Vereinbarung zur Inanspruchnahme von Support- und Wartungsdienstleitungen

zwischen
Nutzer der Dienstleistungen

(nachfolgend „**Auftraggeber**“ genannt)

und

Dr. Staber & Kollegen GmbH
Hofer Straße 15
81737 München
(nachfolgend „**Auftragnehmer**“ genannt)

(beide gemeinsam nachfolgend „**Vertragsparteien**“ genannt)

Präambel

Im Rahmen des Kundensupports bietet der Auftragnehmer seinem Kunden (Auftraggeber) Unterstützung und Hilfestellung bei Installationen, dem Betrieb von Software sowie bei Störungen an. Dies erfolgt in der Regel über telefonischen Kontakt mit den Support-Mitarbeitern des Auftragnehmers. Zudem besteht für den Auftraggeber die Möglichkeit, eine Fernwartungssoftware zu nutzen, die es den Support-Mitarbeitern erlaubt, zum Zwecke der Fernwartung auf das EDV-System des Auftraggebers zuzugreifen und das IT-System des Auftraggebers fernzusteuern. Für die Inanspruchnahme der Support- und Wartungsdienstleitungen schließen die Vertragsparteien den nachfolgenden Vertrag.

Dies vorausgeschickt vereinbaren die Vertragsparteien Folgendes:

§ 1 Gegenstand der Vereinbarung

Gegenstand dieser Vereinbarung sind die Unterstützung und Hilfestellung bei Installationen, dem Betrieb von Software sowie bei Störungen durch den Auftragnehmer für die IT-Systeme des Auftraggebers in der zum Zeitpunkt der Wartung vorgefundenen Konfiguration (nachfolgend „**Support- und Wartungsdienstleistungen**“ genannt). Bei Bedarf können die Support- und Wartungsdienstleistungen mit Hilfe einer Internetverbindung (**Fernwartungssoftware**) durchgeführt werden.

§ 2 Leistungen

Der Support-Mitarbeiter des Auftragnehmers unterstützt fernmündlich oder vor Ort in der Praxis den Auftraggeber durch Erbringung von Support- und Wartungsleistungen am installierten IT-System oder führt im Bedarfsfall per Internetverbindung an den Arbeitsplätzen des Auftraggebers eine Fernwartung durch.

Die Support- und Wartungsdienstleistungen umfassen insbesondere:

- Unterstützung und Hilfeleistung bei Fragen der Software-Installation;
- Unterstützung bei Problemen mit Laborsoftwaresystemen oder Datenübertragung;
- Analyse von Fehlersituationen und Ablaufstörungen an den Arbeitsplätzen;
- Suche nach möglichen technischen Fehlerursachen.

Um eine Fernwartung durchführen zu können, wird dem Auftraggeber eine Fernwartungs-software für die Dauer der Vertragsbeziehung zur Verfügung gestellt. Der Auftraggeber startet auf seinem IT-System die bereitgestellte Fernwartungssoftware.

Die Support- und Wartungsdienstleistungen werden durch den Auftragnehmer auf Einzelanforderung des Auftraggebers erbracht. Die Support- und Wartungsdienstleistungen sind für den Auftraggeber kostenlos.

§ 3 Abschluss von Einzelverträgen

Dieser Vertrag wird für jede vom Auftraggeber zu erbringende Support- und Wartungsdienstleistung zwischen den Vertragsparteien neu abgeschlossen (nachfolgend „**Einzelvertrag**“ genannt). Der Einzelvertrag kommt zwischen dem Auftraggeber und dem Auftragnehmer bei der Verwendung des Fernwartungstools durch aktives Akzeptieren der Vertragsbedingungen oder bei der Wartung vor Ort in der Praxis durch Annahme des Vertragsangebotes durch den Auftraggeber zustande. Ohne neuen Vertragsschluss, mit dem die Vertragsbedingungen der Vereinbarung akzeptiert werden, können Support- und Wartungsdienstleistungen nicht durchgeführt werden. Ohne Vertragsabschluss funktioniert die Fernwartung per Internetverbindung technisch nicht. Der Einzelvertrag endet nach Erbringung der einzelnen Support- und Wartungsdienstleistungen durch den Auftragnehmer.

