Nutzungsbedingungen
ScanAdhoc und Pharma-Control

1. Gegenstand (Allgemeines, Geltungsbereich)

1.1. Die NOVENTI HealthCare GmbH, Berg-am-Laim-Str. 105, 81673 München (im Folgenden „NHC“), hat die exklusiven Nutzungs- und Verwertungsrechte an der Software „ScanAdhoc“ und „Pharma-Control“ (im Folgenden zusammen „Vertragsprodukte“) inne.

1.2. Gegenstand dieser AGB ist die Regelung der Nutzung der dem Anwender/Nutzer in Form der jeweiligen Apotheke (im Folgenden „Vertragspartner“) durch NHC zur Verfügung gestellten Vertragsprodukte.

1.3. Die Vertragsprodukte richten sich an Unternehmer (i.S.v. § 14 BGB) in Form von Apotheken. Ein Nutzungsvertrag auf Grundlage dieser AGB kann somit nur zwischen einem Unternehmer als Vertragspartner (in Form eines Institutionskennzeichens, IK) und dem Lizenzgeber zustande kommen („B2B-Fall“).

1.4. Von diesen AGB abweichende oder sie ergänzende Bedingungen des Vertragspartners werden vom Lizenzgeber nicht anerkannt, auch wenn NHC nicht widerspricht oder der Vertragspartner erklärt, nur zu seinen Bedingungen liefern zu wollen.

2. Vertragsschluss

2.1. Das Vertragsverhältnis über die Nutzung der Vertragsprodukte kommt erst nach einer (Online-) Registrierung des Vertragspartners und der anschließenden Annahmeerklärung von NHC zustande.

2.2. Bei der (Online-) Registrierung gibt der Vertragspartner zunächst seine zur Vertragsdurchführung erforderlichen Daten an. Änderungen dieser Daten teilt der Vertragspartner dem Lizenzgeber während des mit Vertragsschluss (siehe nachstehende Regelungen) eigegangenen Vertragsverhältnisses unverzüglich mit.

2.3. Mit seiner vorzugsweise im Internet (z.B. https://www.vsa.de/formulare/scanadhoc-bestellung) abgegebenen Bestellung (Erklärung) gibt der Vertragspartner einen Antrag an NHC auf Abschluss eines Vertrages über die Nutzung der o. g. Vertragsprodukte zu den jeweiligen Konditionen ab. Dieser Antrag muss vom Lizenzgeber im Wege einer Annahmeerklärung angenommen werden. Die Bestell-/Eingangsbestätigung stellt noch keine solche Annahmeerklärung dar. Die Annahmeerklärung liegt vielmehr in der ausdrücklichen Erklärung von NHC, wonach dieser seine Zustimmung zum o. g. Antrag des Vertragspartners erklärt. Dies erfolgt spätestens mit der Zurverfügungstellung der Vertragsprodukte. Erst durch besagte Annahmeerklärung von NHC kommt ein Vertrag zwischen Vertragspartner und Lizenzgeber auf Basis dieser AGB zustande.

2.4. Nach erfolgtem Vertragsschluss werden die ggf. bereits installierten Vertragsprodukte, je nach getroffener Auswahl, für den Vertragspartner freigeschaltet. Erforderlichenfalls erhält der Vertragspartner bei noch nicht installierten Vertragsprodukten einen Link zum Download der jeweiligen Software. Für den Fall, dass Installationsunterstützung und/oder für den Betrieb der Software erforderliche Komponenten (etwa der unten genannte Scanner) erforderlich sind, wird sich NHC zeitnah mit dem Lizenzgeber in Verbindung setzen.

3. Produktbeschreibung

3.1. **ScanAdhoc** dient zur umfangreichen Rezeptkontrolle mit den Schwerpunkten Retaxationssicherheit sowie Abgabekontrolle. Ziel des Programmes ist das grundsätzliche Auffinden von fehlerhaften Informationen auf Rezepten sowie der bestmögliche Schutz vor Retaxationen. Wesentliche Aufgaben des Programms ScanAdhoc sind vor allem das Scannen und Auslesen der Rezeptinformationen und das anschließende Prüfen auf Abrechnungskonformität.

3.2. **Pharma-Control** ist ein ggf. optionales Zusatzmodul von ScanAdhoc. Pharma-Control soll bei der Überprüfung unterstützen, ob das taxierte Arzneimittel der Verordnung entspricht.

3.3. Für den Leistungs- und Funktionsumfang der Vertragsprodukte sind ausschließlich diese Bedingungen (AGB) maßgeblich. Etwaige anderslautende Beschreibungen (etwa im Internet, Werbemedien, etc.) enthalten lediglich freibleibende Angaben.

4. Systemanforderungen

4.1. Die folgenden Anforderungen müssen auf Seiten des Vertragspartners und auf dessen Kosten erfüllt sein:

4.1.1. **Technische Voraussetzungen**

- Dokumentenscanner mit Duplex-Scanfunktion und TWAIN-Schnittstelle (Scan-Auflösung mindestens 300 dpi)
- Internetverbindung (während der Nutzung der Vertragsprodukte)
- PC-Arbeitsplatz (Mindestanforderungen: Prozessor mind. Intel Core-2 Duo 6600; 2.4 GHz oder vergleichbar, Arbeitsspeicher: mind. 4 GB, minimale Bildschirmauflösung: 1280x1024

4.1.2. **Softwarevoraussetzungen**

- Microsoft Windows-Betriebssystem ab Version Windows 10

5. Laufzeit, Vertragsbeginn, Vertragsende, Kündigungsmöglichkeiten

5.1. Der Vertrag über die Nutzung der Vertragsprodukte beginnt mit der Annahmeerklärung von NHC (vgl. oben unter Ziff. 2. Vertragsschluss) und wird auf unbestimmte Zeit geschlossen. Er kann von beiden Seiten mit einer Frist von einem Monat zum Ende eines Kalendermonats ordentlich gekündigt werden.

5.2. Das Recht zur außerordentlichen Kündigung richtet sich nach den gesetzlichen Bestimmungen. Dem Lizenzgeber steht dabei ein außerordentliches Kündigungsrecht insbesondere zu, wenn sich der Vertragspartner mit mindestens zwei Monatsgebühren in Verzug befindet.

5.3. Nach Beendigung des Vertrages ist die Nutzung der Vertragsprodukte und insbesondere die Online-Prüfung nicht mehr möglich. Der Vertragspartner hat damit keinen Zugriff mehr auf die erfassten und geprüften Rezeptdaten.

6. Nutzungsrecht

6.1. NHC räumt dem Vertragspartner mit vollständiger und termingerechter Bezahlung der vereinbarten Gebühren für die Dauer des Vertragsverhältnisses und für die in diesen Bedingungen geregelten Verwendungszwecke ein einfaches Nutzungsrecht an den Vertragsprodukten (Software ScanAdhoc und ggf. Pharma-Control), zur Installation und Nutzung durch den Vertragspartner, bezogen auf das jeweilige IK (Institutionskennzeichen), ein.

6.2. Sofern nicht anderweitig schriftlich vereinbart, ist der Vertragspartner pro lizenziertem Institutionskennzeichen (IK) zur Installation der Software ScanAdhoc auf einem Server bei unbegrenzter Anzahl von Clients berechtigt. Nicht von dem beschriebenen Nutzungsrecht umfasst ist das Recht zur Erteilung von Unterlizenzen, zur Übertragung auf Dritte oder anderweitigen Verwertung (Vervielfältigung, Verbreitung, Ausstellung, Verleihen, Vermieten, Verkauf), zur öffentlichen Wiedergabe, zur Bearbeitung, Umgestaltung, Weiterentwicklung oder Zurückentwicklung (Dekompilierung).

6.3. Der Vertragspartner hat das Recht, eine Sicherungskopie der Software (in Form der Datenbank) zu erstellen, die von ihm sicher verwahrt und vor Missbrauch und Diebstahl geschützt werden muss.

