Angebot
auf Abschluss eines Vertrages zur Auftragsverarbeitung gemäß Art. 28 DSGVO

an die in Anlage 1 zum EVB-IT-Vertrag genannten **AMEOS Gesellschaften**, jeweils vertreten durch die AMEOS Spitalgesellschaft mbH

– im Folgenden „**Auftraggeber**“ genannt –

von

– im Folgenden „**Auftragnehmer**“ genannt –

Präambel

Dieser Auftragsvertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im EVB-IT-Vertrag (im Folgenden „**Hauptvertrag**“ genannt) beschriebenen Auftragsverarbeitung ergeben.

Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeitende des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen können.

§ 1

Definitionen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DSGVO, § 2 TDDDG und § 2 GeschGehG. Sollten in den Artikeln bzw. Paragrafen sich widersprechende Darstellungen zu finden sein, gelten die Definitionen der DSGVO.

Weiterhin gelten folgende Begriffsbestimmungen:

Anonymisierung: Prozess, bei dem personenbezogene Daten entweder vom für die Verarbeitung der Daten Verantwortlichen allein oder in Zusammenarbeit mit einer anderen Partei unumkehrbar so verändert werden, dass sich die betroffene Person danach weder direkt noch indirekt identifizieren lässt (Quelle: DIN EN ISO 25237).

Unterauftragnehmer: Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt.

Verarbeitung im Auftrag: Verarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch einen Auftragnehmer im Auftrag des Auftraggebers.

Weisung: Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (z. B Anonymisierung, Sperrung, Löschung, Herausgabe etc.) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch einen Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2
Gegenstand des Auftrages

☐ Gegenstand der Vereinbarung ist die Verarbeitung personenbezogener Daten (nachstehend „**Daten**“ genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung in Ergänzung des EVB-IT-Vertrages der Parteien. Der Auftragnehmer erhält durch Bereitstellung oder durch Erlaubnis zur Erhebung Zugriff auf personenbezogene Daten.

Bezeichnung der Daten:

☒ Personaldaten (aktive und ausgeschiedene Mitarbeitende)

☒ Bewerberdaten

☒ Kundendaten (z.B.: Patienten, Bewohner)

☒ Interessentendaten (z.B.: Anfragen zur Therapie ggf. auch Online)

☒ Lieferantendaten

Besondere Kategorien von Daten gemäß Art. 9 DSGVO:

☒ Gesundheitsdaten

☒ genetische Daten

☒ Daten rassischer oder ethnischer Herkunft

☒ Daten religiöser Überzeugung

☐ Daten weltanschaulicher / philosophischer Überzeugung

☐ Daten politischer Überzeugungen / Meinungen

☒ biometrische Daten zur eindeutigen Identifizierung einer Person

☐ Daten zu Gewerkschaftszugehörigkeiten

☒ Daten zum Sexualleben oder der sexuellen Orientierung

Betroffene Personengruppen:

Bei den Betroffenen der oben aufgelisteten Daten handelt es sich um:

- ▣ PatientInnen
- ▣ BewohnerInnen
- ▣ MitarbeiterInnen
- ☐ Angehörige
- ▣ BetreuerInnen
- ▣ KundInnen
- ▣ InteressentInnen
- ☐ AbonnentInnen
- ▣ LieferantInnen
- ☐ HandelsvertreterInnen
- ▣ AnsprechpartnerInnen

Der Zugriff auf die Daten bzw. die Datenerhebung erfolgt durch

- ☐ Übermittlung durch den Auftraggeber
- ▣ Beauftragung durch den Auftraggeber.

☑ Gegenstand dieser Vereinbarung ist der nicht ausgeschlossene Zugriff auf oben genannte personenbezogene Daten durch (Fern-) Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen.

Der Auftragnehmer erbringt für den Auftraggeber folgende Prüf- bzw. Wartungstätigkeiten, bei denen eine Zugriffsmöglichkeit auf die o.g. personenbezogenen Daten nicht ausgeschlossen werden kann:

- ☐ Prüfung / Wartung vor Ort, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann
- ☐ Hardware-Diagnose per Fernzugriff für folgende Hardwareprodukte, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann:

- ☑ Software-Prüfung / Wartung per Fernzugriff für folgende Softwareprodukte, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann:

  Schwachstellenscanner + External Attack Surface Management Lösung

§ 2.1

Leistungen des Auftragnehmers

Der Auftragnehmer erbringt für den Auftraggeber, bezogen auf die in § 2 genannten Daten, folgende Leistungen:

Kontiernuierliche Überpüfung (Scan) des Gesamt-Netzwerkes des Auftraggebers auf Schwachstellen gemäß Anlage 2a und 2b des EVB IT Vertrages.

