Vereinbarung zur Auftragsverarbeitung nach § 28 DSGVO („AV-Vertrag")

Für Praxispartner im Rahmen des Vertrags zur besonderen Versorgung nach § 140a SGB V zwischen der GESUNDES KINZIGTAL GmbH und der AOK Baden-Württemberg

Der Vertrag zur Auftragsverarbeitung (nachfolgend „AV-Vertrag") konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz nach der Datenschutzgrundverordnung (DSGVO), dem BDSG-neu und der ärztlichen Schweigepflicht nach §§ 203, 204 StGB. Der AV-Vertrag findet auf alle Tätigkeiten Anwendung, die mit der Inanspruchnahme Support- und Wartungsdienstleitungen (nachfolgend „BVGK-Vertrag" genannt) in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder beauftragte Dritte (siehe Annex 3 zum AV-Vertrag) – im Folgenden „Support" genannt – personenbezogene Daten des Auftraggebers, seiner Patienten oder seiner Vertragspartner tatsächlich oder möglicherweise verarbeiten.

Die GESUNDES KINZIGTAL GmbH stellt dem Praxispartner die jeweils gültige Fassung auf dem BVGK-Portal zur Verfügung.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Gegenstand, Umfang sowie Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer nach diesem AV-Vertrag sind folgende:

Umfang und Zweck der Datenverarbeitung	Kategorien betroffener Personen	Art der Daten
Softwareinstallation	• Patient • Auftraggeber • Mitarbeiter • Vertragspartner	• Personalstammdaten • Gesundheitsdaten / biometrische Daten / genetische Daten • Kommunikationsdaten • Vertragsstammdaten
Unterstützung beim Softwarebetrieb	• Patient • Auftraggeber • Mitarbeiter • Vertragspartner	• Personalstammdaten • Gesundheitsdaten / biometrische Daten / genetische Daten • Kommunikationsdaten • Vertragsstammdaten
Unterstützung und Hilfestellung bei Störungen im IT-System des Auftraggebers	• Patient • Auftraggeber • Mitarbeiter • Vertragspartner	• Personalstammdaten • Gesundheitsdaten / biometrische Daten / genetische Daten • Kommunikationsdaten • Vertragsstammdaten

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers nach Maßgabe des Punkt 1 des AV-Vertrages. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der geltenden Datenschutzgesetze (insbesondere der DSGVO, des BDSG-neu sowie der §§ 203, 204 StGB) und insoweit vor

allem für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO). Der Auftraggeber entscheidet allein über die Mittel und Zwecke der Verarbeitung nach diesem AV-Vertrag. Der Auftragnehmer wird den Auftraggeber, soweit möglich, in angemessener Weise unterstützen. Die Weisungen werden anfänglich durch diesen AV-Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen (z. B. im Rahmen der Support- und Wartungsdienstleitungen) sind unverzüglich schriftlich oder in Textform zu bestätigen.

(2) Die Verarbeitung der personenbezogenen Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung der Datenverarbeitung in einen anderen Staat als die in Satz 1 genannten bedarf der vorherigen dokumentierten Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO) und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet die personenbezogenen Daten des Auftraggebers ausschließlich zum Zwecke der Erbringung von Support- und Wartungsdienstleistungen nach dem Hauptvertrag sowie im Auftrag und gemäß den Weisungen des Auftraggebers. Die Verwendung der personenbezogenen Daten für andere als die in Punkt 1 des AV-Vertrages genannten Zwecke ist ausgeschlossen.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber schriftlich oder in Textform bestätigt oder abgeändert wurde. Das Recht zur Kündigung des Auftraggebers nach § 8 Abs. 2 des AV-Vertrages bleibt unberührt.

(3) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des Art. 32 DSGVO genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

Das vom Auftragnehmer insoweit erarbeitete Datenschutzkonzept ist in Annex 1 zum AV-Vertrag beschrieben. Dem Auftraggeber sind diese vom Auftragnehmer nach Maßgabe des Annex 1 ergriffenen technischen und organisatorischen Maßnahmen bekannt. Die Vertragsparteien stimmen darin überein, dass diese für die Risiken der zu verarbeitenden personenbezogenen Daten ein angemessenes Schutzniveau bieten. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt

sein muss, dass das zum Zeitpunkt des Vertragsbeginns vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(4) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Art. 12 ff. DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

