BIOSCIENTIA
MEDIZIN. LABOR. SERVICE.

Vereinbarung zur Inanspruchnahme von Support- und Wartungsdienstleistungen

zwischen

Nutzer der Dienstleistungen

(nachfolgend „**Auftraggeber**“ genannt)

und

Bioscientia Institut für Medizinische Diagnostik GmbH
Konrad-Adenauer-Str. 17
55218 Ingelheim

(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 Wartungsdienstleistungen 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 Fernwartungssoftware 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.

BIOSCIENTIA
MEDIZIN. LABOR. SERVICE.

Anlage 1 zur Vereinbarung
zur Nutzung von
Support- und Wartungsdienstleistungen

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 Wartungsdienstleistungen (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 Wartungsdienstleistungen) 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 geprüfte Wirksamkeit wird auf die vorliegende DAkkS Akkreditierungverwiesen (**Annex 2**), 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 3** 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 Auftraggeber 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 »Verantwortlicher « nach Art. 4 Nr. 7 DSGVO hinsichtlich der beim Auftragnehmer 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 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)

1 Technische und organisatorische Maßnahmen des Auftragnehmers

1. Vertraulichkeit

- Zutrittskontrolle

Die Räume der Bioscientia sind entweder durch elektronische Schließanlagen (Interflex), die einen elektronisch lesbaren personenbezogenen Ausweis erfordern, durch einen während der Öffnungszeiten durchgehend besetzten Empfang oder durch verschlossene Türen mit Klingeln gesichert. Der Zutritt wird (nur in der Zentrale in Ingelheim) soweit sinnvoll möglich auch tageszeitabhängig eingeschränkt und soweit räumlich sinnvoll zusätzlich noch über Einzelraumberechtigungen weiter eingeschränkt. Die Datenverarbeitung und Datensicherung erfolgt in zutrittsgeschützten Räumen. Für die sensiblen Bereiche definieren die jeweiligen Vorgesetzten welche Mitarbeiter Zutritt erhalten. Die Pflege und Überwachung des Zutritts obliegt der Personalabteilung. Bei Beendigung des Arbeitsverhältnisses werden elektronische Zutrittskarte und/ oder Schlüssel des Mitarbeiters durch die Personalabteilung systematisch zurückgefordert. Wird der Zutritt externer Personen, z. B. zur Durchführung von Wartungs- oder Instandsetzungsarbeiten erforderlich, so werden diese stets durch Mitarbeiter der Bioscientia begleitet.

- Zugangskontrolle

Die Datenverarbeitungssysteme erfordern eine personenbezogene, passwortgeschützte Anmeldung am jeweiligen System. Die Vergabe des allgemeinen Systemzugangs erfolgt nach der Arbeitsanweisung BIO-EDV-NWD-Security Management logisch.pdf. Hierfür ist ein Antragsverfahren mittels Formular und hierarchischem Freigabeprozess zu durchlaufen. In der Anweisung ist geregelt, dass der Vorgesetzte den Zugang für den Mitarbeiter beantragt. Der Antrag wird von der Personalabteilung genehmigt und von der EDV umgesetzt. Bei Austritt des Mitarbeiters oder Wechsel der Funktion werden die Rechte revidiert. Zum Austritt eines Mitarbeiters aus dem Unternehmen werden alle seine Accounts gesperrt. Sein Postfach wird routinemäßig 6 Monate nach Austritt gelöscht. Passwörter müssen alle 90 Tage zwangsweise gewechselt werden und obliegen einer Prüfung gegen eine Liste unzulässiger Begriffe und erfordern eine Mindestlänge von 8 Zeichen, mindestens bestehend aus 3 von 4 Kategorien (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen). Für den Zugang zum Laborsystem findet die BIO-EDV-SAA-Melos Berechtigungskonzept.pdf Anwendung. Wird ein zentraler Arbeitsplatz (nur im Laborbereich) ganztägig von allen Mitarbeitern der Gruppe genutzt, so erfolgt die Anmeldung am Arbeitsplatz-Rechner ausnahmsweise über einen Gruppennamen und die Anmeldung bleibt ganztägig bestehen. Der letzte Mitarbeiter nimmt bei Arbeitsende die Abmeldung vor und fährt den PC herunter. Dies gilt nur für den Arbeitsplatz-Rechner, nicht für die Laboranwendungen auf dem Arbeitsplatz-Rechner, diese werden unter 3. behandelt. Das gesamte Netzwerk befindet sich hinter einer Firewall mit einem permanent aktualisierten Virenschutzprogramm. Abfragen aus dem Laborsystem von außerhalb der Firewall sind nur den Ärzten und dem Außendienst für Kundenrückfragen möglich und auf konkrete Einzelabfragen beschränkt. Der Remote-Netzwerkzugang erfolgt über eine VPN-Verbindung die durch eine Benutzerkennung gesichert ist.