§ 3

Verantwortlichkeit

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Abs. 7 DSGVO).

(2) Die Inhalte dieses AV-Vertrages gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen werden und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Auftraggeber sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dazu müssen alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Dabei ist jede Partei für die Verpflichtung des eigenen Personals zuständig. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.

(4) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

§ 4

Zustandekommen, Dauer des Auftrags

(1) Der Auftragnehmer bietet dem Auftraggeber mit Einreichung seines Angebotes im Vergabeverfahren für den Zeitraum der Bindefrist unwiderruflich den Abschluss dieses Vertrages an. Der Auftraggeber erklärt mit Zuschlag im Vergabeverfahren die Annahme dieses Angebotes. Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus diesem Vertrag nicht etwas anders ergibt.

(2) Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages, z. B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

(3) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

(4) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

§ 5

Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

(2) Die Weisungen des Auftraggebers werden vom Auftragnehmer dokumentiert und dem Auftraggeber unmittelbar nach erfolgter Dokumentation als unterschriebene Kopie zur Verfügung gestellt.

(3) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer wesentlichen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf der Änderung, steht dem Auftragnehmer ein ordentliches Kündigungsrecht bezüglich des von der Weisung betroffenen AV-Vertrages sowie der von der AV- Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages zu. Verweigert der Auftragnehmer die Änderung durchzuführen, steht auch dem Auftraggeber ein ordentliches Kündigungsrecht zu.

(4) Erfolgt eine Kündigung, so ist für die restliche Vertragslaufzeit weiterhin die vertraglich vereinbarte Leistung durch den Auftragnehmer zu erbringen.

(5) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich bestätigen. Der Auftragnehmer dokumentiert Datum, Uhrzeit und Person, welche die mündliche Weisung erteilte sowie den Grund, warum keine unmittelbare schriftliche Beauftragung erfolgen konnte.

(6) Ansprechpartner / weisungsberechtigte Personen des Auftraggebers sind:

Geschäftsführung / Unternehmensleitung	Dr. A Paeger F. Eppacher – Geschäftsführung
IT-Leitung:	Frau Katrin Weinhold
Weitere vom Auftraggeber autorisierte Personen:	
Gesamt-Projektleitung:	Herr Lars Klötscher
IT-Projektleitung:	Herr Martin Behrens

§ 6
Leistungsort

(1) Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland erbringen. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer. Die zum Zeitpunkt der Auftragserteilung vereinbarten Leistungsstandorte sind in Anlage 1 zum EVB-IT-Vertrag aufgeführt. Erfolgt eine Leistungserbringung in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DSGVO und weist dies auf Verlangen nach.

(2) Der Auftraggeber stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.

(3) Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU / EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, wird der Auftraggeber schriftlich informiert.

(4) Sofern der Auftragnehmer vom Auftraggeber nicht innerhalb einer Frist von 4 Wochen nach Zugang der Mitteilung gemäß Abs. 3 über die Verlagerung der Gründe informiert wird, die eine Verlagerung nicht zulassen, gilt die Zustimmung zu dieser Verlagerung seitens des Auftraggebers als erteilt.

(5) Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU / EWR in einem sog. sicheren „Drittstaat“ erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch den Auftraggeber einholen.

(6) Bei einer Leistungserbringung in einem sicheren Drittstaat wird der Auftraggeber seine Zustimmung zur Verlagerung nicht unbillig verweigern. Die Einhaltung der diesbezüglichen Vorgaben der DSGVO wird durch den Auftragnehmer gewährleistet.

(7) Sofern die Leistungsverlagerung in ein anderes Land nach den vorstehenden Regelungen möglich ist, gilt dies entsprechend für jeglichen Zugriff bzw. jegliche Sicht auf die Daten durch den Auftragnehmer, z. B. im Rahmen von internen Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung.