6.4. Der Vertragspartner hat dem Lizenzgeber auf Verlangen von NHC zu ermöglichen, den ordnungsgemäßen

Einsatz der Vertragsprodukte zu überprüfen. Der Vertragspartner wird dem Lizenzgeber auf Verlangen innerhalb einer angemessenen Frist schriftlich Auskunft darüber erteilen, ob die Vertragsprodukte vertragsgemäß genutzt werden, insbesondere ob der vertraglich vereinbarte Nutzungsumfang (z.B. hinsichtlich der Anzahl bzw. des Umfangs der zur Verfügung gestellten Lizenz) sowie die Nutzungsbedingungen nicht überschritten werden.

6.5. Die Vertragsprodukte sind rechtlich geschützt. Alle Urheberrechte, Patentrechte, Markenrechte und sonstigen Leistungsschutzrechte an den Vertragsprodukten stehen im Verhältnis zum Vertragspartner unbeschadet der vertraglich eingeräumten Nutzungsrechte ausschließlich dem Lizenzgeber zu. Urhebervermerke, Seriennummern oder andere der Identifikation dienende Merkmale dürfen vom Vertragspartner nicht entfernt oder verändert werden.

7. Besondere Bestimmungen AVOXA

7.1. Das im Rahmen der Nutzung der Vertragsprodukte überlassene AVOXA-Datenmaterial ist ebenfalls urheberrechtlich geschützt. Alle Rechte an dem besagten Datenmaterial stehen ausschließlich der AVOXA - Mediengruppe Deutscher Apotheker GmbH, Eschborn zu. Über die in diesen Nutzungsbedingungen geregelten Nutzungsrechte hinaus, erwirbt der Vertragspartner keine Rechte an dem Datenmaterial. Der Vertragspartner darf die AVOXA-Datenbanken ausschließlich zu apothekenspezifischen Zwecken über die zentral vom Lizenzgeber zur Verfügung gestellte Rezeptprüfung innerhalb der ScanAdhoc-Applikation bzw. Pharma-Control nutzen. Der Vertragspartner darf die AVOXA-Datenbanken ohne entsprechende Lizenzierung nicht online, insbesondere nicht im Internet, verfügbar machen. Der Vertragspartner darf die AVOXA-Datenbanken nur für eigene Zwecke nutzen und nicht an Dritte weitergeben, auch nicht in Form von Ausdrucken aus dem Datenmaterial, selbst wenn es sich um unwesentliche Teile handelt. Der Vertragspartner ist verpflichtet, einen unbefugten Zugriff auf das Datenmaterial sowie die unbefugte Nutzung oder Kenntnisnahme des Datenmaterials durch Dritte auszuschließen. Der Vertragspartner darf das AVOXA-Datenmaterial nicht verändern oder verändertes Datenmaterial verwenden.

8. Weitere Rechte und Pflichten des Vertragspartners

8.1. Der Vertragspartner ist berechtigt, pro IK (Institutionskennzeichen) eine Kopie des Programms auf einem Server (bei unbegrenzter Anzahl von Clients) zu installieren und zu verwenden. Der Vertragspartner ist weiterhin berechtigt, Listen, Summen und andere Auswertungen lediglich für den eigenen Bedarf zu erstellen und zu verwerten.

8.2. Der Vertragspartner verpflichtet sich, durch geeignete Maßnahmen den unbefugten Zugriff Dritter auf die Software ScanAdhoc und ggf. Pharma-Control nebst Rezeptdaten zu verhindern. Zu diesem Zweck kann u. a. bei der Installation des Programms ein Passwort vergeben werden. Die Mitarbeiter des Vertragspartners sind auf die Einhaltung der vorliegenden AGB wie auch der Bestimmungen der DSGVO und des Urheberrechtsgesetzes hinzuweisen.

8.3. Ein Missbrauch der Daten auf Seiten des Vertragspartners (z.B. unbefugter Zugriff nicht autorisierter Mitarbeiter des Vertragspartners auf die Datenbank) liegt außerhalb der Verantwortung von NHC.

8.4. Der Vertragspartner wird darauf hingewiesen, dass NHC nach entsprechender Information durch den Vertragspartner durch Vergabe eines neuen Passwortes einen weiteren unbefugten Zugriff verhindern kann. Die Kosten für eine solche Passwort-Änderung trägt der Vertragspartner. NHC darf diese Kosten dem Vertragspartner mit der nächstfolgenden Abrechnung belasten.

8.5. Dem Vertragspartner ist bekannt, dass die von ScanAdhoc erfassten Informationen bzw. Rezeptdaten (inkl. der Bilddateien bzw. „Images“ der gescannten Rezepte) lediglich für eine Dauer von 90 Tagen (Kalendertage) in der Software vorgehalten werden bzw. einsehbar sind. Ein Zugriff auf die Daten ist nach diesem Zeitraum grundsätzlich nicht mehr möglich.

8.6. Es obliegt dem Vertragspartner, sich in regelmäßigen Abständen durch Datensicherung gegen Datenverlust zu schützen. Auch eine Datensicherung kann allerdings nicht das Löschen der Daten nach der o. g. 90 Tage-Dauer verhindern.

8.7. Der Internetzugang ist nicht Gegenstand dieser Nutzungsbedingungen. Für den Zugriff auf das Internet sowie für die Anschaffung und den Zustand der eigenen Hard- und Software ist der Vertragspartner selbst verantwortlich. Die Kosten für die Nutzung des Internets, die bei der Nutzung der Vertragsprodukte entstehen, trägt der Vertragspartner ebenfalls selbst.

9. Prüfungsobliegenheiten und Mitwirkung des Vertragspartners

9.1. Die durch die Software ScanAdhoc mögliche Onlineprüfung dient dazu, dem Auftragnehmer bei der Kontrolle seines Handelns zu unterstützen. Der Auftragnehmer bleibt allerdings dafür verantwortlich, die Abfrageergebnisse auf Aktualität, Unstimmigkeiten oder Fehler zu überprüfen und eigenverantwortlich die durch die Software ScanAdhoc gelieferten Hinweise zu bewerten und auf Basis der Gesetzgebung und Vertragssituation zu entscheiden. Diese Eigenverantwortung kann die Software ScanAdhoc nicht ersetzen. Aufgetretene Mängel, Unstimmigkeiten oder Fehler hat der Vertragspartner unverzüglich per E-Mail an info@vsa.de unter Angabe einer möglichst genauen Fehlerbeschreibung zu melden.

9.2. Der Vertragspartner verpflichtet sich, durch geeignete Maßnahmen den unbefugten Zugriff Dritter auf die Software ScanAdhoc sowie die Daten zu verhindern. Die Mitarbeiter des Vertragspartners sind auf die Einhaltung der vorliegenden Vertragsbedingungen sowie der Bestimmungen der DSGVO und des UrhG hinzuweisen.

9.3. Es obliegt dem Vertragspartner, sich in regelmäßigen Abständen durch Datensicherung gegen Datenverlust zu schützen.

10. Preise

10.1. Preise sind netto zzgl. der jeweils gültigen gesetzlichen Umsatzsteuer.

10.2. Die zu zahlenden Preise werden, soweit nicht anders angegeben, grundsätzlich mit Leistungserbringung von NHC, und bei fortdauernder Leistungserbringung mit erstmaliger Zurverfügungstellung der Vertragsprodukte (beispielsweise der Überlassung der Software ScanAdhoc), sofort fällig. Sofern ein monatlicher Preis vereinbart ist, wird dieser monatlich im Voraus fällig.

