Anlage V3

Regelungen zur Auftragsverarbeitung

1. Konkretisierung des Auftragsinhalts

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers (AN):

Mit der Durchführung von hausarztzentrierten Versorgungsverträgen (HzV) geht gemäß § 73b Abs. 7 SGB V die gesetzliche Verpflichtung einher, die morbiditätsbedingte Gesamtvergütung (MGV, d.h. der budgetierte Teil der ambulanten ärztlichen Gesamtvergütung) zu bereinigen. Gegenüber allen Kassenärztlichen Vereinigungen (KV) ist demzufolge ein Teil der Gesamtvergütung zu kürzen (zu bereinigen). Die MGV-Bereinigung ist mit einem quartalsbezogenen und fristgebundenen Datenaustausch mit allen Kassenärztlichen Vereinigungen im Bundesgebiet verbunden.

Insbesondere dieser quartalsweise Datenaustausch ist unter Berücksichtigung der Beschlussvorgaben des Bewertungsausschusses sowie der regionalspezifischen Bereinigungsverträge durch den AN sicherzustellen. Damit verbunden ist die Ermittlung der quartalsbezogenen Bereinigungsbeträge und deren Abstimmung mit allen Kassenärztlichen Vereinigungen (operativer Bereinigungsgeschäft).

Die Einzelheiten ergeben sich detailliert aus der Anlage V2 TK Leistungsbeschreibung (LB).

(1) Art und Zweck der Erhebung, Verarbeitung und Nutzung von personenbezogenen (Sozial)- Daten

Der AN übernimmt für die TK das operative Bereinigungsgeschäft. Hierzu zählt insbesondere die Annahme von Sozialdaten, die Verarbeitung zu quartals-, KV- und vertragsspezifischen Bereinigungsdaten (Satzarten), die Übermittlung dieser Daten an die jeweiligen Kassenärztlichen Vereinigungen und die Abstimmung der Inhalte. Auch die Rückführung von Sozialdaten an die TK ist Bestandteil der Aufgabe.

Die für die MGV-Bereinigung relevanten Beschlüsse des Bewertungsausschusses sowie alle vertraglichen Regelungen sind vom AN zu berücksichtigen.

Bereits vor der vertraglich definierten Leistungsübernahme erfolgt im Rahmen der Implementierung/Testung ein Testdatenaustausch zwischen TK und AN. Es handelt sich hierbei um Echtdaten, anhand derer ein Bereinigungsquartal testweise durchgespielt wird.

Die Einzelheiten ergeben sich detailliert aus der Anlage V2 TK Leistungsbeschreibung (LB).

(2) Umfang der Erhebung, Verarbeitung und Nutzung von personenbezogenen (Sozial)-Daten

Grundsätzlich erfolgt die MGV-Bereinigung quartals-, KV- und vertragsspezifisch. Es werden hierzu Sozialdaten von Versicherten und Ärzten verarbeitet, die als HZV-Teilnehmer im betreffenden Bereinigungsquartal gemeldet sind oder als ehemalige HZV-Teilnehmer zu berücksichtigen sind.

Es werden von der TK bereinigungsquartalsbezogene Teilnehmerinformationen für ca. 1,25 Mio HZV-Versichertenteilnahmen und 14.200 HZV-Arztteilnahmen übermittelt (Stand Bereinigungsquartal 3/2026) – tendenziell mit positivem Anstieg. Für alle Versichertenteilnehmer werden Versichertenstammdaten sowie relevante historische Versichertenstammdaten zur Verfügung gestellt. Zusätzlich werden die quartalsbezogenen Einzelfallnachweise für alle Neueinschreiber und Bestandteilnehmer (ca. 30 Mio Datensätze/Quartal) geliefert. Für die ersten 4 Bereinigungsquartale ab Leistungsübernahme durch den AN übermittelt die TK die erforderlichen Sozialdaten der jeweiligen Vorjahresquartale in Form der Satzarten. Für die Realisierung von quartalsbezogenen Teilnehmerkorrekturen (L05-Teilnehmerkorrekturlieferung) erhält der AN von der TK aktualisierte Teilnehmerinformationen bzgl. der Versicherten und Ärzte.