(8) Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten in das Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragnehmer für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

§ 7
Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

(2) 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 zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber nachweisen. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus Art. 32 DSGVO resultierenden Maßnahmen.
Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

(3) Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt in **Anlage 1** zu diesem Vertrag.

(4) Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DSGVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DSGVO notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Datenschutz-Folgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.

(6) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.

(7) Weiterhin sind alle Personen des Auftragnehmers bzgl. der Pflichten zur Wahrung von Geschäfts- und Betriebsgeheimnissen des Auftraggebers zu verpflichten und müssen auf § 23 GeschGehG hingewiesen werden.

(8) Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit

benannt.

(10) Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DSGVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt werden muss, wird der Auftragnehmer dem Auftraggeber einen Ansprechpartner bekannt geben.

(11) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen. Er 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. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Art. 33 und 34 DSGVO.

(12) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(13) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder andere Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind.

(14) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer betroffenen Person verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen.

(15) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.

(16) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber nochmals bestätigt oder geändert wird.

(17) 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 die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegen.

(18) Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung und setzt auch keine Mittel zur Verarbeitung ein, die nicht vom Auftraggeber zuvor genehmigt wurden.

(19) Der Auftragnehmer speichert keine Kunden-/ Patientendaten (z.B.: Patienten-, Bewohnerdaten) auf Systemen, die außerhalb der Verfügungsgewalt des Auftraggebers liegen bzw. die nicht dem Beschlagnahmeschutz unterliegen.

(20) Sofern der Auftragnehmer durch das Recht der Union oder Mitgliedstaaten verpflichtet ist, die Daten auch auf andere Weise zu verarbeiten, so teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. Die Mitteilung hat zu unterbleiben, wenn das einschlägige nationale Recht eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet.

(21) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.

§ 8

Fernzugriff bei Prüfung / Wartung eines Systems oder anderen Dienstleistungen über Fernzugriffe

Für die Durchführung von Fernzugriffen bei der Prüfung und / oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen gelten ergänzend folgende Rechte / Pflichten des Auftraggebers / Auftragnehmers:

(1) Fernzugriffe im Rahmen von Prüfungs- und / oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten / zuständigen Mitarbeitenden (im Folgenden auch "MA") des Auftraggebers durchgeführt.

(2) Fernzugriffe im Rahmen von Prüfungs- und / oder Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen werden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, ausschließlich mit Zustimmung des Auftraggebers ausgeführt.

(3) Die Mitarbeitenden des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren.

(4) Vor Durchführung von Fernzugriffen werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherheitsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.

(5) Fernzugriffe im Rahmen von Prüfungs- und / oder Wartungsarbeiten werden dokumentiert und protokolliert. Der Auftraggeber ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei Fernzugriffen ist der Auftraggeber – soweit technisch möglich – berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.

(6) Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insbesondere IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfang – auch in zeitlicher Hinsicht – Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

(7) Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z. B. auch lesender Zugriff) oder ein Zugriff auf Produktivdaten (Wirk- / Echtdaten) des Auftraggebers notwendig ist, wird der Auftragnehmer die vorherige Einwilligung des Auftraggebers einholen.

(8) Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Produktivdaten erforderlich ist, bedürfen der vorherigen Einwilligung des Auftraggebers. Bei Datenabzug der Produktivdaten wird der Auftragnehmer diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers löschen. Produktivdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des Auftraggebers oder auf solchen des Auftragnehmers verwendet werden, sofern die vorherige Einwilligung des Auftraggebers vorliegt. Produktivdaten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (PDAs, USB- Speichersticks oder ähnliche Geräte) kopiert werden.

(9) Fernzugriffe im Rahmen von Prüfungs- und / oder Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt. In diesem Zusammenhang wird der Auftragnehmer die technischen und organisatorischen Maßnahmen, wie im Anhang beschrieben, ergreifen.

§ 9

Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtskonform erbringen kann.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat – neben der eigenen Verpflichtung des Auftragnehmers – ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.

(4) Dem Auftraggeber obliegen die aus Art. 33 und 34 DSGVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.

(5) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und / oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

(6) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

(7) Weiterhin sind alle Personen des Auftraggebers bzgl. der Pflichten zur Wahrung von Geschäfts- und Betriebsgeheimnissen des Auftragnehmers zu verpflichten und müssen auf § 23 GeschGehG hingewiesen werden.