10.3. Der Vertragspartner ist, sofern er nicht Abrechnungskunde von NHC auf Basis eines gesonderten Abrechnungsvertrages ist, verpflichtet, am SEPA-Lastschriftverfahren teilzunehmen, um die vereinbarten monatlichen Preise für die Nutzung der Vertragsprodukte bei Fälligkeit zu begleichen. Er ist verpflichtet, dem Lizenzgeber bei Vertragsschluss ein Lastschriftmandat zu erteilen und dieses während der Vertragsdauer aufrecht zu halten. Bei Zahlung per Lastschrift informiert NHC den Vertragspartner über die Belastung (Betrag und Fälligkeit) mit einer Ankündigungsfrist von einem Tag (Pre-Notification). Fällt das Fälligkeitsdatum auf einen Nicht-Bankarbeitstag, erfolgt die Belastung am nächsten Bankarbeitstag.

10.4. Besteht aktuell oder in Zukunft zwischen den Vertragsparteien eine Abrechnungs- und Factoringvereinbarung (AFV) oder ein vergleichbares Rechtsgeschäft, ist NHC berechtigt, die Preise für die Nutzung der Vertragsprodukte im Rahmen dieses Factoringvertrags bzw. vergleichbaren Rechtsgeschäfts/Vertrags zu berech-

nen/verrechnen. Gleiches gilt für die jeweils gültige gesetzliche Umsatzsteuer, die auf den Preis erhoben wird.

10.5. Nutzt der Vertragspartner die Vertragsprodukte über den vereinbarten Umfang hinaus, so hat NHC Anspruch auf eine gesonderte Vergütung, die auf der Grundlage der tatsächlichen Nutzung und der aktuellen Preisgestaltung von NHC berechnet und bestimmt wird.

10.6. In allen Fällen, in denen der Vertragspartner mit Zahlungen im Zusammenhang Ansprüchen aus diesem Vertrag in Verzug gerät und dem Vertragspartner erfolglos eine Nachfrist gesetzt wurde, ist NHC berechtigt, seine Leistungen einzustellen, ohne dass es einer weiteren Fristsetzung bedarf.

10.7. Eine Aufrechnung oder die Geltendmachung eines Zurückbehaltungsrechtes wegen seitens von NHC nicht anerkannter oder nicht rechtskräftig festgestellter Gegenansprüche ist ausgeschlossen.

11. Preisanpassung

11.1. NHC darf Preise nach billigem Ermessen der Entwicklung der Kosten, die für die Preisberechnung maßgeblich sind, anpassen. Preisänderungsrelevante Kosten sind insbesondere, Versandkosten, Energiekosten, IT-Betriebs- und Entwicklungskosten, Versicherungskosten und Personalkosten sowie Kosten für die Service-Hotline und Programmieraufwand

11.2. Kostensenkungen werden für die Preisanpassung in gleichem Umfang berücksichtigt, wie Kostensteigerungen. Kostensteigerungen dürfen nur in dem Umfang zur Preiserhöhung herangezogen werden, in dem kein Ausgleich durch rückläufige Kosten bei anderen kostenrelevanten Faktoren erfolgt.

11.3. NHC teilt dem Vertragspartner die Anpassung der Preise in Textform oder über ScanAdhoc mindestens fünf Wochen vor dem Wirksamwerden der Anpassung mit.

11.4. Der Vertragspartner kann im Falle einer Preiserhöhung den Vertrag zum Zeitpunkt des Wirksamwerdens der Anpassung kündigen. Die Kündigung seitens des Vertragspartners muss innerhalb von vier Wochen nach Zugang der Änderungsmitteilung erfolgen; die Kündigung bedarf der Textform. NHC wird den Vertrags-partner auf die Folgen seines Schweigens auf die Ankündigung zur Anpassung der Preise hinweisen.

11.5. Abweichend von Ziff. 11.1 bis 18 werden Änderungen der Umsatzsteuer gemäß Umsatzsteuergesetz zum Zeitpunkt des Wirksamwerdens der Änderung ohne Ankündigung und ohne außerordentliche Kündigungsmöglichkeit an den Vertragspartner weitergegeben; gleiches gilt, soweit nach Vertragsschluss neue Abgaben, insb. Steuern, oder sonstige staatlich veranlasste Be- oder Entlastungen wirksam werden.

11.6. Preisanpassungen bei zusätzlichen Leistungen berechtigen nur zur Kündigung der von der Preisanpassung betroffenen Leistung, nicht jedoch zur Kündigung nicht von der Preisanpassung betroffener zusätzlicher Leistungen bzw. des Abrechnungsvertrages

12. Updates

Updates der Vertragsprodukte werden dem Vertragspartner vom Lizenzgeber bei Bedarf (vgl. nachstehende Bestimmungen) und zu gegebener Zeit zur Verfügung gestellt. Es kann für die ordnungsgemäße Funktion der Vertragsprodukte erforderlich sein, diese Updates auch tatsächlich einzuspielen, was prinzipiell durch den Vertragspartner selbstständig erfolgen muss.

13. Installationsunterstützung und Beratung

13.1. ScanAdhoc (und Pharma-Control) ist ein grundsätzlich selbsterklärendes Programm. Kenntnisse zur Verwendung von Datenbankprogrammen sind jedoch von Vorteil. Die Installation erfolgt, so erforderlich, über eine automatisch ablaufende Installationsroutine. Voraussetzung ist in jedem Fall, dass die Hard- und Software-Anforderungen (siehe oben) erfüllt sind, die dem Vertragspartner bekannt sind. Etwaig erforderliche Installationsunterstützung kann der Vertragspartner gegenüber dem Lizenzgeber gegen zusätzliches Entgelt auf Anfrage in Anspruch nehmen.

13.2. Sollte der Vertragspartner die o. g. Anforderungen nicht rechtzeitig vor Inbetriebnahme der Software umsetzen und ein mangelfreier Einsatz der Software daher nicht möglich sein, trägt der Vertragspartner hierfür allein die Verantwortung und hat keinen Anspruch auf eine Rückerstattung der Lizenzgebühren.

13.3. Sollte es trotz der o. g. Umstände erforderlich sein, eine technische Unterstützung zu bieten oder eine Schulung durchzuführen, so ist diese Hilfe kostenpflichtig. Hierfür kann der Vertragspartner beispielsweise mit dem Lizenzgeber eine vom Nutzungsvertrag gesonderte Servicevereinbarung abschließen.

14. Gewährleistung, Mängel

14.1. Der Vertragspartner hat vor Vertragsabschluss überprüft, dass der Funktionsumfang der Vertragsprodukte seinen Erwartungen und Bedürfnissen entspricht. Ihm sind die wesentlichen Funktionsmerkmale und -bedingungen bekannt. Es besteht keine Gewährleistung dafür, dass die Vertragsprodukte den speziellen Anforderungen des Vertragspartners entsprechen. Der Vertragspartner trägt die alleinige Verantwortung für Auswahl, Installation und Nutzung der Vertragsprodukte sowie für die damit erzielten Ergebnisse und den wirtschaftlichen Erfolg.

14.2. Der Vertragspartner erkennt ausdrücklich an, dass Funktionsstörungen der Vertragsprodukte auch bei größter Sorgfalt nicht ausgeschlossen werden können.

14.3. NHC ist während der Vertragslaufzeit für die Aufrechterhaltung der vertraglich vorgesehenen Funktionstüchtigkeit der Vertragsprodukte verantwortlich und behebt in diesem Zusammenhang Mängel und Funktionsstörungen, die den vertraglich vorgesehenen Gebrauch der Vertragsprodukte erheblich mindern (Sachmängel). Im Zuge der Mangelbeseitigung kann NHC Updates, Upgrades, Patches und neue Versionen (Programmaktualisierungen) zum Download oder auf einem Datenträger zur Selbstinstallation bereitstellen. Einen eigenständigen Anspruch auf entsprechende Programmaktualisierungen zum Zwecke der Mangelbeseitigung bzw. Gewährleistung und darüber hinaus hat der Vertragspartner nicht.