(5) Der Support wird vom Auftragnehmer schriftlich darauf verpflichtet, dauerhaft – auch nach Beendigung des Arbeitsverhältnisses – keine Informationen, die sie im Rahmen ihrer Tätigkeit nach dem Hauptvertrag und diesem AV-Vertrag erlangen, an Dritte weiterzugeben. Soweit der Support im Rahmen dieser Tätigkeit personenbezogene Daten des Auftraggebers, die unter die ärztliche Schweigepflicht fallen, zur Kenntnis nehmen können, sind sie „sonstige mitwirkende Personen" i.S.d. § 203 Abs. 3 StGB.
Die Mitarbeiter des Auftragnehmers sowie beauftragte Dritte sind über die ihnen obliegenden Pflichten im Zusammenhang mit der ärztlichen Schweigepflicht, die dem Auftraggeber gegenüber den Patienten obliegt, umfassend aufzuklären. Die schriftliche Verpflichtungserklärung nach § 3 Abs. 5 S. 1 des AV-Vertrages hat sich auf diese Pflichten nach den Regeln der ärztlichen Schweigepflicht zu erstrecken. Auf Aufforderung hat der Auftragnehmer die Erfüllung seiner Pflichten dem Auftraggeber in angemessener Weise nachzuweisen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Vertragsverhältnisses zwischen den Vertragsparteien fort.

(6) Sollten die nach diesem AV-Vertrag oder dem Gesetz geltenden datenschutzrechtlichen Bestimmungen durch Störungen, Verstöße durch Mitarbeiter des Auftragnehmers oder durch sonstige Ereignisse und Maßnahmen Dritter verletzt oder gefährdet worden sein, informiert der Auftragnehmer den Auftraggeber darüber unverzüglich. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Meldungen nach Art. 33 und Art. 34 DSGVO für den Auftraggeber wird der Auftragnehmer nur nach vorheriger Absprache und nach schriftlicher oder in Textform erteilter Weisung des Auftraggebers vornehmen.

(7) Der Auftragnehmer hat einen Datenschutzbeauftragten benannt. Name und Kontaktdaten des Datenschutzbeauftragten sind in Annex 2 zum AV-Vertrag aufgeführt. Änderungen in der Person des Datenschutzbeauftragten sind dem Auftragnehmer erlaubt und der Annex 2 zum AV-Vertrag daraufhin entsprechend anzupassen.

(8) Der Auftragnehmer gewährleistet seinen Pflichten nach Art. 32 DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu implementieren und, wenn erforderlich, durchzuführen. Auf Aufforderung hat der Auftragnehmer die Erfüllung seiner Pflichten dem Auftraggeber in angemessener Weise nachzuweisen.

(9) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und die Löschungsanweisung rechtmäßig ist. Auch im Übrigen hat der Auftragnehmer personenbezogene Daten, Datenträger sowie sämtliche sonstige Datenmaterialien mit personenbezogenen Daten einschließlich etwaiger Kopien nach Beendigung des Einzelauftrages unter Berücksichtigung

etwaiger gesetzlicher Speicher- und Aufbewahrungspflichten unverzüglich und dauerhaft löschen.
Ist eine Löschung dem Auftragnehmer aus rechtlichen oder vertraglichen Gründen nicht erlaubt, teilt er dies dem Auftraggeber schriftlich oder in Textform mit.
Ist eine Löschung für den Auftragnehmer nur mit unverhältnismäßigem Aufwand möglich, können die Vertragsparteien schriftlich eine Sperrung der Daten vereinbaren.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Erfüllung des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

4. Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt § 3 Abs. 10 des AV-Vertrages entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer schriftlich oder in Textform einen Ansprechpartner für die im Rahmen des Haupt- und dieses AV-Vertrages anfallenden Datenschutzfragen. Im Falle der Pflicht zur Benennung eines Datenschutzbeauftragten nach Art. 37 DSGVO gibt der Auftraggeber dem Auftragnehmer unaufgefordert den Namen und die Kontaktdaten des benannten Datenschutzbeauftragten schriftlich oder in Textform bekannt. Änderungen in der Person des Datenschutzbeauftragten sind dem Auftragnehmer erlaubt und dem Auftraggeber auf Nachfrage mitzuteilen.

(4) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner personenbezogenen Daten wenden sollte, wird der Auftragnehmer diesen Antrag unverzüglich an den Auftraggeber weiterleiten.

5. Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollte im Einzelfall der Auftraggeber von seinem Kontrollrecht Gebrauch machen und insoweit eine Begehung beim Auftragnehmer verlangen, wird diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf die Zulassung der Begehung von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der personenbezogenen Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen.
Der Auftraggeber ist grundsätzlich berechtigt, die Begehung durch einen bestellten Prüfer durchführen zu lassen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer das Recht, die Inspektion durch diesen Prüfer zu verweigern. Der Auftragnehmer ist berechtigt, die Person des unabhängigen externen Prüfers zu bestimmen, sofern der Auftraggeber eine Kopie des erstellten Auditberichts erhält.