Zum Abschluss einer bestimmten Anzahl an Einzelverträgen ist der Auftraggeber nicht verpflichtet. Wird über einen längeren Zeitraum als 12 Monate keine Support- und Wartungsdienstleistung durch den Auftraggeber angefordert und durch die Support-Mitarbeiter des Auftragnehmers erbracht, ist der Auftraggeber verpflichtet, die Fernwartungssoftware auf seinen Rechnern und Servern dauerhaft zu löschen.

Der Auftragnehmer führt die Support- und Wartungsdienstleistungen am Arbeitsplatzrechner oder den Servern des Auftraggebers aus.

§ 4 Pflichten des Auftraggebers bei Support und Wartung

Der Auftraggeber ist verpflichtet, die organisatorischen und technischen Voraussetzungen dafür zu schaffen, dass der Auftragnehmer die vereinbarten Leistungen erbringen kann. Dazu gehören ggf. auch der Start der Fernwartungssoftware auf den Arbeitsplatzrechnern und Servern.

Zur Fehleranalyse hat der Auftraggeber Fehler oder auftretende Störungen möglichst genau den Support-Mitarbeitern des Auftragnehmers zu beschreiben. Insbesondere bei der Feststellung und Eingrenzung sowie der Beseitigung von Fehlern hat der Auftraggeber sich an den Empfehlungen der Support-Mitarbeiter zu orientieren. Auftretende Mängel hat der Auftraggeber den Support-Mitarbeitern unverzüglich mitzuteilen.

Dem Auftraggeber obliegt die Verantwortung für eine regelmäßige Datensicherung in geeigneter Form, die eine zeitnahe und wirtschaftlich angemessene Reproduzierung der Daten gewährleistet.

Konnte ein Support-Mitarbeiter bei Durchführung der Support- und Wartungsdienstleistungen Kenntnis von Passwörtern des Auftraggebers erlangen, ist der Auftraggeber darüber unverzüglich in Kenntnis zu setzen. Der Auftraggeber wird das Passwort unmittelbar nach Beendigung des Einzelvertrages ändern.

Der Auftraggeber wird während des gesamten Zeitraumes des Wartungsvorganges den Support- Mitarbeiter des Auftragnehmers aktiv unterstützen. Im Falle der Fernwartung per Internetverbindung hat er die Handlungen des Support-Mitarbeiters am Bildschirm zu überwachen. Sollten in diesem Zusammenhang dem Auftraggeber Unregelmäßigkeiten auffallen, wird er den Wartungsvorgang unverzüglich unterbrechen.

§ 5 Urheberrechte und sonstige Schutzrechte

Bestehende Urheberrechte und sonstige Schutzrechte an Softwaresystemen des Auftragnehmers werden durch diese Vereinbarung nicht berührt. Die bisherigen Regelungen, Urheberschaften und sonstige Schutzrechte bleiben weiter bestehen.

§ 6 Gewährleistung und Haftung

Der Auftragnehmer wird die gemäß dieser Vereinbarung geschuldeten Support- und Wartungsdienstleistungen durch ausgebildetes Fachpersonal unter Einhaltung der branchenüblichen Sorgfalt erbringen.

Der Auftragnehmer haftet nur für vorsätzlich und grob fahrlässig verursachte Schäden, die durch seine Support-Mitarbeiter oder beauftragte Dritte entstehen. Die Haftung für Funktionseinschränkungen, Unterbrechungen, Abstürze von Software, Verlust oder Veränderung von Daten des Auftraggebers, Unterbrechungen, Abstürze oder Funktionsuntüchtigkeit eines Teils oder des gesamten IT-Systems des Auftraggebers sowie für daraus resultierende Folgeschäden ist ausgeschlossen.

Der Auftragnehmer übernimmt keinerlei Gewähr für die Funktionsfähigkeit von Software, die nicht von ihm bereitgestellt wird und für den einwandfreien Betrieb und Funktionsfähigkeit des IT-Systems des Auftraggebers. Der Auftragnehmer übernimmt ferner keine Garantie, dass die Fernwartungssoftware oder andere vom Auftragnehmer bereitgestellte Softwaresysteme dauernd, ununterbrochen und fehlerfrei in allen vom Auftraggeber gewünschten Kombinationen, mit beliebigen Daten, Informationssystemen und Programmen

eingesetzt werden können. Der Auftragnehmer übernimmt auch keine Garantie, dass die Korrektur eines Programmfehlers das Auftreten anderer Programmfehler ausschließt.

