Verträgen sowie die von diesen Unterauftragnehmern weitergehend geschlossenen Verträgen mit den Unterauftragnehmern jeglichen Grades bedürfen der Schriftform und sind dem Verantwortlichen auf Verlangen vorzulegen.

(9) Das Verhalten des Unterauftragnehmers jeglichen Grades ist dem Auftragsverarbeiter wie eigenes Verhalten zuzurechnen. Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter nach Maßgabe des Art. 28 Abs. 4 DSGVO gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Unterauftragnehmers.

(10) Sollen vom Auftragsverarbeiter während der Vertragslaufzeit andere als in Anhang E benannte Unterauftragnehmer jeglichen Grades beauftragt oder Standorte von Unterauftragnehmern jeglichen Grades verlegt/erweitert werden, sind dem Verantwortlichen rechtzeitig vor der geplanten Veränderung folgende Unterlagen zur Zustimmung vorzulegen:

a. Beschreibung der Arbeiten, die der Unterauftragnehmer ausführen soll

b. Bericht der letzten Prüfung

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

(11) Wenn andere Stellen die Prüfung oder Wartung von automatisierten Verfahren oder von Datenverarbeitungsanlagen vornehmen und dabei ein Zugriff auf die Daten des Verantwortlichen nicht ausgeschlossen werden kann, gilt der § 80 Abs. 5 SGB X analog. Derartige Beauftragungen sind dem Verantwortlichen rechtzeitig vor Vertragsabschluss mitzuteilen. Sind Störungen im Betriebsablauf zu erwarten oder bereits eingetreten und ist eine kurzfristige Beauftragung eines Unterauftragnehmers unabdingbar, ist der Vertrag unverzüglich nachzuholen. Bereits bei Zuschlag bestehende Vertragsbeziehungen sind in Anhang F aufzuführen.

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

§ 8

Auskunft, Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen im Rahmen seiner Pflichten gegenüber Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Information unverzüglich zur Verfügung zu stellen.

(2) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken.

(3) Wenn von Betroffenen die Rechte gemäß der Artt. 15 – 18 DSGVO i. V. m. §§ 81, 83 und 84 SGB X geltend gemacht werden, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten. Er stellt sicher, dass die Daten von Betroffenen bei Bedarf auf Anweisung des Verantwortlichen berichtigt, gelöscht oder gesperrt werden können.

(4) Soweit vom Leistungsumfang umfasst sind die Betroffenenrechte nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen. Hierzu gehört die Umsetzung des Löschkonzeptes, Berichtigung und Auskunft.

§ 9

Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche oder von ihm beauftragte externe Prüfeinrichtungen werden sich vor Beginn der Auftragsverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen überzeugen.

(2) Der Auftragsverarbeiter gewährt dem Verantwortlichen bzw. den für den Verantwortlichen zuständigen Aufsichtsbehörden oder von ihm beauftragte externe Prüfeinrichtungen in den Betriebsräumen des Auftragsverarbeiters zu jeder geschäftsmäßigen Zeit nach vorheriger schriftlicher oder elektronischer (Textform) Ankündigung ein Prüfrecht. Das Prüfrecht umfasst die Besichtigung von Grundstücken und Geschäftsräumen, Auskünfte zur Vertragsausführung, Einsicht in Papierunterlagen als auch die Einsichtnahme in die beim Auftragsverarbeiter gespeicherten Daten des Verantwortlichen, 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.

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

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

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

(5) Die genannten Rechte des Verantwortlichen können auch durch Mitarbeiter von damit beauftragten Fremdfirmen wahrgenommen werden. Sofern Mitarbeiter von Fremdfirmen mit den genannten Kontrollmaßnahmen beauftragt werden, sind diese vom Verantwortlichen ausdrücklich auf die Geheimhaltung aller in diesem Zusammenhang erlangten Kenntnisse, Daten sowie Betriebs- und Geschäftsgeheimnisse zu verpflichten.

(6) Die Rechte der für den Auftragsverarbeiter zuständigen Aufsichtsbehörde bleiben davon unberührt.

§ 10

Weisungsbefugnis des Verantwortlichen

Der Verantwortliche ist befugt, erforderlichenfalls schriftliche Weisungen im Rahmen der Artt. 28, 32 DSGVO zur Ergänzung der beim Auftragsverarbeiter vorhandenen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit zu erteilen.

