

ScanAdhoc Nutzungsbedingungen

Allgemeine Geschäftsbedingungen (Nutzungsbedingungen) für ScanAdhoc und Pharma-Control

1. Gegenstand (Allgemeines, Geltungsbereich)
 - 1.1. Die NOVENTI HealthCare GmbH, Tomannweg 6, 81673 München (im Folgenden „Lizenzgeber“), 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 „Lizenznehmer“) durch den Lizenzgeber 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 Lizenznehmer (in Form eines Institutionskennzeichens, IK) und dem Lizenzgeber zustande kommen („B2B-Fall“).
 - 1.4. Von diesen AGB abweichende oder sie ergänzende Bedingungen des Lizenznehmers werden vom Lizenzgeber nicht anerkannt, auch wenn der Lizenzgeber nicht widerspricht oder der Lizenznehmer 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 Lizenznehmers und der anschließenden Annahmeerklärung des Lizenzgebers zustande.
 - 2.2. Bei der (Online-) Registrierung gibt der Lizenznehmer zunächst seine zur Vertragsdurchführung erforderlichen Daten an. Änderungen dieser Daten teilt der Lizenznehmer dem Lizenzgeber während des mit Vertragsschluss (siehe nachstehende Regelungen) eingegangenen Vertragsverhältnisses unverzüglich mit.
 - 2.3. Mit seiner vorzugsweise im Internet (z.B. <https://www.vsa.de/formulare/scanadhoc-bestellung>) abgegebenen Bestellung (Erklärung) gibt der Lizenznehmer einen Antrag an den Lizenzgeber 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 des Lizenzgebers, wonach dieser seine Zustimmung zum o. g. Antrag des Lizenznehmers erklärt. Dies erfolgt spätestens mit der Zurverfügungstellung der Vertragsprodukte. Erst durch besagte Annahmeerklärung des Lizenzgebers kommt ein Vertrag zwischen Lizenznehmer und Lizenzgeber auf Basis dieser AGB zustande.
 - 2.4. Nach erfolgtem Vertragsschluss werden die ggf. bereits installierten Vertragsprodukte, je nach getroffener Auswahl, für den Lizenznehmer freigeschaltet. Erforderlichenfalls erhält der Lizenznehmer 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 der Lizenzgeber 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 Lizenznehmers 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 des Lizenzgebers (vgl. oben unter Ziff. 2. Vertragsschluss) und wird für eine feste Laufzeit von 24 Monaten, gerechnet ab dem Monatsersten des auf den Vertragsschluss folgenden Monats, eingegangen. Er verlängert sich darüber hinaus jeweils automatisch um 12 Monate, sofern er nicht von einer der Vertragsparteien mit einer Frist von einem Monat schriftlich oder in Textform gekündigt wird.
- 5.2. Der Lizenzgeber hat die Software ScanAdhoc und Pharma-Control (Vertragsprodukte) seinerseits lizenziert. Für den Fall, dass die Lizenz des Lizenzgebers (Hauptlizenz) endet, steht diesem gegenüber dem Lizenznehmer ein Sonderkündigungsrecht mit einer Frist von 3 Monaten zum jeweiligen Beendigungszeitpunkt der (Haupt-) Lizenz zu. Die Nutzungsgebühren werden in diesem Fall zeitanteilig erhoben.
- 5.3. Dem Lizenzgeber steht ein außerordentliches Kündigungsrecht zu, wenn sich der Lizenznehmer mit mindestens zwei Monatsgebühren in Verzug befindet.
- 5.4. Nach Beendigung des Vertrages ist die Nutzung der Software und insbesondere die Online-Prüfung nicht mehr möglich. Der Lizenznehmer hat damit keinen Zugriff mehr zu auf die erfassten und geprüften Rezeptdaten.