Für die Unterstützung bei der Durchführung einer Begehung darf der Auftragnehmer eine Vergütung verlangen. Diese ist vor der Begehung separat zu vereinbaren. Der Aufwand einer Begehung ist für den Auftragnehmer auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt § 5 Abs. 2 des AV-Vertrages entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist jedoch nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

6. Subunternehmer (weitere Auftragsverarbeiter)

Der Einsatz von Unterauftragnehmern als weitere Auftragsverarbeiter im Rahmen des Haupt- und AV-Vertrages ist insoweit zulässig, wie sie in Annex 3 vereinbart sind. Weitere Unterauftragnehmer werden dem Auftraggeber unverzüglich mitgeteilt.

7. Haftung und Schadensersatz

Die zwischen den Vertragsparteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung.

8. Laufzeit

(1) Die Laufzeit dieses AV-Vertrages richtet sich nach der Laufzeit des Hauptvertrages.

(2) Das Recht zur fristlosen Kündigung dieses AV-Vertrages aus wichtigem Grund sowie das Recht des Auftraggebers zur Sonderkündigung nach Maßgabe des § 3 Abs. 2 des AV-Vertrages bleiben unberührt.

9. Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass ausschließlich der Auftraggeber als »Verantwortlicher« nach Art. 4 Nr. 7 DSGVO hinsichtlich der beim Auftraggeber vorliegenden personenbezogenen Daten ist.

(2) Änderungen und Ergänzungen dieses AV-Vertrages einschließlich der Annexe, sonstiger Bestandteile und etwaiger Zusicherungen des Auftragnehmers bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann. Die Änderungen und Ergänzungen bedürfen des ausdrücklichen Hinweises, dass es sich um eine Änderung bzw. Ergänzung dieses AV-Vertrages handelt. Das Formerfordernis gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Sollte eine Bestimmung dieses AV-Vertrages – einschließlich dieses Punkts 9 – und/oder künftige Änderungen bzw. Ergänzungen unwirksam sein oder werden, oder sollten sich in diesem AV-Vertrag Lücken herausstellen, so wird dadurch die Wirksamkeit des AV-Vertrages im Übrigen nicht berührt. Anstelle der unwirksamen Bestimmung bzw. zur Ausfüllung der Vertragslücke soll eine Regelung gelten, die in rechtlich zulässiger Weise dem am nächsten kommt, was die Vertragsparteien nach dem Sinn und Zweck des Vertrages wirtschaftlich gewollt haben oder gewollt hätten, hätten sie den entsprechenden Punkt bedacht. Die

Nichtigkeit einzelner Vertragsbestimmungen hat die Nichtigkeit des gesamten Vertrages nur dann zur Folge, wenn dadurch die Fortsetzung des Vertragsverhältnisses für eine Vertragspartei unzumutbar wird.

(4) Es gilt deutsches Recht.

ANNEX 1 ZUM AV-VERTRAG
Technische und organisatorische Maßnahmen des Auftragnehmers

§ 1 Vertraulichkeit

(1) Zutrittskontrolle

Beim Auftragnehmer kommt ein elektronisches Schließsystem zum Einsatz. Besucher erhalten durch den Empfang Zutritt zu dem Bürohaus und dann zu den Büroräumen. Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

Freien Zugang zu dem Bürohaus haben nur der Vermieter und die Mieter der Büroräume. Die Zugänge werden vom Auftragnehmer als Vermieter verwaltet. Jeder Mieter des Bürohauses hat jedoch die Möglichkeit, die jeweils ausgehändigten Transponder-Schlüssel selbst zu verwalten und elektronisches Zutrittsrecht zu erteilen und zu entziehen. Dies wird von der Personalabteilung des Auftragnehmers verwaltet.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt. Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

(2) Zugangskontrolle

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Diese werden von den Administratoren nach Maßgabe der jeweiligen Berechtigungsrichtlinien vergeben. Jeder Benutzer erhält dann einen eindeutigen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen. Beim Verlassen des IT-Systems wird dieses gesperrt und erst nach Passworteingabe wieder freigegeben. Passwörter werden grundsätzlich sicher verwahrt und verschlüsselt gespeichert. Der Remote-Zugriff auf IT-Systeme des Auftragnehmers erfolgt stets über verschlüsselte Verbindungen. Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist durch Firewalls gesichert, gesteuert und begrenzt. Alle Server und Arbeitsplätze sind durch Antivirensoftware und Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.