- Zugriffskontrolle

Die Laborsysteme erfordern bei Anmeldung individuelle, nicht übertragbare Anmeldenamen und Anmeldekennwörter. Die eingesetzten Laborsysteme verfügen über eine abgestufte Rechtevergabe, welche die Möglichkeiten auf die, für die jeweiligen Arbeiten unbedingt erforderlichen Zugriffsrechte beschränkt. Die praktischen Einschränkungen erfolgen dabei arbeitsgruppenbezogen und regeln auf dieser Ebene, welche

Informationen gelesen, kopiert, verändert oder entfernt werden können. Der Zugriff auf patientenbezogene Daten ist auf ausgesuchtes Personal mit medizinischen Aufgaben beschränkt.

- Trennung

Eine stringente Trennung anhand der Kundennummer sorgt dafür, dass Daten unterschiedlicher Kunden nicht vermischt werden..

- Pseudonymisierung & 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.

- Eingabekontrolle

Alle Änderungen von personenbezogenen Daten werden benutzerbezogen zwangsprotokolliert und können entsprechend nachträglich ausgewertet werden (sogenannter Audit-Trail im Laborsystem).

- Weitergabekontrolle

Die erlaubte Datenweitergabe beschränkt sich auf fest definierte Prozesse und erfolgt im erforderlichen Fall benutzer- oder zeitgesteuert in festen Bahnen mit größtmöglicher Einschränkung des personenbezogenen Datenumfangs bzw., wo möglich ohne personenbezogene Daten. Die Datenspeicherung beschränkt sich auf die gesetzlich vorgeschriebenen Aufbewahrungsfristen. Medizinische Befunde in Papierform werden nach Wahl des Auftraggebers entweder im verschlossenen Umschlag per Probenkurier oder per Post „vertraulich“ gekennzeichnet verschickt. Erfolgt die Übertragung der medizinischen Befunde auf Wunsch des Auftraggebers auf elektronischem Wege, so werden die Daten im Download über das Protokoll SFTP (mind. SHA1, AES128) und über das Protokoll https (mind. TLS 1.0 in Verbindung mit Client Zertifikaten) verschlüsselt verschickt. Ausnahmsweise erfolgt die Übermittlung nach festgelegten Regeln auch per Telefon oder Telefax. Näheres regelt die ING-BSC-SAA-Telefon-Ergebnisübermittlung.pdf. Die Weitergabe von Daten (z.B. Befunde, Aufträge) wird systemseitig unter Angabe des Nutzers, des Weges und des Datums der Weitergabe dokumentiert. Die Datenvernichtung erfolgt gemäß der entsprechenden BIO-QM-VAW-Aufbewahrungsfristen.pdf. Die VAW regelt, dass papierhafte Auftragsscheine 4 Wochen aufbewahrt werden, die elektronischen Kopien und elektronisch erhaltene Aufträge 10 Jahre. Laborbefunde und Berichte werden 10 Jahre elektronisch aufbewahrt. Probenmaterial wird 14 Tage aufbewahrt.