Der AN verarbeitet die Sozialdaten für die quartalsbezogenen Erstdatenlieferungen sowie alle Korrektur- und Spitzabrechnungsdatenlieferungen sowie spätere Teilnehmerkorrekturdatenlieferungen.

Für die jahresbezogene Datenlieferung an das Institut des Bewertungsausschusses gem. gültiger Beschlüsse des Bewertungsausschusses liefert die TK dem AN zusätzlich HZV-Diagnosedaten für einen Teil der HZV-Teilnehmenden (Geburtstagsstichprobe) für das betreffende Berichtsjahr zur Erstellung der Satzart 005.

Die Einzelheiten ergeben sich detailliert aus der Anlage V2 TK Leistungsbeschreibung (LB).

(3) Art der personenbezogenen (Sozial)-Daten

Für die Erstellung der Testdaten und der ersten vier Bereinigungsquartale ab Leistungsübernahme erhält der AN von der TK die Satzarten L01-L10 (inkl. L04 oder L05) des jeweiligen Vorjahresquartal.

Darüber hinaus stellt die TK dem AN die für das jeweilige Bereinigungsquartal relevanten Versichertenstammdaten wie Versichertennummer, Name, Vorname, Geburtsdatum, Geschlecht, PLZ und Wohnort, Versichertenstammdaten aus dem Vorjahresquartal wie PLZ und Wohnort sowie ambulante Abrechnungsdaten/ Einzelfallnachweise (inkl. Gebührenordnungsposition, abrechnender und überweisender Arzt, Abrechnungsdatum), relevante Informationen von der Gesundheitskarte (bspw. Status SVA, BVG) sowie HZV-Teilnahmeinformationen (Beginndatum, ggf. Teilnahmeende, eingeschriebener Arzt und Betriebsstätte) zur Verfügung. Von der TK werden zudem Informationen von den an der HzV teilnehmenden Ärzten bzgl. Name, Vorname, KV-Zugehörigkeit, lebenslange Arztnummer, Facharztgruppenschlüssel, Betriebsstätte, HZV-Teilnahmebeginn und ggf. Teilnahmeendedatum sowie die Information zu den bei ihnen teilnehmenden HZV-

Versicherten übermittelt. Darüber hinaus sind in den Sozialdaten für die Interpretation der Datensätze entsprechende IDs, Kennzeichen und Schlüssel sowie auswertungsrelevante Zusatzinformationen enthalten.

(4) Kategorien betroffener Personen

- *An der Hausarztzentrierten Versorgung können grundsätzlich alle Versicherte der TK ohne Einschränkungen teilnehmen. In einigen Vertragsregionen gelten Alterseinschränkungen (bspw. keine Teilnahme unter 18 Jahre) oder Ausschlüsse bei Teilnahme an mehreren sich ausschließenden Selektivverträgen (bspw. DMP-Programme).*
- *Leistungserbringer mit den gültigen Zugangsvoraussetzungen gemäß der HZV-Verträge.*

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Soweit Sozialdaten betroffen sind, müssen die Voraussetzungen des § 80 SGB X beachtet werden.

Der Standort der Geschäftsräume des Auftragnehmers, an denen die Daten verarbeitet werden (Ort der Datenverarbeitung), ergibt sich aus der Anlage "Angebot". Sofern die Anlage nicht verwendet wird, ist der Ort der Datenverarbeitung dem Auftraggeber in Textform mitzuteilen. Eine Veränderung der Orte der Datenverarbeitung oder ein Verlagern der Auftragsdurchführung an eine andere Örtlichkeit als die mit dem Auftraggeber vereinbarte, ist dem Auftraggeber vorab anzuzeigen.

2. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung – insbesondere hinsichtlich der konkreten Auftragsdurchführung – zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit gem. Ziffer 6 des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c und 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 (vgl. die Auflistung der technisch-organisatorischen Maßnahmen am Ende dieser Anlage).

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind revisionssicher zu dokumentieren.

(4) Der Auftragnehmer hat die technisch-organisatorischen Maßnahmen in einem Sicherheitshandbuch zu dokumentieren.

Hiervon wird abgewichen, wenn gemäß § 80 Abs. 5 SGB X eine Prüfung oder Wartung automatisierter Verfahren erfolgt und die Tätigkeit in den Räumlichkeiten der Auftraggeberin vorgenommen wird.

(5) Das Sicherheitshandbuch und Dokumente, die in unmittelbarem Zusammenhang mit der Auftragsverarbeitung stehen, müssen in deutscher Sprache verfasst bzw. in deutscher Übersetzung bereitgehalten werden. Dieses gilt insbesondere für sämtliche Dokumentationen zu den technischen und organisatorischen Maßnahmen, Dokumentationen von Regelungen zum Datenschutz und zur Informationssicherheit und Audit- bzw. Prüfberichte.

(6) 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.

3. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. 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 Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO sowie des Sozialgeheimnisses nach § 35 Abs. 1 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, schriftlich verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Dies umfasst die Verpflichtung zur Geheimhaltung auch über das bestehende Dienst- oder Beschäftigungsverhältnis hinaus. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

b) 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 spätestens 14 Tage nach Vertragsunterzeichnung mitgeteilt.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c und 32 DSGVO.

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit den Aufsichtsbehörden 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 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.

h) Sollte das Eigentum des Auftraggebers 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 Auftraggeber unverzüglich darüber zu

informieren. Der Auftragsverarbeiter 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.

i) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 6 dieses Vertrages.

j) Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

k) Der Auftragsverarbeiter führt entsprechend den Vorgaben den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

l) Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home-Office, mobiles Arbeiten) bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann.

m) 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 die technische und organisatorische Sicherstellung der Infrastruktur des Anbieters den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entspricht. Soweit Sozialdaten und / oder Gesundheitsdaten verarbeitet werden, hat der Auftragnehmer die Vorgaben des § 393 SGB V und die Anforderungen des § 80 SGB X, insbesondere Abs. 2, bezüglich der räumlichen Beschränkungen der Verarbeitung einzuhalten.

5. Unterauftragsverhältnisse

(1) Die vertraglichen Vereinbarungen zwischen Auftragnehmer und Unterauftragnehmer sind derart auszugestalten, dass sowohl die gesetzlichen Bestimmungen zum Datenschutz, die für den Auftraggeber und den Auftragnehmer gelten, als auch die mit dem Auftragnehmer vertraglich vereinbarten Bestimmungen zum Datenschutz von dem Unterauftragnehmer einzuhalten sind. Die Einhaltung dieser Bestimmungen beim Unterauftragnehmer hat der Auftragnehmer zu gewährleisten. In dem mit dem Unterauftragnehmer zu schließenden Vertrag ist zudem der Arbeitsablauf und die von dem Auftragnehmer an den Unterauftragnehmer abzugebenden Tätigkeiten zum Zwecke der auftragsgemäßen Datenerhebung, -verarbeitung und -nutzung konkret zu beschreiben. Die vorgenannten Verpflichtungen gelten auch für Unterauftragnehmer, welche lediglich Wartungsarbeiten beim Auftragnehmer in Anspruch nehmen oder dessen Daten löschen bzw. vernichten, wenn in diesem Rahmen nicht ausgeschlossen werden kann, dass der Unterauftragnehmer innerhalb seiner vertraglichen Vereinbarung mit dem Auftragnehmer

auch Zugriff auf personenbezogene Daten, Sozialdaten und/oder diese gleichgestellten Daten als Geschäfts- und Betriebsgeheimnisse hat bzw. haben kann.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher dokumentierter Zustimmung (mind. Textform) des Auftraggebers beauftragen. Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind datenschutzrechtlich zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber schriftlich zugestimmt hat,
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