14.4. NHC gewährleistet, dass die Vertragsprodukte frei von Sachmängeln sind. NHC haftet nicht für Sachmängel, die auf einer fehlerhaften Anwendung der Vertragsprodukte oder darauf beruhen, dass die Voraussetzungen zum Einsatz der Vertragsprodukte nicht oder nicht vollständig durch den Vertragspartner geschaffen worden sind, Software Dritter einen Mangel aufweist, die Vertragsprodukte in einer falschen Systemumgebung eingesetzt werden oder die aus von dem Vertragspartner vorgenommenen Änderungen oder Ergänzungen der Vertragsprodukte oder der Systemumgebung sowie verbundener Software, insbesondere Software Dritter, nach Installation der Vertragsprodukte resultieren. Etwas anderes gilt nur, soweit der Vertragspartner nachweist, dass die Sachmängel bereits bei Überlassung der Vertragsprodukte vorlagen und mit vorstehend benannten Umständen in keinem ursächlichen Zusammenhang stehen oder der Vertragspartner zu den betreffenden Änderungen aus gesetzlichen Vorschriften berechtigt ist und diese fachgerecht ausgeführt hat sowie die Änderungen nachvollziehbar dokumentiert werden. Mängelansprüche bestehen auch nicht bei einer unerheblichen Abweichung von der vereinbarten Beschaffenheit oder einer unerheblichen Beeinträchtigung der Gebrauchstauglichkeit der Vertragsprodukte.

14.5. Im Rahmen der Mangelbeseitigung ist NHC berechtigt, nach seiner Wahl den Mangel durch Beseitigung des Mangels (Nachbesserung), ggf. mehrfach, oder Ersatzlieferung zu beheben oder zu umgehen. Das Recht von NHC, die gewählte Art der Nacherfüllung unter den ge-

setzlichen Voraussetzungen zu verweigern, bleibt unberührt. NHC ist im Rahmen der Mangelbeseitigung unter Beibehaltung des vertraglich vorgesehenen Funktionsumfangs berechtigt, dem Vertragspartner zur Instandsetzung Programmaktualisierungen zu überlassen, die den gerügten Mangel nicht mehr enthalten.

14.6. Der Vertragspartner ist verpflichtet, die Vertragsprodukte unverzüglich nach Bereitstellung zu untersuchen und erkannte Sachmängel schriftlich oder in Textform unter genauer Beschreibung des Fehlers zu rügen. Im Übrigen ist der Vertragspartner verpflichtet, NHC unverzüglich nach erstmaliger Kenntnis von einem Sachmangel schriftlich oder in Textform zu unterrichten und nachprüfbare Unterlagen über Art und Auftreten des behaupteten Sachmangels zur Verfügung zu stellen sowie einen sachkundigen Mitarbeiter zu benennen, der die zur Durchführung des Vertrages und zur Mangelbeseitigung erforderlichen Auskünfte erteilen und Entscheidungen treffen oder Maßnahmen veranlassen kann. Der Vertragspartner hat darüber hinaus die Pflicht, bei der Eingrenzung von Fehlern ernsthaft und nach besten Kräften mitzuwirken sowie dem Lizenzgeber ggf. Zugriff auf seine IT-Systeme zu verschaffen und dessen Anweisungen zur Fehlerbehebung zu befolgen.

14.7. Stellt sich bei Überprüfung des gemeldeten Mangels heraus, dass kein gewährleistungspflichtiger Mangel der Vertragsprodukte vorliegt, kann NHC von dem Vertragspartner Ersatz der nachweislich angefallenen Kosten der Mangelbeseitigung verlangen, insbesondere Prüf- und Transportkosten, es sei denn das Fehlen eines zur Instandsetzung verpflichtenden Mangels war für den Vertragspartner nicht erkennbar. Dies gilt insbesondere bei fehlerhafter Bedienung durch den Vertragspartner.

14.8. NHC übernimmt keine Gewähr für den Inhalt, die Aktualität und Vollständigkeit der Datenbanken wenn das Datenmaterial von Dritten (z.B. der AVOXA - Mediengruppe Deutscher Apotheker GmbH) stammt.

14.9. Ansprüche aus Sachmängeln verjähren in einem Jahr ab Überlassung der Vertragsprodukte.

15. Haftung

15.1. NHC erstellt die mittels der Vertragsprodukte generierten Rezept-Prüfdaten nach bestem Wissen und mit größtmöglicher Sorgfalt. Da jedoch die Daten zunächst in der Apotheke per Scanner erfasst werden, können Daten- und Verarbeitungsfehler, welche die Prüfergebnisse beeinflussen, nicht ausgeschlossen werden.

15.2. NHC haftet daher insbesondere nicht für Fehler in Zusammenhang mit den seitens des Vertragspartners bereitgestellten Daten, insbesondere Rezeptinhalten.

15.3. Die Parteien haften wechselseitig aus und im Zusammenhang mit diesem Vertragsverhältnis – gleich ob aus dem Vertrag oder aus dem Gesetz – nur bei grober Fahrlässigkeit oder bei Vorsatz. Für die Verletzung von Vertragspflichten, die zur Erreichung des Vertragszieles unverzichtbar sind (Kardinalpflichten) sowie für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit haften die Vertragsparteien auch im Falle leichter Fahrlässigkeit. Bei der haftungsbegründenden Verletzung vertragswesentlicher Pflichten ist die Ersatzpflicht der Höhe nach beschränkt auf die bei Vertragsschluss vorhersehbaren und vertragstypischen Schäden.

15.4. Die Haftungsausschlüsse und Beschränkungen gelten nicht, soweit NHC den Mangel arglistig verschwiegen hat, oder im Fall der Übernahme ausdrücklicher Garantien und nicht für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit sowie im Fall entgegenstehender zwingender gesetzlicher Regelungen. Die Vorschriften des Produkthaftungsgesetzes bleiben unberührt.

15.5. Mittelbare Schäden und Folgeschäden, die Folge von Mängeln des Vertragsprodukts sind, sind nur ersatzfähig, soweit solche Schäden bei bestimmungsgemäßer Verwendung des Vertragsprodukts typischerweise zu erwarten sind. Die Haftung für Datenverlust wird auf den typischen Wiederherstellungsaufwand beschränkt, der bei regelmäßiger und Gefahr entsprechender Anfertigung von Sicherungskopien eingetreten wäre. Soweit NHC technische Auskünfte gibt oder beratend tätig wird und diese Auskünfte oder Beratung nicht zu dem von dem Lizenzgeber geschuldeten, vertraglich vereinbarten Leistungsumfang gehören, geschieht dies unentgeltlich und unter Ausschluss der vertraglichen Haftung.

15.6. Die von den Vertragsprodukten vorgenommenen Auswertungen erfolgen teilweise auf Basis der von der AVOXA (einem Dritten) bereitgestellten Informationen und ABDA-Artikelstamm-Daten, deren Verwendung der Vertragspartner ausdrücklich zustimmt und für deren Richtigkeit und Vollständigkeit eine Haftung von NHC und von AVOXA ausgeschlossen ist. Fehler in den von der AVOXA zur Verfügung gestellten Datenbeständen hat der Vertragspartner der AVOXA und dem Lizenzgeber unverzüglich schriftlich oder in Textform mitzuteilen. Die Haftung ist ebenfalls für einen von AVOXA zu vertretenden Verlust von Daten des Vertragspartners ausgeschlossen, in jedem Fall aber auf den Aufwand beschränkt, der bei einer üblichen, mindestens täglichen Datensicherung zur Wiederherstellung der Daten notwendig ist.

15.7. Vorgenannte Haftungsbeschränkungen gelten in gleicher Weise zugunsten der Organe, sonstigen Vertreter, Mitarbeiter und Erfüllungsgehilfen der NHC.