§ 11

Mitteilungspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artt. 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Verzeichnis von Verarbeitungstätigkeiten, Meldepflichten bei Datenschutzverletzungen, gegebenenfalls erforderlichen 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 personenbezogener Daten - auch durch seine Mitarbeiter oder Unterauftragnehmer - gemäß Art. 33 Abs. 2 und 3 DSGVO unverzüglich an den Verantwortlichen zu melden. In diesem Falle hat der Auftragsverarbeiter sofort alle erforderlichen Maßnahmen zur Sicherung der Daten zu treffen und weitere Anweisungen durch den Verantwortlichen abzuwarten.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Meinung ist, dass eine Weisung des Verantwortlichen gegen die DSGVO oder eine andere Datenschutzvorschrift verstößt. Der Auftragsverarbeiter ist in diesem Fall berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

§ 12

Löschung und Rückgabe von personenbezogenen Daten

(1) Sämtliche Daten und Unterlagen sowie Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem in § 1 dieser Datenschutzbestimmungen genannten Zwecke in die Verfügungsgewalt des Auftragsverarbeiters gelangt sind, hat dieser entsprechend der jeweiligen Vereinbarungen im Einzelfall bzw. nach Abschluss der vertraglichen Arbeiten dem Verantwortlichen auf seine Kosten auszuhändigen bzw. zu übermitteln.

(2) Auf Verlangen des Verantwortlichen hat der Auftragsverarbeiter in seinem Besitz befindliche Daten bzw. Datenbestände (z.B. physische Datenträger, elektronische Dateien oder Datenbanken in seinen DV-Systemen) nichtreproduzierbar auf seine Kosten zu löschen bzw. physisch zu vernichten. Die Vernichtung hat nach DIN 66399 Teile 1-3 mindestens mit Sicherheitsstufe P-4, F-4, O-4, T-4, H-4 bzw. E-4 zu erfolgen (Schutzklasse 3). Die Datenlöschung hat nach anerkanntem BSI-Standard 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 Verantwortlichen für jede weitere Verarbeitung einzuschränken.

(3) Die Löschung und Vernichtung hat der Auftragsverarbeiter in geeigneter Weise zu protokollieren und auf Verlangen dem Verantwortlichen vorzulegen. Im Zweifelsfall sind geeignete Maßnahmen mit dem Verantwortlichen abzustimmen.

(4) Endet das Vertragsverhältnis, hat der Auftragsverarbeiter gegenüber dem Verantwortlichen 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.

§ 13

Haftung

(1) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen nach Maßgabe der gesetzlichen Bestimmungen für Schäden, die infolge seines oder seiner Unterauftragnehmer (§ 7) Verhaltens gegen Datenschutzbestimmungen und/oder durch die Verletzung dieses Vertrages entstehen. Etwaige vertragliche Haftungsbeschränkungen gelten nicht für Ansprüche, die dem Verantwortlichen gemäß Art. 82 Abs. 5 DSGVO gegen den Auftragsverarbeiter zustehen.

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

§ 14

Nebenabreden

Änderungen und Nebenabreden zu diesen Datenschutzbestimmungen bedürfen der Schriftform.

§ 15

Laufzeit des Vertrages und Kündigung

(1) Beginn und Ende des Auftragsverhältnisses sind im Datenstellenvertrag geregelt. Unabhängig davon unterliegen der Auftragsverarbeiter und dessen eingesetzte Mitarbeiter auch nach dem im Datenstellenvertrag genannten Vertragsende hinaus hinsichtlich der im Rahmen des Auftragsverhältnisses übermittelten Daten und bekannt gewordenen Vertraulichkeiten der Geheimhaltungspflicht.

(2) Die Verletzung von gesetzlichen oder vertraglichen Datenschutzbestimmungen durch den Auftragsverarbeiter ist ein wichtiger Grund für den Verantwortlichen, das im Datenstellenvertrag vorbehaltene Recht zur außerordentlichen Kündigung auszuüben.

(3) Der Verantwortliche kann den Datenstellenvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn

a. ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutz-vorschriften oder diese Datenschutzbestimmungen vorliegt (ein schwerwiegender Verstoß ist u.a. anzunehmen, wenn gegen die in § 4 Abs. 7, 8 bzw. § 5 Abs. 4, 5 bezeichneten Vorgaben verstoßen wird) oder

b. der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will oder

c. der Auftragsverarbeiter 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.

§ 16

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.

§ 17

Inkrafttreten

(1) Diese Datenschutzbestimmungen treten mit Inkrafttreten der 14. Ergänzungsvereinbarung zum Datenstellenvertrag ab 01.04.2024 in Kraft.

(2) Es gilt die Gerichtsstandsvereinbarung des Datenstellenvertrages.

Anhänge:

Anhang A	Datenschutzbeauftragter, IT-Verantwortlicher und Informationssicherheitsbeauftragter des Bieters/Auftragsverarbeiters
Anhang B	Standorte der Geschäftsräume des Auftragsverarbeiters
Anhang C	Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit
Anhang D	Muster der Verpflichtungserklärung zur Wahrung der Vertraulichkeit
Anhang E	Übersicht über die Unterauftragnehmer
Anhang F	Übersicht über die Wartungsfirmen
Anhang G	Datenkategorien und Personengruppen