Die im Rahmen des Auftrags beauftragten Unterauftragnehmer sind in der Anlage "Angebotsschreiben" aufzuführen. Sofern die Anlage nicht verwendet wird, sind die beauftragten Unterauftragnehmer dem Auftraggeber in Textform mitzuteilen. Änderungen sind dem Auftraggeber unverzüglich und rechtzeitig zur Zustimmung mitzuteilen.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller gesetzlichen und vertraglich vereinbarten Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform), und sämtliche vertragliche Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(5) Die vertraglichen Vereinbarungen zwischen Auftragnehmer und Unterauftragnehmer sind so zu gestalten, dass sie den Bestimmungen des Vertragsverhältnisses zwischen Auftraggeber und Auftragnehmer entsprechen. Der Auftragnehmer hat den Unterauftragnehmer bezüglich der Einhaltung der vertraglichen Pflichten regelmäßig zu prüfen. Das Ergebnis ist zu dokumentieren und auf Verlangen dem Auftraggeber vorzulegen.

(6) Bei der Unterbeauftragung sind dem Auftraggeber Kontrollrechte entsprechend dieser Vereinbarung einzuräumen.

(7) Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der jeweilige Auftragsverarbeiter nach Maßgabe des Art. 28 Abs. 4 DSGVO gegenüber dem jeweiligen Auftraggeber für die Einhaltung der Pflichten jenes anderen Unterauftragnehmers.

6. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber und dessen zuständige Aufsichtsbehörden und sonstige Beauftrage des Auftraggebers (z.B. Prüfdienstleister oder Prüfgemeinschaften) haben das Recht, im

Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder diese im Einzelfall durch zu benennende Prüfer durchführen zu lassen. Sie haben das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. In dringenden Fällen kann eine kurzfristige Prüfung durch den Auftraggeber durchgeführt werden.

(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) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, erfolgen durch
   a) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO und/oder
   b) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) und/oder
   c) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. BSI-Grundschutz oder ISO 27001).

Die vorgenannten Nachweise dienen dem Auftraggeber für seine Überzeugungsbildung gemäß Absatz 2 und ersetzen diese nicht.

(4) Für die Durchführung von Kontrollen durch den Auftraggeber kann der Auftragnehmer keinen Vergütungsanspruch geltend machen.

7. Mitteilungspflichten bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen der Aufsichtsbehörden. Hierzu gehören u.a.

   a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,
   b) die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden. In diesem Falle hat der Auftragsverarbeiter sofort die erforderlichen Maßnahmen zur Sicherung der Daten zu treffen und weitere Anweisungen durch den Auftraggeber abzuwarten.
   c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung,
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8. Weisungsbefugnis des Auftraggebers

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

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. 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.

(4) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung durch den Verantwortlichen erteilen.

(5) Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Eigenständige Datenverarbeitungsvorgänge des Auftragsverarbeiters, wie beispielweise eine Anonymisierung zur Auswertung zu eigenen Zwecken, sind ausgeschlossen.

9. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Zustimmung 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Vertrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Daten, erstellte Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

10. Haftung und Schadensersatz

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

(2) Der Auftragnehmer haftet gegenüber dem Auftraggeber gemäß den vertraglichen Regelungen. Im Übrigen gelten die gesetzlichen Regelungen.

Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B. Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen,
- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B. (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern,
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen,
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing,
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO, Art. 25 Abs. 1 DSGVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur,
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B. Protokollierung, Dokumentenmanagement

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B. Backup-Strategie (online/offline, on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne,
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)

- Datenschutz-Management,
- Incident-Response-Management,
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO),
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B. eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen,
- Risikoanalyse zur Ableitung der Sicherungsmaßnahmen einschließlich Dokumentation