16. Höhere Gewalt

16.1. Bei höherer Gewalt und unvorhergesehenen Ereignissen, die die AVOXA und NHC nicht zu vertreten haben und welche die Einschränkung oder Einstellung des Betriebes von der AVOXA und von NHC oder von deren Erfüllungsgehilfen erforderlich machen, sind die AVOXA und NHC für die Dauer der Behinderung sowie einer angemessenen Anlaufzeit von der Pflicht zur Leistung und der Vertragspartner von der Verpflichtung zur Entrichtung des vereinbarten Entgeltes befreit.

16.2. Höherer Gewalt stehen Feuer, Streik, Aussperrung, der Ausfall von fremden Telekommunikationssystemen und sonstige Umstände gleich, die die AVOXA und NHC nicht zu vertreten haben, die aber deren Leistungen wesentlich erschweren oder unmöglich machen. Höherer Gewalt steht schließlich gleich, wenn die Leistungen von der AVOXA und von NHC infolge eines sogenannten Schadprogramms in deren Systemen oder in den Systemen von deren Erfüllungsgehilfen beeinträchtigt oder unmöglich werden, gegen dessen Eindringen die AVOXA und NHC oder der betroffene Erfüllungsgehilfe sich nicht oder nicht zu angemessenen Bedingungen schützen konnten.

17. Datenschutz

17.1. Im Rahmen des Vertragsverhältnisses werden Informationen und Daten des Vertragspartners vom Lizenzgeber erhoben. Die Einzelheiten insoweit ergeben sich aus der Datenschutzerklärung: https://www.vsa.de/footer/datenschutz/

17.2. Da die Vertragsprodukte vom Vertragspartner ggf. in der Konstellation einer Auftragsdatenverarbeitung eingesetzt werden, schließen die Vertragsparteien gleichzeitig mit dem Nutzungsvertrag über ScanAdhoc (und ggf. Pharma-Control) außerdem einen Vertrag über eine Auftragsverarbeitung gemäß Art. 28 DSGVO, wie in der Anlage 1 zu diesen Nutzungsbedingungen vollständig wiedergegeben.

18. Änderung der Vertragsbedingungen

18.1. NHC kann die Vertragsbedingungen ändern. Ziff. 18 gilt nicht für die Änderung von Hauptleistungspflichten, soweit die Änderung nicht auf einer Änderung der zwingenden gesetzlichen Rahmenbedingungen beruht; für Preisanpassungen gilt Ziff. 17.

18.2. NHC informiert den Vertragspartner in Textform oder über ScanAdhoc mindestens fünf Wochen vorher über

die geplante Änderung. Darin teilt NHC dem Vertragspartner auch den Zeitpunkt mit, ab dem die geänderten Bedingungen gelten sollen.

18.3. Bei Änderungen hat der Vertragspartner ein Sonderkündigungsrecht zum Zeitpunkt des Wirksamwerdens der Änderungen. Die Kündigung seitens des Vertragspartners muss innerhalb von vier Wochen nach Zugang der Änderungsmitteilung erfolgen; andernfalls werden die Änderungen zum Zeitpunkt des Wirksamwerdens Vertragsbestandteil. Die Kündigung bedarf der Textform. NHC wird den Vertragspartner auf seine Rechte und die Folgen seines Schweigens hinweisen.

18.4. Ein Kündigungsrecht des Vertragspartners besteht nicht, wenn die Änderungen (1) ausschließlich zum Vorteil des Vertragspartners sind, (2) rein administrativer Art sind und keine negativen Auswirkungen auf den Vertragspartner haben, oder (3) unmittelbar durch Unionsrecht oder innerstaatlich geltendes Recht vorgeschrieben sind.

18.5. Erweist sich eine Änderung als ungültig, nichtig oder aus irgendeinem Grund nicht durchsetzbar, wird hierdurch die Gültigkeit und Durchsetzbarkeit der übrigen Änderungen nicht berührt.

19. Schlussbestimmungen

19.1. Änderungen und Ergänzungen dieser AGB einschließlich dieser Klausel bedürfen der Textform; Änderungen und/oder Ergänzungen dieses Vertrages können auch in elektronischer Form über das Postfach des Vertragspartners durchgeführt werden.

19.2. Diese AGB und die anlässlich des Vertragsschlusses von den Vertragsparteien abgegebenen Erklärungen enthalten alle zwischen den Parteien über den Vertragsgegenstand getroffenen Vereinbarungen. Mündliche Nebenabreden bestehen nicht. Abweichende, entgegenstehende oder ergänzende Geschäftsbedingungen des Vertragspartners werden, selbst bei Kenntnis von NHC, nicht Vertragsbestandteil.

19.3. Bei Widersprüchen zwischen den vertraglichen Regelungen eines etwaigen zwischen den Vertragsparteien gegenwärtig oder zukünftig bestehenden Abrechnungs- und Factoringvertrages (oder ähnlichen Rechtsgeschäfts) und diesen Regelungen haben die Regelungen dieses Vertrages in Bezug auf die Vertragsprodukte Vorrang.

19.4. Sollten eine oder mehrere Bestimmungen dieser Nutzungsbedingungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen hiervon unberührt. Sofern die Bestimmungen eine Regelungslücke enthalten sollten, gelten zur Ausfüllung dieser diejenigen rechtlich wirksamen Regelungen als vereinbart, welche die Parteien nach den wirtschaftlichen Zielsetzungen und dem Zweck des Vertragsverhältnisses vereinbart hätten, wenn sie die Regelungslücke gekannt hätten.

19.5. Erfüllungsort und ausschließlicher Gerichtsstand für alle sich aus dem Vertragsverhältnis unmittelbar oder mittelbar ergebenden Streitigkeiten ist München. Für sämtliche Rechtsbeziehungen gilt ausschließlich deutsches Recht unter Ausschluss internationalen Einheitsrechts, insbesondere des UN-Kaufrechts.

20. Daten des Anbieters (Lizenzgebers)

NOVENTI HealthCare GmbH
Berg-am-Laim-Str. 105, 81673 München
Telefon: +49 89 43184-0
Telefax: +49 89 43184-460
info@noventi.healthcare
www.noventi.healthcare

- Anlage 1 -

Vertrag über eine Auftragsverarbeitung gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO)
vereinbart durch Vertragsschluss der Nutzungsvereinbarung zu ScanAdhoc

zwischen dem

Lizenznehmer (Apotheke bzw. Apotheker/in)
für die Verarbeitung Verantwortlicher, nachfolgend „Auftraggeber“ genannt

und

Lizenzgeber (NOVENTI HealthCare GmbH),
Berg-am-Laim-Str. 105, 81673 München
Auftragsverarbeiter, nachfolgend „Auftragnehmer“ genannt

Präambel
Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 DSGVO zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

1. Gegenstand des Auftrags, Art und Zweck der Verarbeitung

1.1. Der Auftragnehmer stellt dem Auftraggeber die Softwarelösung ScanAdhoc zur Prüfung und Korrektur der Verordnungen bereit. Der Abgleich der Rezeptdaten erfolgt auf Systemen des Auftragnehmers. Der Auftraggeber kann hierfür erforderliche Rezeptdaten über eine Schnittstelle bereitstellen. Der Auftragnehmer führt zudem Support- und (Fern-)Wartungsarbeiten („Arbeiten“) an der Software ScanAdhoc (on-premise) des Auftraggebers durch. Die Arbeiten erfolgen entweder vor Ort, per Fernzugriff auf den Systemen des Auftraggebers oder auf den Systemen des Auftragnehmers. Im Übrigen ergibt sich der Gegenstand des Auftrags aus dem (auf Basis der Nutzungsbedingungen für ScanAdhoc und Pharma-Control abgeschlossenen bzw. abzuschließenden) Nutzungsvertrag, auf den hier verwiesen wird (im Folgenden „Hauptvertrag“).