§ 7 Datenschutz und Geheimhaltung

Es kann nicht ausgeschlossen werden, dass der Auftragnehmer und die von ihm eingesetzten Support-Mitarbeiter bei der Erfüllung der Support- und Wartungsdienstleistungen nach dieser Vereinbarung Zugriff auf personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO haben bzw. davon Kenntnis erlangen und diese personenbezogenen Daten verarbeiten. Aus diesem Grund schließen die Vertragsparteien einen Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO (nachfolgend „**AV-Vertrag**“ genannt). Der AV-Vertrag ist als **Anlage 1** Bestandteil dieser Vereinbarung.

Der Auftragnehmer wird sämtliche ihm auf Grund der Durchführung der Vereinbarung bekannt gewordenen betrieblichen Abläufe, sonstigen Betriebs- und Geschäftsgeheimnisse sowie Passwörter des Auftraggebers streng vertraulich behandeln und die vom ihm eingesetzten Support-Mitarbeiter auf die Geheimhaltung verpflichten.

Dem Auftragnehmer ist untersagt, Kenntnisse oder Informationen, die er im Zusammenhang mit der Wartung beim oder vom Auftraggeber erhält, in irgendeiner Weise für sich selbst oder für Dritte zu verarbeiten und/oder anderweitig zu nutzen.

Der Auftraggeber gestattet mit Unterzeichnung dieser Vereinbarung, dass ausschließlich der Ablauf, nicht jedoch der Inhalt des Einzelvertrages von dem Auftragnehmer protokolliert und für die gesetzlich zulässige Dauer für Nachweiszwecke durch diesen archiviert werden.

§ 8 Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung, einschließlich ihrer Anlage und sonstiger Bestandteile sowie etwaige Zusicherungen des Auftragnehmers bedürfen einer schriftlichen Vereinbarung zwischen den Vertragsparteien mit dem ausdrücklichen Hinweis, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Das Formerfordernis gilt auch für den Verzicht auf diese Schriftformklausel.

Erfüllungsort und Gerichtsstand ist der Sitz des Auftragnehmers.

Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1 zur Vereinbarung
zur Nutzung von
Support- und Wartungsdienstleitungen

Auftragsverarbeitung nach Art. 28 DSGVO

Präambel

Der AV-Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz nach der DSGVO, dem BDSG-neu und der ärztlichen Schweigepflicht nach §§ 203, 204 StGB. Der AV-Vertrag findet auf alle Tätigkeiten Anwendung, die mit der Vereinbarung zur Nutzung von Support- und Wartungsdienstleitungen (nachfolgend „**Hauptvertrag**“ genannt) in Zusammenhang stehen und bei denen Support-Mitarbeiter des Auftragnehmers personenbezogene Daten des Auftraggebers, seiner Patienten oder seiner Vertragspartner tatsächlich oder möglicherweise verarbeiten.

§ 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
Software-Installation	Patient, Auftraggeber, Mitarbeiter, Vertragspartner	Personalstammdaten, Gesundheitsdaten/ biometrische Daten/ genetische Daten, Kommunikationsdaten, Vertragsstammdaten
Unterstützung beim Software Betrieb	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 § 1 des AV-Vertrages. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der geltenden Datenschutzgesetze (insbesondere die DSGVO, das BDSG-neu und die §§ 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.

(2) 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.

(3) Die Verarbeitung der personenbezogenen Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union 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 § 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.

Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren Wirksamkeit wird auf die vorliegenden Technischen und Organisatorischen Maßnahmen verwiesen, deren Vorlage dem Auftragnehmer für den Nachweis geeigneter Garantien solange und soweit ausreicht, bis eine Zertifizierung nach Art. 42 DSGVO existiert und etwas anderes vorschreibt.

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) Die Support-Mitarbeiter des Auftragnehmers werden von diesen schriftlich darauf verpflichtet, dauerhaft – auch nach Beendigung ihres Arbeitsverhältnisses – keine Informationen, die sie im Rahmen ihrer Tätigkeit nach dem Hauptvertrag und diesem AV-Vertrag erlangen, an Dritte weiterzugeben. Soweit die Support-Mitarbeiter des Auftragnehmers im Rahmen dieser Tätigkeit personenbezogene Daten des Auftraggeber, die der ärztlichen Schweigepflicht unterfallen, zur Kenntnis nehmen können, sind sie „sonstige mitwirkende Personen“ i.S.d. § 203 Abs. 3 StGB. Die Mitarbeiter des Auftragnehmer 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 der 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 3 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 Einzelvertrages 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 Auftragnehmer 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, werden 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 nicht zulässig.

