ANHANG

STANDARDVERTRAGSKLAUSELN

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1 Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den

Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6 Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste

aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung

von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

   1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

   2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

   3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

   4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend,

damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

   1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

   2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

   3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

   a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.
Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I – LISTE DER PARTEIEN

1. Verantwortliche(r):

Firma und Anschrift des Verantwortlichen ergeben sich aus dem Angebot der WGsystem GmbH.

Eine gesonderte Unterzeichnung dieser Standardvertragsklauseln durch den Verantwortlichen ist nicht erforderlich. Diese Standardvertragsklauseln sind integraler Bestandteil des Subskriptions-Vertrages. Mit Gegenzeichnung des Angebots der WGsystem GmbH zum Abschluss des Subskriptions-Vertrages durch den Verantwortlichen werden auch diese Standardvertragsklauseln verbindlich abgeschlossen.

2. Auftragsverarbeiter:

Name: WGsystem GmbH
Anschrift: Salzstraße 25, 87499 Wildpoldsried

Name, Funktion und Kontaktdaten der Kontaktperson(en):

Claudia Kirchgessner
Head of Backoffice
Unterschrift: i.V. C. Kirchgessner

Silvia Emilius
Backoffice
Unterschrift: i.A. Emilius

Datenschutzbeauftragte(r): Joachim Hanke

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden
Mitarbeiter des Kunden, Organe des Kunden, sonstige Personen, deren Daten der Kunden in seinen Systemen speichert, auf die WGsystem Zugriff hat.
Kategorien personenbezogener Daten, die verarbeitet werden
Daten, die Auskunft über den Zugriff und die sonstige Nutzung der WGsystem-Software durch die oben genannten Personengruppen auf Seiten des Kunden geben, wie z.B. Log-Daten, etc.
Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen
Es erfolgt keine Verarbeitung sensibler Daten
Art der Verarbeitung
Die Daten werden nicht zielgerichtet seitens der WGsystem verarbeitet. Vielmehr erfolgt eine Verarbeitung lediglich insoweit, als ein Zugriff auf die Daten unumgänglich ist, um den Subskriptions-Vertrag, insbesondere die darunter geschuldeten Pflegeleistungen, erfüllen zu können.
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden
Durchführung des Subskriptions-Vertrag.
Dauer der Verarbeitung
Für die Laufzeit des Subskriptions-Vertrages.
Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.
Eine Verarbeitung durch Unter-Auftragsverarbeiter erfolgt lediglich in dem oben angegebenen Umfang und für die oben angegebene Dauer und nur insoweit, als der Subskriptions-Vertrag die Einschaltung von Unter-Auftragsverarbeitern erlaubt.

ANHANG III – Technische und organisatorische Maßnahmen

1. Pseudonymisierung
Es findet eine direkte Verarbeitung von personenbezogenen Daten im Auftrag statt. Die mögliche Sichtbarkeit oder ein möglicher Zugriff auf personenbezogene Daten besteht. Eine Pseudonymisierung oder Anonymisierung findet nicht statt.

2. Verschlüsselung
Alle mobilen Datenträger werden nach dem Stand der Technik verschlüsselt. Die internen IT-Richtlinien regeln den Umgang mit Daten sowie deren Speicherung.