6. Nutzungsrecht

- 6.1. Der Lizenzgeber räumt dem Lizenznehmer 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 Lizenznehmer, bezogen auf das jeweilige IK (Institutionskennzeichen), ein.
- 6.2. Sofern nicht anderweitig schriftlich vereinbart, ist der Lizenznehmer 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 Lizenznehmer 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 Lizenznehmer hat dem Lizenzgeber auf Verlangen des Lizenzgebers zu ermöglichen, den ordnungsgemäßen Einsatz der Vertragsprodukte zu überprüfen. Der Lizenznehmer 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 Lizenznehmer unbeschadet der vertraglich eingeräumten Nutzungsrechte ausschließlich dem Lizenzgeber zu. Urhebervermerke, Seriennummern oder andere der Identifikation dienende Merkmale dürfen vom Lizenznehmer 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 Lizenznehmer keine Rechte an dem Datenmaterial. Der Lizenznehmer 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 Lizenznehmer darf die AVOXA-Datenbanken ohne entsprechende Lizenzierung nicht online, insbesondere nicht im Internet, verfügbar machen. Der Lizenznehmer 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 Lizenznehmer ist verpflichtet, einen unbefugten Zugriff auf das Datenmaterial sowie die unbefugte Nutzung oder Kenntnisnahme des Datenmaterials durch Dritte auszuschließen. Der Lizenznehmer darf das AVOXA-Datenmaterial nicht verändern oder verändertes Datenmaterial verwenden.

8. Weitere Rechte und Pflichten des Lizenznehmers

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

- 8.2. Der Lizenznehmer 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 Lizenznehmers 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 Lizenznehmers (z.B. unbefugter Zugriff nicht autorisierter Mitarbeiter des Lizenznehmers auf die Datenbank) liegt außerhalb der Verantwortung des Lizenzgebers.
 - 8.4. Der Lizenznehmer wird darauf hingewiesen, dass der Lizenzgeber nach entsprechender Information durch den Lizenznehmer durch Vergabe eines neuen Passwortes einen weiteren unbefugten Zugriff verhindern kann. Die Kosten für eine solche Passwort-Änderung trägt der Lizenznehmer. Der Lizenzgeber darf diese Kosten dem Lizenznehmer mit der nächstfolgenden Abrechnung belasten.
 - 8.5. Dem Lizenznehmer 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 Lizenznehmer, 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.
9. Prüfungsobliegenheiten und Mitwirkung des Lizenznehmers
- 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 Lizenznehmer unverzüglich per E-Mail an info@vsa.de unter Angabe einer möglichst genauen Fehlerbeschreibung zu melden.
 - 9.2. Der Lizenznehmer verpflichtet sich, durch geeignete Maßnahmen den unbefugten Zugriff Dritter auf die Software ScanAdhoc sowie die Daten zu verhindern. Die Mitarbeiter des Lizenznehmers sind auf die Einhaltung der vorliegenden Vertragsbedingungen sowie der Bestimmungen der DSGVO und des UrhG hinzuweisen.
 - 9.3. Es obliegt dem Lizenznehmer, sich in regelmäßigen Abständen durch Datensicherung gegen Datenverlust zu schützen.
10. Gebühren
- 10.1. Die Gebühren für die Nutzung der Vertragsprodukte ergeben sich aus den beim Bestellvorgang im Internet im Einzelnen genannten bzw. angezeigten Informationen. Sämtliche angegebenen und vereinbarten Preise sind in Euro und verstehen sich netto zuzüglich Umsatzsteuer in der jeweiligen gesetzlichen Höhe.
 - 10.2. Die zu zahlenden Gebühren werden mit Leistungserbringung des Lizenzgebers, und bei fortdauernder Leistungserbringung mit ihrer erstmaligen Zurverfügungstellung (beispielsweise der Überlassung der Software ScanAdhoc), sofort fällig. Sofern eine monatliche Gebühr vereinbart ist, wird diese monatlich im Voraus ab dem auf den Vertragsschluss folgenden Monat fällig.
 - 10.3. Der Lizenznehmer ist, sofern er nicht Abrechnungskunde des Lizenzgebers auf Basis eines gesonderten Abrechnungsvertrages ist, verpflichtet, am SEPA-Lastschriftverfahren teilzunehmen, um die vereinbarten monatlichen Gebühren 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 der Lizenzgeber den Lizenznehmer 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 der Lizenzgeber berechtigt, die Gebühren für die Nutzung der Vertragsprodukte im Rahmen dieses Factoringvertrages bzw. vergleichbaren Rechtsgeschäfts/Vertrags zu berechnen/verrechnen. Gleiches gilt für die jeweils gültige gesetzliche Umsatzsteuer, die auf die Gebühr erhoben wird.
 - 10.5. Nutzt der Lizenznehmer die Vertragsprodukte über den vereinbarten Umfang hinaus, so hat der Lizenzgeber Anspruch auf eine gesonderte Vergütung, die auf der Grundlage der tatsächlichen Nutzung und der aktuellen Preisgestaltung des Lizenzgebers berechnet und bestimmt wird.
 - 10.6. In allen Fällen, in denen der Lizenznehmer mit Zahlungen im Zusammenhang Ansprüchen aus diesem Vertrag in Verzug gerät und dem Lizenznehmer erfolglos eine Nachfrist gesetzt wurde, ist der Lizenzgeber berechtigt, seine Leistungen einzustellen, ohne dass es einer weiteren Fristsetzung bedarf.
 - 10.7. Eine Aufrechnung oder die Geltendmachung eines Zurückbehaltungsrechtes wegen seitens des Lizenzgebers nicht anerkannter oder nicht rechtskräftig festgestellter Gegenansprüche ist ausgeschlossen.