§ 7 Haftung und Schadensersatz

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

§ 8 Laufzeit des AV-Vertrag

(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 § 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 Vertrags-bestimmungen 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

INHALT

VERTRAULICHKEIT

ZUTRITTSKONTROLLE

Art.32 Abs.1 lit.b DS-GVO

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten und besonderen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	Organisatorische Maßnahmen
Manuelles Schließsystem	Schlüsselregelung/Schlüsselbuch
Magnet- und/oder Chipkarten-System	Schlüsselregelung (Schlüsselausgabe etc.)
Sicherheitsschlösser	Personenkontrolle beim Pförtner/Empfang
	Protokollieren der Besucher mittels QM-Dokument
	Tragepflicht von Mitarbeiter-/Gästeausweisen
	Sorgfältige Auswahl von Reinigungspersonal

ZUGANGSKONTROLLE

Art.32 Abs.1 lit.b DS-GVO

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Automatische Sperrmechanismen	Zuordnung + Verwaltung von Benutzerrechten
Einsatz von Antiviren-Software	Erstellen von Benutzerprofilen
Einsatz einer Hardware-Firewall	Passwortvergabe
Einsatz einer Software-Firewall	Sorgfältige Auswahl von Reinigungspersonal
Verschlüsselung von Datenträgern und Smartphones (Baramundi)	
Einsatz von VPN-Technologie	
Authentifikation mit Benutzername/Passwort	
Zuordnung von Benutzerprofilen zu IT-Systemen	

ZUGRIFFSKONTROLLE

Art.32 Abs.1 lit.b DS-GVO

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei ihrer Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Anzahl der Administratoren auf das „Notwendigste“ reduziert	Erstellen eines Berechtigungskonzeptes
Stufenregelung der Zugriffsberechtigung	Anzahl der Administratoren auf das „Notwendigste“ reduziert
Verschlüsselung von Datenträgern und Smartphones	Sichere Aufbewahrung von Datenträgern
Verwaltung der Benutzerrechte durch Systemadministratoren	Physische Löschung von Datenträgern vor Wiederverwendung
Protokollierung der „Fehl“-Zugriffe	Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
	Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutzsiegel) und deren Protokollierung

TRENNUNGSKONTROLLE

Art.32 Abs.1 lit.b DS-GVO

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Logische Mandantentrennung (Softwareseitig)	Erstellung eines Berechtigungskonzeptes
Versehen der Datensätze mit Zweckattributen/Datenfeldern	Festlegung von Datenbankrechten
Trennung von Produktiv- und Testsystem	

PSEUDONYMISIERUNG/ANONYMISIERUNG/VERSCHLÜSSELUNG

Art.32 Abs.1 lit.a DS-GVO

Maßnahmen, die gewährleisten, dass die Verarbeitung personenbezogener Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Technische Maßnahmen	Organisatorische Maßnahmen
Kryptographische Verschlüsselung bei E-Mail Korrespondenz intern wie sofern möglich extern	Erstellen von anonymen Statistiken
	Erstellung pseudonymisierter Kundenprofile nach Zweckabwägung
	Verwenden personalisierter Nicknames oder vereinbarter Codewörter
	Schwärzung der personenbezogenen Daten bei Papierdokumenten

INTEGRITÄT

(WEITERGABEKONTROLLE)

Art.32 Abs.1 lit.b DS-GVO

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von SSL-Verbindungen, Standleitungen bzw. VPN-Tunneln (zur Befundübermittlung und zu den Standorten)	Erstellen einer Übersicht von regelmäßigen Abruf-und Übermittlungsvorgängen
E-Mail Verschlüsselung	Dokumentation der Empfänger von Daten und der Zeitspannen und der geplanten Überlassung bzw. vereinbarter Löschfristen
Für die elektronische Übertragung von personenbezogenen Daten, insbesondere Patientendaten werden nur im deutschen Gesundheitswesen genutzte Übertragungsprotokolle genutzt (elektronische Befundübermittlungen an Praxen und Kliniken).	Beim physischen Transport: sichere Transportbehälter/-verpackungen (Probenmaterial mit Anforderungsbelegen und Befunde in geschlossenen Umschlägen)
	Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -Fahrzeugen (Probenmaterial mit Anforderungsbelegen und Befunde in geschlossenen Umschlägen)