(3) Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten. Eine Protokollierung des Zugriffs ist bei wichtigen Systemen vorgesehen.

Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet. Alle Mitarbeiter des Auftragnehmers sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen.

(4) Trennung

Eine Trennung zwischen Entwicklungs-, Test- und Produktivsystemen ist ebenso vorgesehen

wie eine Trennung der Netzwerksegmente nach Schutzbedarf.

(5) Pseudonymisierung und Verschlüsselung
Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

§ 2 Integrität

Alle Mitarbeiter sind zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden und werden regelmäßig im Umgang mit diesen Daten geschult.

(1) Eingabekontrolle
Die Eingabe, Änderung und Löschung von personenbezogenen Daten ist durch Benutzerprofile kleinskalig geregelt. Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt oder gemeinsam genutzt werden. Sammel-Accounts werden nicht genutzt.

(2) Weitergabekontrolle
Eine Weitergabe von personenbezogenen Daten darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Auftraggeber abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Auftraggeber erforderlich ist. Soweit möglich werden Daten verschlüsselt an Empfänger übertragen und die Übertragung protokolliert.
Datenträger werden dokumentiert verwaltet, gesichert aufbewahrt und kontrolliert vernichtet.

§ 3 Verfügbarkeit, Belastbarkeit und Widerstandsfähigkeit

Daten auf Serversystemen des Auftragnehmers werden mindestens täglich inkrementell und wöchentlich „voll" gesichert. Darüber hinaus werden systemspezifische Datensicherungskonzepte erstellt und angewandt. Die Sicherungsmedien werden an einen physisch getrennten Ort verbracht. Das Einspielen von Backups und die Lesbarkeit der Medien werden regelmäßig getestet.
Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung (USV). Im Serverraum befinden sich eine Brandmeldeanlage sowie eine Löschanlage. Es existiert ein Notfallplan, der auch einen Wiederanlaufplan beinhaltet. Die Server und Kommunikationseinrichtungen unterliegen einem permanenten Monitoring der Auslastung und der Verfügbarkeit. So ist sichergestellt, dass auf Lastspitzen, Überlast oder Ausfall schnell reagiert werden kann. Besonders kritische Systeme sind hochverfügbar und/oder redundant ausgelegt. Hierzu zählen zum Beispiel Speichernetzwerke sowie wichtige Kommunikationsleitungen.

§ 4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Für die Datenhaltung kann der Auftragnehmer einen externen Dienstleister beauftragen, welcher unter Annex 3 zum AV-Vertrag aufgeführt ist, wenn hierdurch die geforderten Sicherheitsstandards eingehalten werden. Der Auftragnehmer bzw. ggf. der externe Dienstleister hat ein Information Security Management System (ISMS) zu implementieren, welches auch den Datenschutz umfasst. Zudem werden eine IT-Sicherheitsleitlinie und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird, geschaffen.
Es gibt einen Informationssicherheitsbeauftragten und einen Datenschutzbeauftragten, die Maßnahmen im Bereich von Datenschutz und Datensicherheit planen, umsetzen und Anpassungen vornehmen.
Die Richtlinien, insbesondere auch die Verfahrensverzeichnisse, werden regelmäßig im Hinblick auf ihre Wirksamkeit und Aktualität evaluiert und angepasst.

Es ist sichergestellt, dass Datenschutz- und Sicherheitsvorfälle von allen Mitarbeitern erkannt und unverzüglich gemeldet werden. Soweit Daten betroffen sind, die im Auftrag von Auftraggebern verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

Abrechnung:
Deutsches Medizinrechenzentrum GmbH
Wiesenstraße 21
40549 Düsseldorf
Telefon: +49 211 6355-9087
E-Mail: support@dmrz.de

ANNEX 2 ZUM AV-VERTRAG

Name und Kontaktdaten des Datenschutzbeauftragten

Rebecca Wiemer
Wiemer und Arndt UG
E-Mail: datenschutz@gesundes-kinzigtal.de

ANNEX 3 ZUM AV-VERTRAG

Name und Kontaktdaten von Subunternehmen

Serverbereitstellung und Datenhosting:
Leitwerk AG
Im Ettenbach 13a
77767 Appenweier
Telefon: +49 7805 9180
E-Mail: info@leitwerk.de

Softwareentwicklung:
axaris – software & systeme GmbH
Max-Eyth-Weg 2
89160 Dornstadt
Telefon: +49 731 1518990
E-Mail: info@axaris.de