- 10.8. 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 Lizenznehmer selbst verantwortlich. Die Kosten für die Nutzung des Internets, die bei der Nutzung der Vertragsprodukte entstehen, trägt der Lizenznehmer ebenfalls selbst.
11. Updates
- 11.1. Updates der Vertragsprodukte werden dem Lizenznehmer 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 Lizenznehmer selbstständig erfolgen muss.
12. Installationsunterstützung und Beratung
- 12.1. 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 Lizenznehmer bekannt sind. Etwaig erforderliche Installationsunterstützung kann der Lizenznehmer gegenüber dem Lizenzgeber gegen zusätzliches Entgelt auf Anfrage in Anspruch nehmen.
- 12.2. Sollte der Lizenznehmer die o. g. Anforderungen nicht rechtzeitig vor Inbetriebnahme der Software umsetzen und ein mangelfreier Einsatz der Software daher nicht möglich sein, trägt der Lizenznehmer hierfür allein die Verantwortung und hat keinen Anspruch auf eine Rückerstattung der Lizenzgebühren.
- 12.3. 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 Lizenznehmer beispielsweise mit dem Lizenzgeber eine vom Nutzungsvertrag gesonderte Servicevereinbarung abschließen.
13. Gewährleistung, Mängel
- 13.1. Der Lizenznehmer 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 Lizenznehmers entsprechen. Der Lizenznehmer trägt die alleinige Verantwortung für Auswahl, Installation und Nutzung der Vertragsprodukte sowie für die damit erzielten Ergebnisse und den wirtschaftlichen Erfolg.
- 13.2. Der Lizenznehmer erkennt ausdrücklich an, dass Funktionsstörungen der Vertragsprodukte auch bei größter Sorgfalt nicht ausgeschlossen werden können.
- 13.3. Der Lizenzgeber 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 der Lizenzgeber 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 Lizenznehmer nicht.
- 13.4. Der Lizenzgeber gewährleistet, dass die Vertragsprodukte frei von Sachmängeln sind. Der Lizenzgeber 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 Lizenznehmer geschaffen worden sind, Software Dritter einen Mangel aufweist, die Vertragsprodukte in einer falschen Systemumgebung eingesetzt werden oder die aus von dem Lizenznehmer 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 Lizenznehmer nachweist, dass die Sachmängel bereits bei Überlassung der Vertragsprodukte vorlagen und mit vorstehend benannten Umständen in keinem ursächlichen Zusammenhang stehen oder der Lizenznehmer 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.
- 13.5. Im Rahmen der Mangelbeseitigung ist der Lizenzgeber berechtigt, nach seiner Wahl den Mangel durch Beseitigung des Mangels (Nachbesserung), ggf. mehrfach, oder Ersatzlieferung zu beheben oder zu umgehen. Das Recht des Lizenzgebers, die gewählte Art der Nacherfüllung unter den gesetzlichen Voraussetzungen zu verweigern, bleibt unberührt. Der Lizenzgeber ist im Rahmen der Mangelbeseitigung unter Beibehaltung des vertraglich vorgesehenen Funktionsumfangs berechtigt, dem Lizenznehmer zur Instandsetzung Programmaktualisierungen zu überlassen, die den gerügten Mangel nicht mehr enthalten.
- 13.6. Der Lizenznehmer 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 Lizenznehmer verpflichtet, den Lizenzgeber 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 Ver-