EINGABEKONTROLLE

Art.32 Abs.1 lit.b DS-GVO

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)

Technische Maßnahmen	Organisatorische Maßnahmen
Protokollierung der IT, welcher Benutzer auf welche Daten zu welchem Zeitpunkt zugegriffen hat. Die Protokolle stehen der IT-Administration zur Verfügung mittels Protokollierungs-und Protokollauswertsysteme	Aufbewahrung von Formularen, deren Daten in automatisierte Verarbeitungen übernommen wurden
Protokollierung der Änderungen an Daten, Anwendungen und Systemen	Festlegung der Eingabebefugnisse
Protokollierung der Administrator-Aktivitäten	
Sicherung der Protokolldaten gegen Verlust und/oder Veränderung	
Elektronische Signatur geplant	

VERFÜGBARKEIT UND BELASTBARKEIT

VERFÜGBARKEITSKONTROLLE

Art.32 Abs.1 lit.b DS-GVO

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	Organisatorische Maßnahmen
Unterbrechungsfreie Stromversorgung (USV)	Erstellen eines Notfallplans
Klimaanlage in Serverräumen	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	Serverräume nicht unter sanitären Anlagen
Schutzsteckdosenleisten in Serverräumen	In Hochwassergebieten: Serverräume über der Wassergrenze
Erstellen eines Backup- & Recoverykonzeptes	Feuer und Rauchmeldeanlagen
Testen von Datenwiederherstellung	Feuerlöschgeräte für Serverräumen
Virenschutz	

WIEDERHERSTELLBARKEIT

Art.32 Abs.1 lit.c DS-GVO

Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wieder hergestellt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Zeitnahes Einspielen der gesicherten Daten durch die IT-Administration	Sicherung der Daten in einem zeitlich vorgegebenen Abstand
Testung in periodischen Abständen	

SPEICHERKONTROLLE

Maßnahmen zur Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Technische Maßnahmen	Organisatorische Maßnahmen
Softwareverriegelung des Bildschirmes bei längerem Inaktivsein des Benutzers	Definierter Zugang zu Speichermedien mithilfe von Benutzercodes -> Berechtigungskonzept
Verwendung des Schreibschutzes bei Datenträgern	Zugriffsprotokoll und Zugriffsregelung
Datenverschlüsselung	Trennung des Test- und Produktionsbetriebes

DATENTRÄGERKONTROLLE

Art.32 Abs.1 lit.a DS-GVO

Maßnahmen, die das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern verhindern.

Technische Maßnahmen	Organisatorische Maßnahmen
Verfahren für Datenträgeraustausch	Kontrolle der zur Verfügung stehenden Speichermedien DVD, USB-Stick, Festplatte und Papier
Speicherung der Daten auf einem bestimmten Laufwerk des Servers bei Laptop/PC	Zugriffsichere Aufbewahrung von Datenträgern -> Data Safe -> Datenträgerarchiv
	Fachgerechte Entsorgung von Datenträgern, Formatieren, physische Zerstörung nach vorgegebenem Lebenszyklus
	Protokollierung + Nachvollziehbarkeit bei der autorisierten Ausgabe und Weitergabe von Datenträgern ->maschinelle Datenträgerverwaltung
	Kein Einsatz von fremden Datenträgern
	Aufbewahrungs- und Löschkonzept von Datenträgern
	Räumliche Trennung der Back-up Datenträger
	Einstufung von Papierdokumenten als Datenträger
	Dokumentation von Datenträgeraustausch
	Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger

BENUTZERKONTROLLE

Maßnahmen zur Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

Technische Maßnahmen	Organisatorische Maßnahmen
Sicherung der Datenstationen, Netze und Übertragungsleitungen	Festlegung der nutzungsberechtigten Personen
Verschlüsselung der zu übertragenden Daten	Identifikation und Authentifizierung der Benutzer
	Protokollierung der Benutzer und deren Aktivitäten

ÜBERTRAGUNGSKONTROLLE

Maßnahmen, mit deren Hilfe überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Elektronische Übertragung nur an berechtigte Empfänger	Festgelegte Übermittlungswege der Datenempfänger
Verschlüsselung von Daten	Adresscheck
Firewall, Virenschutz	Passwortschutz einzelner Dokumente mit getrennter Kennwortübermittlung
Content-Filter, SSl-Scanner	Verwendung der Daten für Schriftstücke im Vier-Augen-Prinzip
Verschlüsselung der Datenträger intern	Sicher versiegelte Transportbehälter
	Zuverlässigkeit des Transporteurs