3. Sicherstellung der Vertraulichkeit	
Zutrittskontrolle:	Bei der Art des Gebäudes handelt es sich um ein Bürogebäude, welches nur durch die Firmen SEMA GmbH und WGsystem GmbH genutzt wird. Die Eingangstüren werden durch ein Sicherheitsschloss mit Elektromotor gesichert. Diese Schlösser lassen sich nur mittels Chipkarte öffnen. Nach außen sind die Eingangstüren nur mit einem starren Türknauf anstelle einer Klinke versehen und außerhalb der Geschäftszeiten durch das Motorschloß gesperrt. Die Personalunterlagen sind außerhalb der Geschäftszeiten in Aktenschränken eingesperrt. Der Serverraum wird ebenfalls durch ein Sicherheitsschloss mit Elektromotor gesichert, welches sich nur durch eine Chipkarte öffnen lässt. Dieser Raum ist rund um die Uhr abgesperrt. Chipkarten werden ausschließlich an Berechtigte ausgegeben und sofort eingezogen, wenn die Berechtigung erlischt. Die Berechtigung zum Betreten wird durch geeignete Maßnahmen protokolliert und dokumentiert. Bei Verlust eines Zutrittsmittels oder wenn ein ehemals Berechtigter ein Zutrittsmittel nicht freiwillig zurückgibt, wird das Zutrittsmittel individuell gesperrt. Bei der Fensterart des Gebäudes und der Büro- und Geschäftsräume handelt es sich um 3-fach Isolierverglasung. Die Fenster sind in allen Lagen außerhalb der Geschäftszeiten geschlossen. Fremden Personen ist der Aufenthalt im gesamten Unternehmensgebäude nur in Anwesenheit von Mitarbeitern gestattet. Hilfspersonen werden stets sorgfältig ausgewählt. Es liegt eine Chipkarte mit der Zutritts-Berechtigung zu allen drei Außentüren bei der freiwilligen Feuerwehr Wildpoldsried in einem dafür vorgesehenen Safe.
Zugangs- und Zugriffskontrolle	Für den Zugriff auf die Datenverarbeitungssysteme ist ein Passwortsystem eingerichtet. Eine Passwortrichtlinie ist festgelegt. Jeder Berechtigte erhält eine individuelle Benutzerkennung und ein persönliches, geheim zu haltendes Passwort, welches nicht an Dritte weitergegeben werden darf. Für den Fall der Abwesenheit besteht eine Regelung. Berechtigungen werden regelmäßig kontrolliert. Das Passwort wird gesperrt, falls die Berechtigung erlischt. Das Passwort besteht aus wenigstens 14 Zeichen (zufällig ausgewählten Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen). Nach drei Fehlversuchen erfolgt eine Sperre der Benutzerkennung. Interne Netze werden nach dem Stand der Technik gegen Zugriffe von außen durch eine vollständige physische Trennung interner und externer Netze abgeschottet. Eine Firewall mit wenigstens täglicher Softwareaktualisierung ist eingerichtet. Verbindungswege von außen werden über https und Zertifikate abgesichert. Die Zugriffe der Benutzer werden bei An- und Abmeldung protokolliert. Organisatorische Voraussetzungen wie z.B. Organigramme, Stellenbeschreibungen und Aufgabenbeschreibungen sind vorhanden. Diese werden regelmäßig aktualisiert und in Rollendefinitionen umgesetzt. Die

	Rollenzuordnung wird regelmäßig überprüft. Ein Berechtigungskonzept ist im Einsatz. Innerhalb des Zugriffsberechtigungskonzepts sind abgestufte Zugriffsberechtigungen aufgebaut, die das Eingeben, Lesen, Kopieren, Verändern oder Entfernen von Auftraggeber-Daten bei der Verarbeitung, Nutzung und nach der Speicherung nur in dem für die jeweilige Aufgabe erforderlichen Umfang erlauben und ansonsten verhindern. Das Zugriffsberechtigungskonzept umfasst die Verwaltung der Zugriffsrechte durch Systemadministratoren. Der Testbetrieb wird vom Produktionsbetrieb getrennt. Die Internet- und E-Mail-Nutzung erfolgt kontrolliert und organisiert, zudem ist die private Internet- und E-Mail-Nutzung im Unternehmen geregelt. Bereiche, in welchen Datenträger aufbewahrt werden sind besonders abgesichert. Nicht mehr benötigte Datenträger und Fehldrucke werden datenschutzgerecht entsorgt.
Trennungskontrolle	Die Daten werden für mehr als eine verantwortliche Stelle gespeichert, die Speicherung erfolgt in einer mandantenfähigen Datenbank. Die Zwecke, für die die jeweiligen Daten verarbeitet und genutzt werden sollen werden dokumentiert. Die Zugriffsrechte sind klar festgelegt. Ein Konzept für die Datenerhebung- und Verarbeitung ist vorhanden. Die Produktionsnetze sind durch geeignete Maßnahmen physikalisch vom Testnetz getrennt. Das Sicherheitsniveau der Testsysteme ist ebenso hoch wie das der Produktionssysteme. Es ist gewährleistet, dass nur nach Rücksprache mit dem Auftraggeber Produktionsdaten als Testdaten verwendet werden.