1.2. Es kann nicht ausgeschlossen werden, dass der Auftragnehmer im Rahmen dieser Arbeiten Zugriff auf personenbezogene Daten erlangt, die in den zu wartenden Systemen gespeichert sind und dort verarbeitet werden. Diese werden nur im Auftrag und nach dokumentierter Weisung des Auftraggebers gemäß Art. 28 DSGVO (Auftragsverarbeitung) und den nachfolgenden Bestimmungen verarbeitet.

1.3. Die Verarbeitung der 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 in ein Drittland bedarf der vorherigen dokumentierten Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO) und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44-49 DSGVO erfüllt sind.

2. Dauer des Auftrages

2.1. Die Laufzeit dieser Auftragsvereinbarung („Vereinbarung“) entspricht der Laufzeit des jeweiligen Hauptvertrags zwischen Auftraggeber und Auftragnehmer.

3. Art der personenbezogenen Daten und Kategorien betroffener Personen

3.1. Im Rahmen von ScanAdhoc werden die folgenden personenbezogenen Daten verarbeitet:

- Alle erforderlichen Daten gemäß der jeweils aktuellen Version der technischen Anlage 3 und Anlage 4 zur Vereinbarung zur Datenübermittlung nach § 300 SGB V.
- Alle erforderlichen Daten gemäß der jeweils aktuellen Version der Anlage 1 der technischen Anlage für die maschinelle Abrechnung (elektronische Datenübermittlung) zu den Richtlinien der Spitzenverbände der Krankenkassen nach § 302 Abs. 2 SGB V • Ggf. weitere personenbezogene Daten gemäß den technischen Anlagen zu den §§ 300 oder 302 SGB V. • Log-In Daten von Mitarbeitern (Benutzername, Passwort)

3.2. Unabhängig von der Art der Abrechnung werden die folgenden personenbezogenen Daten verarbeitet

- Versichertenstamm: Name, Geburtsdatum, Anschrift, Versichertennummer
- Arztstamm Arzt-/Praxisname, Anschrift Arztpraxis, BSNR
- Herstellerstamm: Name, Anschrift
- Sozialversicherungs- und Gesundheitsdaten

3.3. Kreis der betroffenen Personen

- Kunden der Auftraggeber bzw. Patienten
- Ärzte, Leistungserbringer
- Beschäftigte bei Leistungserbringern, Lieferanten und Leistungsträgern

4. Verantwortlichkeit und Weisungsbefugnis

4.1. Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Etwas anderes gilt nur in dem in Absatz 4.2 genannten Umfang.

4.2. Die Verarbeitung der Daten erfolgt ausschließlich gemäß dem zwischen den Parteien geschlossenen Hauptvertrag und auf dokumentierte Weisung des Auftraggebers, es sei denn es besteht eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragnehmer unterliegt. Im Falle einer anderweitigen Verpflichtung teilt der Auftragnehmer dem Auftraggeber vor der Verarbeitung unverzüglich die entsprechenden rechtlichen Anforderungen mit.

4.3. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

4.4. Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

5. Vertraulichkeit und Verpflichtung zur Geheimhaltung

5.1. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit sowie gemäß § 35 Abs. 1 SGB I auf das Sozialgeheimnis verpflichtet worden sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

5.2. Im Rahmen der Vereinbarung werden auch Daten verarbeitet, die gemäß § 203 StGB unter ein Berufsgeheimnis fallen. Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu

verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, nach § 203 Abs. 4 S. 1 StGB strafbar machen. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

5.3. Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

5.4. Der Auftragnehmer ist nach Ziffer 7 dieser Vereinbarung berechtigt, Unterauftragnehmer zur Vertragserfüllung heranzuziehen. Im Ausland dürfen Unterauftragnehmer zur Vertragserfüllung nur dann herangezogen werden, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist. Der Auftragnehmer wird etwaige Unterauftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zum Stillschweigen verpflichten. Der Auftragnehmer wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzte Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren. Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.

6. Datensicherheit

6.1. Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

6.2. Die Vertragsparteien vereinbaren die in dem Anlage 2 „Technische und organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen.

6.3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

7. Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

7.1. Als Subunternehmer im Sinne dieser Regelung gelten vom Auftragnehmer beauftragte Auftragsverarbeiter, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post/Transportdienstleistungen und Reinigung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

7.2. Die Auslagerung auf Subunternehmer oder der Wechsel des bestehenden Subunternehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Subunternehmer dem Auftraggeber mindestens 14 Tage vor Datenübergabe vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten schriftlich oder in Textform gegenüber dem Auftragnehmer Einspruch gegen die geplante Auslagerung erhebt.

und, soweit zutreffend, die Vorgaben der Ziffer 5 dieser Vereinbarung eingehalten werden.

7.3. Mit dem Subunternehmer ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 3 und 4 DSGVO abzuschließen, die den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieser Vereinbarung entspricht. Der Auftraggeber ist berechtigt, beim Auftragnehmer Einsicht in dessen Verträge mit Subunternehmern zu nehmen.

7.4. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die durch den Auftraggeber zum Zeitpunkt des Vertragsschlusses genehmigten Subunternehmer sind in der Anlage 4 zu diesem Vertrag aufgelistet.

8. Unterstützung bei der Wahrung der Betroffenenrechte

8.1. Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO).

8.2. 8.2.Der Auftragnehmer darf personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Auskünfte an Dritte oder betroffene Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

8.3. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

9. Unterstützung bei Dokumentations- und Meldepflichten

9.1. Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO). Das Gleiche gilt, wenn beim Auftragnehmer beschäftigte Personen gegen diese Vereinbarung verstoßen.

9.2. Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen.

9.3. Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Meldepflichten gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DSGVO und ggf. gegenüber den von der Verletzung des Schutzes personenbezogener Daten Betroffenen gemäß Art. 34 DSGVO.

9.4. Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten.

10. Beendigung des Auftrags

10.1. Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

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

11. Kontrollrecht des Auftraggebers

11.1. Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistungen und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen sowie die Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zu kontrollieren. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers sowie die Einhaltung dieser Vereinbarung nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

11.2. Der Auftragnehmer ist verpflichtet, dem Auftraggeber zu den üblichen Geschäftszeiten Zutritt zu den Räumlichkeiten zu gewähren, in denen die Daten des Auftraggebers physisch oder elektronisch verarbeitet werden. Der Auftraggeber stimmt die Durchführung der Inspektionen mit dem Auftragnehmer so ab, dass der Betriebsablauf beim Auftragnehmer so wenig wie möglich beeinträchtigt wird. Vor Ort Kontrollen sind grundsätzlich vier Wochen vor der Durchführung der Kontrolle anzukündigen. Der Auftraggeber wird vor Ort Kontrollen nicht häufiger als einmal Jährlich durchführen, soweit eine Kontrolle aufgrund besonderer Umstände nicht zwingend erforderlich ist. Die Umstände sind dem Auftragnehmer darzulegen.

11.3. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der technischen und organisatorischen Maßnahmen sowie der Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zur Verfügung. Zu diesen Informationen gehören insbesondere aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, externe Sachverständige, IT-Sicherheits- oder Datenschutzauditoren) und geeignete Zertifizierung (z.B. nach BSI-Grundschutz). Der Auftragnehmer erteilt dem Auftraggeber unverzüglich konkrete Auskunft im Einzelfall.

12. Haftung

12.1. Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 und 4 DSGVO für den materiellen und immateriellen Schaden, den eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind für einen solchen Schaden sowohl der Auftraggeber als auch der Auftragnehmer verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung für den Schaden entspricht.

13. Schlussbestimmungen

13.1. Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

13.2. Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrere Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen, die der unwirksamen Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht.