trages und zur Mangelbeseitigung erforderlichen Auskünfte erteilen und Entscheidungen treffen oder Maßnahmen veranlassen kann. Der Lizenznehmer 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.

- 13.7. Stellt sich bei Überprüfung des gemeldeten Mangels heraus, dass kein gewährleistungspflichtiger Mangel der Vertragsprodukte vorliegt, kann der Lizenzgeber von dem Lizenznehmer 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 Lizenznehmer nicht erkennbar. Dies gilt insbesondere bei fehlerhafter Bedienung durch den Lizenznehmer.
 - 13.8. Der Lizenzgeber 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.
 - 13.9. Ansprüche aus Sachmängeln verjähren in einem Jahr ab Überlassung der Vertragsprodukte.
- #### 14. Haftung
- 14.1. Der Lizenzgeber 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.
 - 14.2. Der Lizenzgeber haftet daher insbesondere nicht für Fehler in Zusammenhang mit den seitens des Lizenznehmers bereitgestellten Daten, insbesondere Rezeptinhalten.
 - 14.3. 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.
 - 14.4. Die Haftungsausschlüsse und Beschränkungen gelten nicht, soweit der Lizenzgeber 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.
 - 14.5. 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 der Lizenzgeber 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.
 - 14.6. 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 Lizenznehmer ausdrücklich zustimmt und für deren Richtigkeit und Vollständigkeit eine Haftung des Lizenzgebers und von AVOXA ausgeschlossen ist. Fehler in den von der AVOXA zur Verfügung gestellten Datenbeständen hat der Lizenznehmer 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 Lizenznehmers ausgeschlossen, in jedem Fall aber auf den Aufwand beschränkt, der bei einer üblichen, mindestens täglichen Datensicherung zur Wiederherstellung der Daten notwendig ist.
 - 14.7. Vorgenannte Haftungsbeschränkungen gelten in gleicher Weise zugunsten der Organe, sonstigen Vertreter, Mitarbeiter und Erfüllungsgehilfen des Lizenzgebers.
- #### 15. Höhere Gewalt
- 15.1. Bei höherer Gewalt und unvorhergesehenen Ereignissen, die die AVOXA und der Lizenzgeber nicht zu vertreten haben und welche die Einschränkung oder Einstellung des Betriebes von der AVOXA und des Lizenzgebers oder von deren Erfüllungsgehilfen erforderlich machen, sind die AVOXA und der Lizenzgeber für die Dauer der Behinderung sowie einer angemessenen Anlaufzeit von der Pflicht zur Leistung und der Lizenznehmer von der Verpflichtung zur Entrichtung des vereinbarten Entgeltes befreit.
 - 15.2. Höherer Gewalt stehen Feuer, Streik, Aussperrung, der Ausfall von fremden Telekommunikationssystemen und sonstige Umstände gleich, die die AVOXA und der Lizenzgeber 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 des Lizenzgebers infolge eines sogenannten Schadprogramms in deren Systemen oder in den Systemen von deren Erfüllungsgehilfen beeinträchtigt oder unmöglich werden, gegen dessen Eindringen die AVOXA und der Lizenzgeber oder der betroffene Erfüllungsgehilfe sich nicht oder nicht zu angemessenen Bedingungen schützen konnten.
- #### 16. Datenschutz
- 16.1. Im Rahmen des Vertragsverhältnisses werden Informationen und Daten des Lizenznehmers vom Lizenzgeber erhoben. Die Einzelheiten insoweit ergeben sich aus der Datenschutzerklärung: <https://www.vsa.de/footer/datenschutz/>