(8) Der Auftraggeber stellt sicher, dass die aus Art. 32 DSGVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden. Insbesondere gilt dies für Fernzugriffe des Auftragnehmers auf die Datenbestände des Auftraggebers.

(9) Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen. Sofern der vereinbarte Leistungsumfang überschritten wird, ist hierzu vorab eine gesonderte schriftliche Vereinbarung zu treffen.

§ 10

Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichend Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte und Freiheiten der betroffenen Person gewährleistet. Er dokumentiert das Ergebnis seiner Auswahl.

Hierfür kann er beispielsweise

- datenschutzspezifische Zertifizierungen oder Datenschutzsiegel und -prüfzeichen berücksichtigen,
- schriftliche Selbstauskünfte des Auftragnehmers einholen,
- sich ein Testat eines Sachverständigen vorlegen lassen oder

- sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen darf, von der Einhaltung der vereinbarten Regelungen überzeugen.

(2) Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte auch hierbei weitestgehend vermieden werden.

(3) Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftraggeber im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags wird vom Auftragnehmer unterstützt. Insbesondere verpflichtet sich der Auftragnehmer, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

(4) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 11

Berichtigung, Beschränkung von Verarbeitung, Löschung und Rückgabe von Datenträgern

(1) Während der laufenden Beauftragung berichtigt, löscht oder sperrt der Auftragnehmer die vertragsgegenständlichen Daten nur auf Anweisung des Auftraggebers.

(2) Sofern eine Vernichtung während der laufenden Beauftragung vorzunehmen ist, übernimmt der Auftragnehmer die nachweislich datenschutzkonforme Vernichtung von Datenträgern und sonstiger Materialien nur aufgrund entsprechender Einzelbeauftragung durch den Auftraggeber. Dies gilt nicht, sofern im Hauptvertrag bereits eine entsprechende Regelung getroffen worden ist.

(3) In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

(4) Nach Abschluss der Erbringung der Verarbeitungsleistungen oder bereits nach Aufforderung durch den Auftraggeber muss der Auftragnehmer alle personenbezogenen Datenträger an den Auftraggeber aushändigen und die Daten und Verarbeitungsergebnisse auf Anweisung des Auftraggebers datenschutzkonform zu löschen bzw. zu vernichten, sofern nicht nach dem Unionsrecht oder dem für den Auftragnehmer geltendem nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Gleiches gilt für alle Daten, die Betriebs- oder Geschäftsgeheimnisse des Auftraggebers beinhalten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(5) Sofern zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten entstehen, bedarf es einer vorherigen schriftlichen Vereinbarung über die Kostenverteilung bzw. Kostenübernahme.

(6) Soweit ein Transport des Speichermediums vor Löschung unverzichtbar ist, wird der Auftragnehmer angemessene Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtes Lesen, Kopieren oder Verändern treffen. Die Maßnahmen und die anzuwendenden Löschverfahren werden bei Bedarf ergänzend zu den Leistungsbeschreibungen konkretisierend vereinbart.

(7) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(8) Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer aufgrund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag anders vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(9) Sollte dem Auftraggeber eine Rücknahme der Daten nicht möglich sein, wird er den Auftragnehmer rechtzeitig schriftlich informieren. Der Auftragnehmer ist dann berechtigt, personenbezogene Daten im Auftrag des Auftraggebers zu löschen.

(10) Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung bzgl. einer Löschung nicht erforderlich, diese müssen direkt nach Zweckerfüllung gelöscht werden.

§ 12

Unterauftragnehmer

(1) Der Auftragnehmer nimmt keinen Unterauftragnehmer ohne vorherige explizite schriftliche oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch. Dies gilt in gleicher Weise für den Fall, dass weitere Unterauftragsverhältnisse durch Unterauftragnehmer begründet werden. Der Auftragnehmer stellt sicher, dass eine entsprechende Genehmigung des Auftragsgebers für alle im Zusammenhang mit der vertragsgegenständlichen Verarbeitung eingesetzten weiteren Unterauftragnehmer vorliegt.

(2) Die nachfolgenden Regelungen finden sowohl für den Unterauftragnehmer als auch für alle in der Folge eingesetzten weiteren Unterauftragnehmer entsprechende Anwendung.