4. Sicherstellung der Verfügbarkeit und Belastbarkeit	
Verfügbarkeitskontrolle	Der Auftragnehmer gewährleistet hinreichenden Softwareschutz gegen die Verletzung der Systemintegrität durch speicherresidente Scanner gegen Viren, Trojaner, Würmer und sonstige Malware. Die Ausführung arbeitsplatzfremder Software wird durch vertragliche Verbote der Nutzer, Spamfilter, Lizenzüberwachung und eine wenigstens tägliche Aktualisierung des Betriebssystems, der vorhandenen Betriebs- und Sicherheitssoftware verhindert. Durch eine unterbrechungsfreie Stromversorgung und die Einhaltung der einschlägigen Brandschutzvorschriften wird ein hinreichender Hardwareschutz gewährleistet. Ein Datensicherheitskonzept ist vorhanden. Dieses Konzept sieht vor, dass Sicherungskopien nach dem Generationenprinzip in geeigneten zeitlichen Abständen erstellt werden. Der Datenbestand wird wenigstens einmal täglich inkrementell gesichert und einmal wöchentlich vollständig auf externen Speichermedien verschlüsselt gesichert. Eine wöchentliche Vollsicherung wird im Datenzentrum der Fa. IDKom Networks abgelegt. Ein Notfall-Handbuch/ Notfallkonzept liegt vor.
Auftragskontrolle	Bei der Aushändigung lesbarer Datenträger ist sichergestellt, dass sich darauf keine Restdaten, etwa von anderen Verarbeitungen befinden.

5. Sicherstellung der Integrität	
Weitergabekontrolle	Die Datenübertragung erfolgt über einen Glasfaseranschluss der Telekom via synchronem VDSL, Zweck der Übertragung ist die Auftragsverarbeitung. Die Beteiligten werden identifiziert und authentifiziert. Die Authentifizierung erfolgt über eine Benutzerkennung und ein Passwort. Mobile Datenträger mit Auftraggeber-Daten, mobile Endgeräte mit Auftraggeber-Daten und USB-Ports dürfen nur von speziell zur Datenweitergabe und -sicherung befugten Mitarbeitern ausschließlich für Vertrags- und Sicherungszwecke eingesetzt werden. Das Passwort besteht aus wenigstens 14 Zeichen (zufällig ausgewählten Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen). Generische Begriffe oder Eigennamen dürfen nicht verwendet werden. Eine Dokumentation von Datenempfängern erfolgt. Die Datenträgerentsorgung erfolgt über Herrn Joachim Hanke und der Firma Dorr. Bis zur Vernichtung

	werden die Datenträger im verschlossenen Lager der Abteilung Technik gelagert. Es existiert eine Vereinbarung zur Auftragsverarbeitung mit einem externen Dienstleister.
Eingabekontrolle	Unbefugte Eingaben, Veränderungen und Löschungen werden durch ein Passwortsystem verhindert. Die Eingabe, Veränderung oder Löschung personenbezogener Daten wird revisionssicher protokolliert. Die Eingabeberechtigungen werden revisionssicher geführt und schriftlich erteilt. Die Eingabebefugnisse sind auf erstellte Protokolldaten geregelt. Als zentrale Maßnahme werden in der Eingabekontrolle die Systemprotokolle regelmäßig ausgewertet. Die Systemprotokolle werden anonym ausgewertet und nur bei konkretem Anlass werden die betreffenden Nutzer identifiziert. Es besteht eine Löschregelung für Protokolldaten. Alle Mitarbeiter sind auf die Vertraulichkeit verpflichtet. Folgende Anwendungen haben eine zweite Zugangskontrolle: Adito, Outlook, SAGE, BBS Reisekosten, HR Works, Sämtliche Banksoftware, Docuguide, WGsystem. Keine zweite Zugangskontrolle haben hingegen folgende Anwendungen: gesamt Office, außer Outlook.

6. Wiederherstellung der Daten

Es besteht ein eigenes, umfangreiches Backup-Konzept und ein Notfallhandbuch. Es wird Backupsoftware namhafter Hersteller eingesetzt.

7. Laufende Bewertung und Evaluierung

Eine Datenschutzleitlinie ist implementiert. Ein Datenschutzbeauftragter ist bestellt und wird regelmäßig im Datenschutz geschult. Die Mitarbeiter-/innen werden regelmäßig in Datenschutzangelegenheiten unterwiesen. Ein Meldeprozess für eine Datenschutzverletzung ist implementiert.
Die technischen und organisatorischen Maßnahmen werden jährlich durch den Datenschutzbeauftragten sowie den Leiter IT auditiert. Im Rahmen des Audits werden die Maßnahmen in Bezug auf den Stand der Technik, sowie die notwendigen technischen und rechtlichen Anforderungen geprüft und ggf. angepasst. Das Ergebnis des Audits wird entsprechend dokumentiert.