16.2. Da die Vertragsprodukte vom Lizenznehmer 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.

17. Änderung der AGB

17.1. Der Lizenzgeber ist berechtigt, die für die Nutzung der Vertragssoftware zu erhebenden Entgelte angemessen anzupassen, wenn sich der Aufwand des Lizenzgebers für IT-Betrieb, Service-Hotline oder Programmieraufwand ändert oder wesentliche neue Funktionen ergänzt werden. Die Preisänderung muss mindestens vier Wochen im Voraus in Textform angekündigt werden und wird erst ab dem auf die Mitteilung folgenden Monat wirksam.

17.2. Der Lizenzgeber kann die vorliegenden Nutzungsbedingungen einschließlich ihrer etwaigen Anlagen inhaltlich ändern und auch das Vertragsverhältnis insgesamt auf einen Dritten übertragen. Jegliche derartigen Änderungen der Nutzungsbedingungen werden dem Lizenznehmer mindestens vier Wochen vor ihrem Inkrafttreten (Stichtag) in Textform mitgeteilt. Der Verweis auf die Internetadresse, unter der die aktualisierte Fassung abrufbar ist, ist dabei ausreichend. Wird der Änderung von Seiten des Lizenznehmers nicht binnen zwei Wochen ab dem Zugang der Mitteilung schriftlich oder in Textform widersprochen, gilt sie als akzeptiert. Im Falle eines rechtzeitigen Widerspruchs endet das Vertragsverhältnis zum Stichtag. Der Lizenzgeber wird den Lizenznehmer bei Mitteilung der Änderung über sein o. g. Widerspruchsrecht belehren und ihn auf die Folgen einer Erhebung und Nichterhebung des Widerspruchs hinweisen.

18. Schlussbestimmungen

18.1. Änderungen und Ergänzungen dieser AGB einschließlich dieser Klausel bedürfen mit Ausnahme von Änderungen gemäß o.g. Regelung unter Ziff. 17. (Änderung der AGB) der Schriftform.

18.2. 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 Lizenznehmers werden, selbst bei Kenntnis des Lizenzgebers, nicht Vertragsbestandteil.

18.3. 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.

18.4. 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.

18.5. 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.

19. Daten des Anbieters (Lizenzgebers)

NOVENTI HealthCare GmbH
Tomannweg 6, 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),
Tomannweg 6, 81673 München

Auftragsverarbeiter, nachfolgend „Auftragnehmer“ genannt

Präambel

Um die Rechte und Pflichten aus dem Auftragsverhältnis 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

- 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 gewordenen 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 gewordenen 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 eine angemessene Zeit 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 3 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. 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 mehrerer 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	<input checked="" type="checkbox"/>
• Sorgfältige Auswahl externer Wachdienst	<input checked="" type="checkbox"/>
• Alarmanlage	<input checked="" type="checkbox"/>
• Verbindung Alarmanlage zu Wachdienst/ Polizei	<input checked="" type="checkbox"/>
• Lichtschranken/ Bewegungsmelder	<input checked="" type="checkbox"/>
• Verbindung Bewegungsmelder zu Wachdienst/ Polizei	<input checked="" type="checkbox"/>
• Videoüberwachung im NOVENTI Rechenzentrum Tomannweg 6, München	<input checked="" type="checkbox"/>
• Wachdienst vor Ort/ Sicherung außerhalb der Arbeitszeiten	<input checked="" type="checkbox"/>
• Personenüberprüfung bei Pfortner /Empfang	<input checked="" type="checkbox"/>
Berechtigungsausweise	<input checked="" type="checkbox"/>
Besucherausweise	<input checked="" type="checkbox"/>
Protokollierung von Besucherzutritten / Besucherbuch	<input checked="" type="checkbox"/>
Begleitung von Besucherzutritten durch eigene Mitarbeiter	<input checked="" type="checkbox"/>
Elektronische Zutrittscodekarten/ Zutrittstransponder	<input checked="" type="checkbox"/>
Schlüsselregelung	<input checked="" type="checkbox"/>
Zutrittsberechtigungskonzept	<input checked="" type="checkbox"/>
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	<input checked="" type="checkbox"/>
Gesicherter Eingang für An- und Ablieferungen	<input checked="" type="checkbox"/>
Gesondert gesicherter Zutritt zum Serverraum	<input checked="" type="checkbox"/>
Gesondert gesicherter Zutritt zum Rechenzentrum	<input checked="" type="checkbox"/>
Arbeitsanweisungen /Richtlinien bzgl. des Verschließens von Räumlichkeiten bei Verlassen/Arbeitsende	<input checked="" type="checkbox"/>
Sorgfältige Auswahl von Reinigungspersonal	<input checked="" type="checkbox"/>
Sonstiges: --	<input type="checkbox"/>