(3) Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

(4) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht. Hierbei muss jedoch jeder Unterauftragnehmer (verbundenes Unternehmen) vor Beauftragung dem Auftraggeber schriftlich angezeigt werden, so dass der Auftraggeber bei Vorliegen wichtiger Gründe die Beauftragung untersagen kann.

(5) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der **Anlage 2** aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und / oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt.

(6) Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.

(7) Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Unterauftragnehmer im Wege eines Vertrages dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie den in diesem AV-Vertrag beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

(8) Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

(9) Ein zustimmungspflichtiges Unterauftragnehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei Reinigungs-, Post- und Versanddienstleistungen.

Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremdvergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Die Nebenleistungen sind vorab detailliert zu benennen.

(10) Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Nichteinhaltung der Pflichten jenes Unterauftragnehmers.

§ 13
Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen, es sei denn, die Gegenrechte des Auftragnehmers sind unstreitig oder rechtskräftig festgestellt.

§ 14
Haftung

(1) Auftraggeber und Auftragnehmer haften gemeinsam für den Schaden, der im Außenverhältnis gegenüber der jeweiligen betroffenen Person durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wird.

(2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der er den aus der DSGVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder

- er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
- er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

(3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er

- seinen ihm speziell durch die DSGVO auferlegten Pflichten nicht nachgekommen ist oder
- unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder

- gegen diese Anweisungen gehandelt hat.

(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

§ 15

Schriftformklausel

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaier Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Regelungen handelt. Das Schriftformerfordernis gilt auch für den Verzicht auf dieses Formerfordernis.

§ 16

Salvatorische Klausel

(1) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

(2) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(3) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

(4) Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter § 11 Abs. 1 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Daten im Sinne dieses Vertrages am besten gewährleistet.

§ 17

Rechtswahl, Gerichtsstand

Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftraggebers.

_____

Ort, Datum

_____

Auftragnehmer

Anlage 1 zu § 7 Abs. 3 des AV-Vertrages

Technisch-organisatorische Maßnahmen“ nach Art. 28 Abs. 3 Ziffer c, 32 DSGVO

1. Technische und organisatorische Sicherheitsmaßnahmen

Gemäß Art. 28 Abs. 3 Ziffer c, Art. 32 DSGVO sind die Vertragspartner verpflichtet, die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.

2. Innerbetriebliche Organisation des Auftragnehmers

Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

3. Konkretisierung der Einzelmaßnahmen

Im Einzelnen werden folgende Maßnahmen bestimmt (bitte Zutreffendes ankreuzen oder unter „Sonstiges“ ergänzen)

Nr.	Maßnahme	Eingehalten	
		Ja	Nein
1	**Vertraulichkeit**		
1.1	**Zutrittskontrolle**: Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	☐	☐
	Zutrittsregelung für betriebsfremde Personen	☐	☐
	Protokollierung Besucher, externe Dienstleister	☐	☐
	Zentraler Empfangsbereich (Pförtner / Empfang) vorhanden	☐	☐
	Ausgabe und Rücknahme von Besucherausweisen	☐	☐
	Aufenthalt betriebsfremder Personen nur in Anwesenheit von Mitarbeitern	☐	☐
	Gebäudesicherung durch Alarmanlage	☐	☐
	Gebäudeüberwachung durch Video, Werkschutz oder Nachtwächter	☐	☐
	Maßnahmen zur Objektsicherung bei Fenster und Schächten	☐	☐
	Automatische Türsicherungen (elektrische Türöffner und Schließautomatik)	☐	☐
	Chipkarten-/Transponder-Schließsystem	☐	☐
	Manuelles Schließsystem	☐	☐
	Festgelegte Serverraumzutrittsberechtigungen einschließlich Schlüsselregelung und Zutrittsprotokollierung.	☐	☐
	Sonstiges:	☐	☐