13.3. Im Falle eines Widerspruchs zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

13.4. Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:

- Anlage 3 (technische und organisatorische Maßnahmen)
- Anlage 4 (Unterauftragnehmer

- Anlage 3 -

Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO

1 Maßnahmen zu Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle Soll verhindern, dass Unbefugte räumlich Zugang zu Datenverarbeitungsanlagen erhalten. Maßnahmen zur Gebäude- und Raumsicherung.	**Zutreffend (falls ja, bitte ankreuzen)**
• Schließsystem/ Schließanlage	☒
• Sorgfältige Auswahl externer Wachdienst	☒
• Alarmanlage	☒
• Verbindung Alarmanlage zu Wachdienst/ Polizei	☒
• Lichtschranken/ Bewegungsmelder	☒
• Verbindung Bewegungsmelder zu Wachdienst/ Polizei	☒
• Videoüberwachung im NOVENTI Rechenzentrum Tomannweg 6, München	☒
• Wachdienst vor Ort/ Sicherung außerhalb der Arbeitszeiten	☒
• Personenüberprüfung bei Pförtner /Empfang	☒
Berechtigungsausweise	☒
Besucherausweise	☒
Protokollierung von Besucherzutritten / Besucherbuch	☒
Begleitung von Besucherzutritten durch eigene Mitarbeiter	☒
Elektronische Zutrittscodekarten/ Zutrittstransponder	☒
Schlüsselregelung	☒
Zutrittsberechtigungskonzept	☒
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	☒
Gesicherter Eingang für An- und Ablieferungen	☒
Gesondert gesicherter Zutritt zum Serverraum	☒
Gesondert gesicherter Zutritt zum Rechenzentrum	☒
Arbeitsanweisungen /Richtlinien bzgl. des Verschließens von Räumlichkeiten bei Verlassen/Arbeitsende	☒
Sorgfältige Auswahl von Reinigungspersonal	☒

Sonstiges: --	☐

1.2 Zugangskontrolle Soll den Zugang Unbefugter zu Datenverarbeitungssystemen und deren unbefugte Nutzung verhindern. Systemabsicherung	**Zutreffend (falls ja, bitte ankreuzen)**
Zuordnung von Benutzerrechten	☒
Erstellen von Benutzerprofilen	☒
Berechtigungsmanagement	☒
Dokumentierter Prozess zu Rechtevergabe bei Neueintritt von Mitarbeitern	☒
Dokumentierter Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern	☒
Dokumentierter Prozess zum Rechteentzug bei Austritt von Mitarbeitern	☒
Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen	☒
Verwendung von individuellen Passwörtern	☒
Login mit Benutzername und Passwort	☒
Login mit biometrischen Daten	☐
Separates BIOS-Passwort	☒
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)	☒
Passwortrichtlinie mit Mindestvorgaben zur Passwortkomplexität	☒
• Mindestens 8 Zeichen	☒
• Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. 4 Kriterien)	☒
• Verhinderung von Trivialpasswörtern (z.B. Passwort1, Passwort2, 123456, qwertz)	☒
• Passworthistorie	☒
• Verhinderung von PW nach positivem Abgleich mit Wörterbüchern	☐
• Eingabebeschränkung bestimmter Sonderzeichen zur Verhinderung von SQL-Injections	☒
• Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern	☒
• Angemessen sicheres Verfahren zum Zurücksetzen von Passwörtern	☒
Sonstiges: (z.B. Nutzung von Fido2)	☐

Hashing von gespeicherten Passwörtern	☒
Hashes werden „gesalzen“ (Salt) oder „gepfeffert“ (Pepper)	☐

Verschlüsselung von Netzwerken	☒
Verschluss von Datenverarbeitungsanlagen (z.B. verschlossener Cage für Server)	☒
Sperrung von externen Schnittstellen (z.B: USB)	☐
Programmprüfungs- und Freigabeverfahren bei Neuinstallationen	☒
Verwendung von Intrusion-Prevention-Systemen	☐
Nutzung von VPN-Technologie	☒
Einsatz von Anti-Viren-Software: Server	☒
Einsatz von Anti-Viren-Software: Clients	☒
Einsatz einer Software-Firewall	☐
Einsatz einer Hardware-Firewall	☒
Mobile-Device-Management	☒
Aufbewahrung personenbezogener Daten/Datenträgern in verschließbaren Sicherheitsschränken oder in gesondert gesicherten Räumen	☒
Regelung zum Home Office / zu Telearbeit	☒
Sonstige Maßnahmen: -	☐

1.3 Zugriffskontrolle Soll unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen verhindern	**Zutreffend (falls ja, bitte ankreuzen)**
Nutzung eines Berechtigungskonzepts	☒
Minimaler Einsatz von Administratoren-Konten	☒
Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)	☒
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)	☒
Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im zutrittsgeschützten Safe	☒
Regelmäßige Überprüfung von Berechtigungen	☒
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken	☒
Regelmäßige Auswertung von Protokollen (Logfiles)	☒
Zeitliche Begrenzung von Zugriffsmöglichkeiten	☒
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)	☒
Protokollierung von Datenzugriffen	☐

Protokollierung von Datenlöschung	☐
Protokollierung von Datenveränderungen	☐
• SPAM-Filter	☒
• Intrusiondetection (IDS)	☐
• Software für das Security Information and Event Management (SIEM)	☐
Beschränkter Zugriff auf LogFiles (nur Log-Admin)	☒
Speicherung von Log-Files auf dediziertem LogFile-Server	☒
Verschlüsselte Speicherung der Daten	☒
• Verwendete Verschlüsselungsalgorithmen	☒
- AES (128/256 bit)	☒
- RSA (1024/2048 bit)	☐
- Sonstiges:	☐
• Verwendete Hash-Funktion	☒
- SHA2 (256,384, 512 bit)	☒
- SHA3	☒
- bcrypt	☐
- Andere Verfahren:	☐
- Hashes werden „gesalzen“ (Salt) oder „gepfeffert“ (Pepper)	☐
Kontrollierte Vernichtung der Daten:	
Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister	☒
Datenträgerentsorgung – sichere Löschung von Datenträgern (DIN 66399):	☒
Sonstiges Vernichtungsverfahren:	☐
Richtlinie zur Datenvernichtung	☒
Clean Desk-Policy	☒
Sonstige Maßnahmen: -	☐

1.4 Auftragskontrolle Soll sicherstellen, dass Daten, die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftraggebers verarbeitet werden.	**Zutreffend (falls ja, bitte ankreuzen)**
Vertragsgestaltung gem. gesetzlichen Vorgaben (ART. 28 DSGVO)	☒
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)	☒
Vorabkotrollen beim Auftragnehmer vor Vertragsbeginn	☒
Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer)	☒
Vor-Ort-Kontrollen beim Auftragnehmer	☒
Überprüfung des Datensicherheitskonzepts beim Auftragnehmer	☒
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer	☒
Auftragnehmer hat Datenschutzbeauftragten benannt	☒
Erteilung von Weisungen zur Verbesserung des Datenschutzes ggü. Auftragnehmer	☒
Sonstige Maßnahmen: -	☐

1.5 Trennungskontrolle Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt voneinander zu verarbeiten.	**Zutreffend (falls ja, bitte ankreuzen)**
Trennung von Kunden (Mandatenfähigkeit des verwendeten Systems?	☒
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)	☒
Datensicherungen der Auftraggeber-Daten auf separaten Datenträgern (ohne Daten anderer Kunden)	☒
Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt	☒
Trennung von Entwicklungs-, Test- und Produktivsystem	☒
Sonstige Maßnahmen: -	☐

2 Maßnahmen zu Gewährleistung der Integrität

2.1 Weitergabekontrolle Soll die Sicherheit der Daten bei elektronischer Übertragung und Datentransport und die Nachvollziehbarkeit der Weitergabe gewährleisten	**Zutreffend (falls ja, bitte ankreuzen)**
Wie werden Daten zwischen Verantwortlichem und Dritten übermittelt?	
• VPN-Verbindung	☒
• Secure File Transfer Protocol (sftp)	☒
• Citrix-Verbindung	☒
• E-Mail-Verschlüsselung	☒
• SMIME	☐
• OpenPGP	☒
• E-Mail Versand mit verschlüsselten ZIP-Dateien	☒
• Datenaustausch über https-Verbindung	☒
• Verwendetes Verschlüsselungsprotokoll:	
- TLS 1.3	☒
Sonstige Versendungsart: Gem. SGB V	☒
• Verwendete Verschlüsselungsalgorithmen	
- AES (128/256 bit)	☒
- RSA (1024/2048 bit)	☐
- Diffie-Hellmann	☐
- Sonstiges:	☐
Nutzung von Signaturverfahren	☐
Verwendetes Signaturverfahren	
- RSA	☐
- EIGAMAL	☐
- DSA	☐
- Sonstige: PGP, eigene	☒
Digitales Signieren von Makros	☐

Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle	☐
Verschlüsselung vertraulicher Datensätze	☒
Verschlüsselung mobiler Datenträger (z.B. Laptop-Festplatten, externe Festplatten, USB-Sticks)	☒
Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken sowie Mobiltelefonen in Sicherheits-bereiche	☐
Regelung zu Anfertigung von Datensatz-Kopien	☐
Erstellen von Sicherheitskopien von Datenträgern, die transportiert werden müssen	☐
Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege	☒
Direktabholung, Kurierdienst, Transportbegleitung	☒
Vollständigkeits- und Richtigkeitsprüfung	☒
Sonstiges: --	☐

2.2 Eingabekontrolle Soll gewährleisten, dass nachvollzogen werden kann, ob, wer, wann personenbezogene Daten in Datenverarbeitungssysteme eingeben, geändert oder gelöscht hat	**Zutreffend (falls ja, bitte ankreuzen)**
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒
Manuelle oder automatisierte Auswertung der Protokoll	☒
Differenzierte Benutzerberechtigungen:	☒
• Einzelne Benutzernamen, keine Benutzergruppen	☒
• Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	☒
• Feldzugriff bei Datenbanken	☒
Organisatorische Festlegung von Eingabezuständigkeiten	☒
Verpflichtung auf das Datengeheimnis	☒
Dezidierter Logserver	☒
Regelung der Zugriffsberechtigungen für Logserver (LogAdmin)	☒
Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke	☒
Sonstige Maßnahmen: -	☐

3 Maßnahmen zur Gewährleistung der Verfügbarkeit & Belastbarkeit

3.1 Verfügbarkeitskontrolle Soll Daten gegen zufällige Zerstörung oder Verlust schützen.	**Zutreffend (falls ja, bitte ankreuzen)**
Brandmeldeanlagen in Serverräumen	☒
Rauchmelder in Serverräumen	☒
Brandschutztüren an papierverarbeitenden Standorten und im Rechenzentrum	☒
Wasserlose Brandbekämpfungssysteme in Serverräumen	☒
Wassersensoren in Serverräumen - Wasserableitung	☒
Blitz-/ Überspannungsschutz	☒
Klimatisierte Serverräume	☒
Serverräumlichkeiten in separaten Brandabschnitt	☒
Unterbringung von Backupsystemen in separaten Räumlichkeiten und in separatem Brandabschnitt	☒
Serverräume nicht unter oder neben sanitären Anlagen	☒
Zutrittsbegrenzung bei Serverräumen auf notwendiges Personal	☒
Alarmmeldung bei unberechtigtem Zutritt zu Serverräumen	☒
Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)	☒
CO2-Feuerlöscher in unmittelbarer Nähe der Serverräume	☒
USV-Anlage (Unterbrechungsfreie Stromversorgung)	☒
Stromgenerator	☒
Datenschutztresor	☒
Dokumentiertes Datensicherungs- und Backupkonzept	☒
Durchführung von Datensicherungen und Erstellen von Backups	☒
Regelmäßige Tests zur Datenwiederherstellung	☒
Spiegeln der Festplatten (z.B. RAID)	☒
Getrennte Partitionen für Betriebssystem und Daten	☐
Havariearchiv (Auslagerung von Daten)	☐
Notfallplan vorhanden (BSI-Standard 100-4)	☒
Gewährleistung der langfristigen technischen Lesbarkeit von Backupspeichermedien	☒
Sonstige Maßnahmen: --	☐

3.2 Belastbarkeit (Widerstandsfähigkeit und Ausfallkontrolle) Soll Systeme befähigen, mit risikobedingten Veränderungen umgehen zu können und Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufzuweisen.	**Zutreffend** **(falls ja, bitte ankreuzen)**
Redundante Stromversorgung	☒
Redundante Datenanbindung	☒
Redundante Klimatisierung	☒
Ausweich-Rechenzentren vorhanden (Hot- bzw. Cold-Stand-by?): Hot	☒
sonstige redundante Systeme/Verfahren:	☐
Einsatz einer hochverfügbaren SAN-Lösung (Storage Area Network)	☒
Computer Emergency Response Team (CERT)	☐
Einsatz von Lastenverteilung (Load Balancing)	☒
Abgrenzung kritischer Komponenten	☒
Durchführung von Penetrationstests	☒
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)	☒
Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	☒
Regelmäßige Sensibilisierung der Mitarbeiter (mind. jährlich)	☒
Prozess zur unverzüglichen Meldung von Vorkommnissen an die IT ist allen Mitarbeitern bekannt	☒
Abschluss einer Cyber-Versicherung	☒
Sonstige Maßnahmen: --	☐

4 Cloudlösungen bei Partnerunternehmen

Unsere Partner sind sorgfältig ausgewählt und verfügen über entsprechende Zertifizierungen.

5 Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Kontrollverfahren Soll die Wirksamkeit der Datensicherheitsmaßnahmen gewährleisten.	**Zutreffend (falls ja, bitte ankreuzen)**
Verarbeitungsverzeichnisse (Art. 30 I und II DSGVO) werden jährlich aktualisiert	☒
Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten	☒
Meldung neuer/veränderter Datenverarbeitsungsverfahren an den IT-Sciherheitsbeauftragten	☒
Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert	☒
Prüfung der Wirksamkeit getroffener Sciherheitsmaßnahmen mind. jährlich	☒
Bei negativen Feststellungen im Rahmen der zuvor gen. Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst	☒
Prozess zur Reaktion auf Sicherheitsverletzungen (Angriffe) und Systemstörungen existiert (Incident-Response-Management)	☒
Dokumentation von Sicherheitsvorfällen	☒
Einsatz Security Intelligence	☒
Sicherheitszertifizierungen (ISO 27001, BSI IT-Grundschutz etc.)	☒
Sonstige Maßnahmen: --	☐

5.2 Sonstiges Datenschutzmanagement	**Zutreffend (falls ja, bitte ankreuzen)**
Einsatz einer Datenschutzmanagement-Software	☐
Datenschutzbeauftragter benannt	☒
IT-Sicherheitsbeauftragter benannt	☒
Dokumentierter Prozess zum Umgang mit Datenschutzvorfällen	☒
Klare Verantwortlichkeiten bei der Handhabung von Datenschutz- und Sicherheitsvorfällen	☒
Dokumentierter Prozess zur Sicherstellung von Betroffenenrechten	☒
Zentrale, für alle Mitarbeiter zugängliche Ablage von Richtlinien/Verfahrensanweisungen	☒
Sonstige Maßnahmen: --	☐

Anlage 4

Unterauftragnehmer

Im Zusammenhang mit der Erbringung der vertraglichen Leistungen beauftragt der Auftragnehmer folgende Subunternehmer:

Unterauftragnehmer	**Aufgabenfeld**
NOVENTI HEALTH SE Berg-am-Laim 105 81673 München	IT Services, techn. Support
Privat Code Sp. z o.o. Plac Lasoty 3/1 30-539 Kraków	Programm- und Schnittstellenentwicklung
pace-IT GmbH Kimplerstr. 294 47807 Krefeld	Managed Cloud Service
Microsoft Deutschland GmbH Walter-Gropius-Straße 5 80807 München	Kundensupport
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen	Kundensupport