1.2 Zugangskontrolle Soll den Zugang Unbefugter zu Datenverarbeitungssystemen und deren unbefugte Nutzung verhindern. Systemabsicherung	Zutreffend (falls ja, bitte ankreuzen)
Zuordnung von Benutzerrechten	<input checked="" type="checkbox"/>
Erstellen von Benutzerprofilen	<input checked="" type="checkbox"/>
Berechtigungsmanagement	<input checked="" type="checkbox"/>
Dokumentierter Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern	<input checked="" type="checkbox"/>
Dokumentierter Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern	<input checked="" type="checkbox"/>
Dokumentierter Prozess zum Rechteentzug bei Austritt von Mitarbeitern	<input checked="" type="checkbox"/>
Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen	<input checked="" type="checkbox"/>
Verwendung von individuellen Passwörtern	<input checked="" type="checkbox"/>
Login mit Benutzername und Passwort	<input checked="" type="checkbox"/>
Login mit biometrischen Daten	<input type="checkbox"/>
Separates BIOS-Passwort	<input checked="" type="checkbox"/>
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)	<input checked="" type="checkbox"/>
Passwortrichtlinie mit Mindestvorgaben zur Passwortkomplexität:	<input checked="" type="checkbox"/>
• Mindestens 8 Zeichen	<input checked="" type="checkbox"/>
• Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. 4 Kriterien)	<input checked="" type="checkbox"/>
• Verhinderung von Trivialpasswörtern (z.B. Passwort1, Passwort2, 123456, qwertz)	<input checked="" type="checkbox"/>
• Passworthistorie	<input checked="" type="checkbox"/>
• Verhinderung von PW nach positivem Abgleich mit Wörterbüchern	<input type="checkbox"/>
• Eingabebeschränkung bestimmter Sonderzeichen zur Verhinderung von SQL-Injections	<input checked="" type="checkbox"/>
• Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern	<input checked="" type="checkbox"/>
• Angemessen sicheres Verfahren zum Zurücksetzen von Passwörtern	<input checked="" type="checkbox"/>
Sonstiges: (z.B. Nutzung von Fido2)	<input type="checkbox"/>
Hashing von gespeicherten Passwörtern	<input checked="" type="checkbox"/>
Hashes werden „gesalzen“ (Salt) oder „gepfeffert“ (Pepper)	<input type="checkbox"/>
Verschlüsselung von Netzwerken	<input checked="" type="checkbox"/>
Verschluss von Datenverarbeitungsanlagen (z.B. verschlossener Cage für Server)	<input checked="" type="checkbox"/>
Sperrung von externen Schnittstellen (z.B. USB)	<input type="checkbox"/>
Programmprüfungs- und Freigabeverfahren bei Neuinstallationen	<input checked="" type="checkbox"/>
Verwendung von Intrusion-Prevention-Systemen	<input type="checkbox"/>
Nutzung von VPN-Technologie	<input checked="" type="checkbox"/>
Einsatz von Anti-Viren-Software: Server	<input checked="" type="checkbox"/>
Einsatz von Anti-Viren-Software: Clients	<input checked="" type="checkbox"/>