Nr.	Maßnahme	Eingehalten	
		Ja	Nein
1.2	**Zugangskontrolle**: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	☐	☐
	Authentifikation mit individuellem Benutzername/Passwort bzw. bio- metrisches Verfahren	☐	☐
	Regelung Passwortvergabe (Art, Dauer, Sperrung)	☐	☐
	Zuordnen von Benutzerprofilen zu IT-Systemen	☐	☐
	Automatische, passwortgeschützte Rechnersperre	☐	☐
	Regelung für die Löschung von Berechtigungen ausgeschiedener MA	☐	☐
	Verbindliches Verfahren zur Vergabe von Berechtigungen	☐	☐
	Einsatz von Anti-Viren-Software	☐	☐
	Verschlüsselung von Datenträger	☐	☐
	Sicherung interner Netze gegen unberechtigte Zugriffe von extern (Firewall)	☐	☐
	Externer Zugriff auf interne Netze durch VPN-Technologie	☐	☐
	Sonstiges:	☐	☐

Nr.	Maßnahme	Eingehalten	
		Ja	Nein
1.3	**Zugriffskontrolle**: Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	☐	☐
	Erstellung von Benutzerprofilen	☐	☐
	Erstellen Berechtigungskonzept mit differenzierten Berechtigungsstufen	☐	☐
	Dokumentation der Berechtigungen	☐	☐
	Regelung zum Kopieren von Daten	☐	☐
	Deaktivierung oder Sicherung von USB-Anschlüssen und Brennern	☐	☐
	Zeitliche Begrenzung der Zugriffsmöglichkeiten (z.B. Wochenende)	☐	☐
	Protokollierung und datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	☐	☐

	Alle MA sind zur Vertraulichkeit und auf die Weisungsgebundenheit verpflichtet	☐	☐
	Sonstiges:	☐	☐

Nr.	Maßnahme	Eingehalten	
		Ja	Nein
1.4	**Trennungskontrolle**: Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	☐	☐
	Logische Mandantentrennung	☐	☐
	Berechtigungskonzept mit Festlegung der Zugriffsrechte	☐	☐
	Daten unterschiedlicher Auftraggeber/Projekte werden soweit möglich auf unterschiedlichen Systemen verarbeitet	☐	☐
	Trennung von Produktiv- und Testsystem	☐	☐
	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System	☐	☐
	Sonstiges:	☐	☐

Nr.	Maßnahme	Eingehalten	
		Ja	Nein
1.5	**Pseudonymisierung:** Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.	☐	☐
	In der Datenverarbeitung wird nach Buchung die Daten, die den Personenbezug ermöglichen (Name, Vorname, Adresse etc.) durch ein Pseudonym ersetzt.	☐	☐
	Die Tabelle, die Re-Pseudonymisierung ermöglicht, wird in einem verschlüsselten Verzeichnis aufbewahrt. Auf dieses Verzeichnis hat nur ein sehr kleiner Personenkreis Zugriffsrechte.	☐	☐
	Sonstiges:	☐	☐

Nr.	Maßnahme	Eingehalten	
		Ja	Nein
2	**Integrität**	☐	☐
2.1	**Weitergabekontrolle:** Es ist zu 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	☐	☐
	Einsatz von Verschlüsselung in Aufbewahrung und Transport	☐	☐
	Zugriff auf personenbezogene Daten nur über authentifizierte Kanäle	☐	☐
	Dokumentation von Datenempfängern bei Transport oder Übermittlung	☐	☐
	Dokumentation der Abruf- und Übermittlungsprogramme	☐	☐
	Auswertemöglichkeiten der Übermittlungsprotokolle	☐	☐
	Führen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen	☐	☐
	Automatische Sperre bei mehrmaliger fehlerhafter Authentifizierung	☐	☐
	Bei physischem Transport sichere Transportbehälter/-verpackungen	☐	☐
	Einsatz von E-Mail-Verschlüsselungen bei personenbezogenen Daten	☐	☐
	Datenschutzgerechte Vernichtung von Datenträgern (z.B. Fehldrucke)	☐	☐
	Sonstiges:	☐	☐

Nr.	Maßnahme	Eingehalten	
		Ja	Nein
2.2	**Eingabekontrolle**: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	☐	☐
	Protokollierung der Eingabe, Änderung und Löschung von Daten	☐	☐
	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	☐	☐
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	☐	☐
	Übersicht, mit welchen Applikationen Daten eingegeben, geändert oder gelöscht werden können.	☐	☐
	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden.	☐	☐