ÜBERMITTLUNGSKONTROLLE

Ziel der Übermittlungskontrolle ist es, mit Hilfe geeigneter Maßnahmen gewährleisten zu können, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen der Datenübertragung übermittelt werden können. Hier kommt es nicht auf die tatsächliche oder theoretisch mögliche, sondern auf die nach der Verfahrenskonzeption vorgesehene Übermittlung an (auch im Rahmen von automatisierten Abrufverfahren). Die Überprüfung und Feststellung muss nicht dauernd erfolgen, aber sie muss jederzeit möglich sein.

Technische Maßnahmen	Organisatorische Maßnahmen
Auswertungsmöglichkeiten der Übermittlungsprotokolle, um die Empfänger	Festlegung der Übermittlungswege und der Datenempfänger
Protokollierung der Datenübermittlung	Dokumentation der Abruf- und Übermittlungsprogramme

ZUVERLÄSSIGKEIT

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
Auswertungen der aufgetretenen Sicherheitsvorfälle	Überwachung im Sinne einer Erfolgskontrolle
Sicherheitskonzept	Durchführen von Penetrationstests geplant
Back-Up Verfahren	Meldung, Protokollierung und Auswertung von Fehlfunktionen

TRANSPORTKONTROLLE

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird.

Technische Maßnahmen	Organisatorische Maßnahmen
Duplizierung der Datenträger	Keine Speicherung sensibler personenbezogener Daten auf Smartphones
Verschlüsselung der Daten intern	Nutzung und Transport von Laptop/PC nur von befugten Personen
Überprüfung aller Daten und Datenträger hinsichtlich Virenbefall	Bei Reparatur außer Haus ist vertraglich sichergestellt, dass der Empfänger die Daten vertraulich behandelt
	Festlegung, der für die Übermittlung oder den Transport berechtigten Personen
	Regelungen für die Versandart und Festlegung des Transportweges
	Verwendung sicherer Transportbehälter
	Sicherung des Übertragungs- und Transportweges
	Physikalische Löschung aller Datenträger vor einer neuen Beschreibung und nach jeder Verarbeitung
	Überwachung der Transportzeit

DATENINTEGRITÄT

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktion des Systems beschädigt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Virenscanner	Datensicherung ->Back-Up
Firewall	Verwendung von Prüfnummern
Software-Updates der Betriebssysteme	Zugriffsrechte
Verschlüsselung	
Verschlüsseln von Wechselmedien	
VPN Anbindung mobiler Mitarbeiter	

AUFTRAGSKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
	Eindeutige Vertragsgestaltung -> Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber
	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
	Kontrolle + Protokollierung der ordnungsgemäßen Vertragsgestaltung und -ausführung
	Formalisierte Auftragserteilung (Auftragsformular)
	Sorgfältige Auswahl des Auftragnehmers
	Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber
	Sanktionen bei Vertragsverletzung der Vertragsausführung
	Vereinbarte Kontrollrechte gegenüber dem Auftragsnehmer

ORGANISATIONSKONTROLLE

Ziel der Organisationskontrolle ist es, die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Gemeint ist damit, dass sich der Datenschutz nicht an die Organisation, sondern die Organisation an den Datenschutz anpassen sollte.

Technische Maßnahmen	Organisatorische Maßnahmen
Erlass von Programmierrichtlinien	Bestellung eines behördlichen Datenschutzbeauftragten
Zentrale Beschaffung der Hard- und Software	Funktionstrennung innerhalb der DV-Abteilung, sofern das die Abteilungsgröße erlaubt
Regelmäßige Datensicherung	Formalisierte Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen
Revisionsfähige Benutzerverwaltung	Erlass von Datenschutzrichtlinien und Dienstanweisungen
	Schulung der Mitarbeiter
	Erstellen eines Notfallkonzepts
	Erstellen von Bedienungs- und Benutzeranweisungen
	Vorgabe der Regelungen für die Passwortvergabe und -verwaltung
	Vorgaben für die Dokumentation der Programme

Annex 2 (zum AV-Vertrag) - Name und Kontaktdaten des Datenschutzbeauftragten

Dr. Staber &Kollegen GmbH
Martina Arnold Datenschutzbeauftragte (TÜV)
Herkulessstraße 34 a
34119 Kassel
Datenschutz@labor-staber.de