Die Entsorgung erfolgt ausschließlich über zertifizierte Firmen.

3. Verfügbarkeit, Belastbarkeit und Widerstandsfähigkeit

Zum Schutz personenbezogener Daten vor zufälliger Zerstörung und Verlust erfolgt eine tägliche generische Sicherung der Daten an allen Standorten. Die Sicherung erfolgt in zutrittsgeschützten Räumen.

Das Datensicherungskonzept am Hauptstandort Ingelheim ist ein zweistufiges Konzept. Im Rahmen des Continuity Management wird ein komplettes Ersatz Laborinformationssystem (LIS) standby vorgehalten, welches in einem automatischen Prozess mit dem Produktions LIS synchron gehalten wird (asynchrone Spiegelung).

Zusätzlich ist ein Datensicherungsprozess für das LIS eingerichtet (Availability Management). Das Tool Dataprotector (DP), Hersteller HP, sichert täglich die Daten des Produktionssystems in eine virtuelle Tape Library (Festplatten Speichersystem). Zur optimierten Durchführung des Sicherungsprozesses (Backup Zeit vs. Restore Zeit) kommt eine inkrementelle Sicherung zur Anwendung. DP verfügt zudem über das Verfahren der Datendeduplikation zur weiteren Optimierung des Sicherungsprozesses bezüglich Datenvolumen und Performance. Durch interne Datenkonsolidierung der im System vorgehaltenen Datenbestände entsteht ein synthetischer Full Backup mit Auslagerung dieser Daten auf Bändern einer HP Tape Library (LTO Technologie).

Die Backup Aufbewahrungszeiten: Alle inkrementellen Datensicherungen verbleiben in der virtuellen Tape Library. Diese werden 3 Monate vorgehalten und danach überschrieben. Full Backup Sicherungen befinden sich auf Band und werden 12 Monate vorgehalten. Danach werden diese Bänder dem Sicherungsprozess wieder zugeführt. Full Backup Tapes (Generation -1) werden der Tape Library entnommen und in einen Data Safe ausgelagert.

Datensicherungsmedien die nicht mehr eingesetzt und verwendet werden können, z.B. weil die Anzahl der Beschreibzyklen überschritten ist, bzw. defekte Datenträger, werden als Datenmüll deklariert und in einem abgeschlossenen Behälter bis zur Vernichtung angesammelt. Die Entsorgung des Datenmülls übernimmt ein hierauf spezialisiertes Unternehmen (die Medien werden geschreddert).

Das Datensicherungskonzept umfasst im Wesentlichen folgende Dokumente: ING-EDV-VAW-Backup-Restore Data Protector.pdf, welches die generischen Sicherungen beschreibt, die ING-EDV-VAW-Katastrophenplan-Ingelheim.pdf welche die Systeme mit Wiederanlaufzeiten, Ersatzkomponenten, Ausweichmöglichkeiten und Wartungsverträge definiert. Darüber hinaus verfügt der Standort Ingelheim über eine USV-Anlage, bestehend aus Batterien und einem Notstromdiesel. An die USV sind die EDV und betriebsnotwendige Laborgeräte und Kühlvorrichtungen angeschlossen. Die USV wird von der Haustechnik alle 4 Wochen getestet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Es gibt eine IT-Sicherheitsleitlinie und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.
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 Auftraggeber verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

Annex 2 (zum AV-Vertrag) - Akkreditierung der DAkkS

Annex 3 (zum AV-Vertrag) - Name und Kontaktdaten des Datenschutzbeauftragten

Externe Beauftragte für den Datenschutz:
Monika Ganter-Häcker und Eberhard Häcker
Tel. 0172 6302169
E-Mail: bioscientia@team-datenschutz.de

Interner Ansprechpartner für den Datenschutz:
Wolfgang Pohl
Tel. 06132 - 781 115
E-Mail: datenschutz@bioscientia.de