	Löschungsregelung für Protokolldaten	☐	☐
	Sonstiges:	☐	☐

Nr.	Maßnahme	Eingehalten	
		Ja	Nein
3	**Verfügbarkeit und Belastbarkeit**	☐	☐
3.1	**Verfügbarkeitskontrolle**: Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	☐	☐
	Notfallkonzept bei IT-Störungen vorhanden	☐	☐
	Redundante Absicherung von Servern und Datenbeständen	☐	☐
	Unterbrechungsfreie Stromversorgung (USV) in Serverräumen	☐	☐
	(Redundante) Klimaanlage in Serverräumen	☐	☐
	Automatische Feuer- und Rauchmeldeanlagen	☐	☐
	Feuerlöscheinrichtungen im Serverraum	☐	☐
	Alarmmeldungen bei unberechtigten Zutritten zu Serverräumen	☐	☐
	Sicherungs- und Wiederherstellungskonzept von Daten	☐	☐
	Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort	☐	☐
	Rekonstruktion von Datenbeständen und Test der Datenbestände	☐	☐
	Einsatz von Virenscannern	☐	☐
	Automatisierte Aktualisierung von Virenscannern	☐	☐
	Richtlinien zur Wartung und Durchführung von Updates	☐	☐
	Automatisches und permanentes Monitoring zur Erkennung von Störungen	☐	☐
	Sonstiges:	☐	☐

Nr.	Maßnahme	Eingehalten	
		Ja	Nein
3.2	**Belastbarkeit:** Sicherstellung der Belastbarkeit der Systeme und Dienste.	☐	☐
	Es werden regelmäßige Belastungstest durchgeführt und deren Ergebnis dokumentiert	☐	☐

	Ein Load Balancing verteilt die Last auf der Serverfarm, um eine gleiche Verteilung der Belastung der Server zu gewährleisten.	☐	☐
	Sonstiges:	☐	☐

Nr.	Maßnahme	Eingehalten	
		Ja	Nein
4	**Rasche Wiederherstellbarkeit:** Fähigkeit zur raschen Wiederherstellung personenbezogenen Daten nach einem physischen oder technischen Zwischenfall.	☐	☐
	Es wird ein IT-Notfallhandbuch eingesetzt, das regelmäßig aktualisiert und auf dem neusten Stand gehalten wird.	☐	☐
	Es wird regelmäßig eine Wiederherstellung (Recovery) zentraler Anwendungen getestet.	☐	☐
	Sonstiges:	☐	☐

Nr.	Maßnahme	Eingehalten	
		Ja	Nein
5	**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** Regelmäßige Durchführung eines Verfahrens zur Überprüfung, Bewer- tung und Evaluierung der Wirksamkeit der technischen und organisatori- schen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.	☐	☐
5.1	**Datenschutzmanagementsystem (DSMS):**		
	Es besteht eine Richtlinie im Rahmen des Datenschutzmanagement- systems, die die regelmäßige Durchführung, Bewertung und Evaluierung der technisch organisatorischen Maßnahmen festlegt.	☐	☐
	Es werden regelmäßig Audits durchgeführt und dokumentiert, um die Beachtung und Umsetzung der Richtlinie im Unternehmen zu prüfen.	☐	☐
	Das DSMS wird als Plan-Do-Check-Act Regelkreis umgesetzt, so dass in einem Audit erkannte Defizite behoben werden	☐	☐
	Sonstiges:	☐	☐

	Maßnahme	Eingehalten	
5.2	**Datenschutz als Standard:**	**Ja**	**Nein**
	Datenschutzfreundliche Voreinstellungen – Das Prinzip aus Art. 25 DSGVO Privacy by default wird umgesetzt.	☐	☐
	Datenschutz durch Technikgestaltung – Das Prinzip aus Art. 25 DSGVO Privacy by design wird umgesetzt.	☐	☐

	Sonstiges:	☐	☐

	Maßnahme	Eingehalten	
		Ja	**Nein**
5.3	**Auftragskontrolle:** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	☐	☐
	Kontrolle der Datensicherheitsvorkehrungen und schriftlicher Nachweis	☐	☐
	Bestellung eines Datenschutzbeauftragten	☐	☐
	Verpflichtung der MA auf das Datengeheimnis	☐	☐
	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags	☐	☐
	Sonstiges:	☐	☐

Anlage 2 zu § 12 Abs. 5 des AV-Vertrages

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungser- bringung