Einsatz einer Software-Firewall	<input type="checkbox"/>
Einsatz einer Hardware-Firewall	<input checked="" type="checkbox"/>
Mobile-Device-Management	<input checked="" type="checkbox"/>
Aufbewahrung personenbezogener Daten/Datenträgern in verschließbaren Sicherheitsschränken oder in gesondert gesicherten Räumen	<input checked="" type="checkbox"/>
Regelung zum Home Office / zu Telearbeit	<input checked="" type="checkbox"/>
Sonstige Maßnahmen: --	<input type="checkbox"/>

1.3 Zugriffskontrolle Soll unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen verhindern.	Zutreffend (falls ja, bitte ankreuzen)
Nutzung eines Berechtigungskonzepts	<input checked="" type="checkbox"/>
Minimaler Einsatz von Administratoren-Konten	<input checked="" type="checkbox"/>
Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)	<input checked="" type="checkbox"/>
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)	<input checked="" type="checkbox"/>
Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im zutrittsgeschützten Safe	<input checked="" type="checkbox"/>
Regelmäßige Überprüfung von Berechtigungen	<input checked="" type="checkbox"/>
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken	<input checked="" type="checkbox"/>
Regelmäßige Auswertung von Protokollen (Logfiles)	<input checked="" type="checkbox"/>
Zeitliche Begrenzung von Zugriffsmöglichkeiten	<input checked="" type="checkbox"/>
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)	<input checked="" type="checkbox"/>
Protokollierung von Dateizugriffen	<input type="checkbox"/>
Protokollierung von Dateilöschungen	<input type="checkbox"/>
Protokollierung von Dateiveränderungen	<input type="checkbox"/>
• SPAM-Filter	<input checked="" type="checkbox"/>
• Intrusiondetection (IDS)	<input type="checkbox"/>
• Software für das Security Information and Event Management (SIEM)	<input type="checkbox"/>
Beschränkter Zugriff auf LogFiles (nur Log-Admin)	<input checked="" type="checkbox"/>
Speicherung von Log-Files auf dediziertem LogFile-Server	<input checked="" type="checkbox"/>
Verschlüsselte Speicherung der Daten	<input checked="" type="checkbox"/>
• verwendete Verschlüsselungsalgorithmen:	<input checked="" type="checkbox"/>
- AES (128/256 bit)	<input checked="" type="checkbox"/>
- RSA (1024/2048 bit)	<input type="checkbox"/>
- Sonstiges:	<input type="checkbox"/>
• Verwendete Hash-Funktion:	<input checked="" type="checkbox"/>
- SHA2 (256, 384, 512 bit)	<input checked="" type="checkbox"/>
- SHA3	<input checked="" type="checkbox"/>
- bcrypt	<input type="checkbox"/>
- Andere Verfahren:	<input type="checkbox"/>
- Hashes werden „gesalzen“ (Salt) oder „gepfeffert“ (Pepper)	<input type="checkbox"/>
Kontrollierte Vernichtung von Daten:	

Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister	<input checked="" type="checkbox"/>
Datenträgerentsorgung - Sichere Löschung von Datenträgern (DIN 66399):	<input checked="" type="checkbox"/>
Sonstiges Vernichtungsverfahren:	<input type="checkbox"/>
Richtlinie zur Datenvernichtung	<input checked="" type="checkbox"/>
Clean Desk-Policy	<input checked="" type="checkbox"/>
Sonstige Maßnahmen: --	<input type="checkbox"/>

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)	<input checked="" type="checkbox"/>
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)	<input checked="" type="checkbox"/>
Vorabkontrollen beim Auftragnehmer vor Vertragsbeginn	<input checked="" type="checkbox"/>
Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer)	<input checked="" type="checkbox"/>
Vor-Ort-Kontrollen beim Auftragnehmer	<input checked="" type="checkbox"/>
Überprüfung des Datensicherheitskonzepts beim Auftragnehmer	<input checked="" type="checkbox"/>
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer	<input checked="" type="checkbox"/>
Auftragnehmer hat Datenschutzbeauftragten benannt	<input checked="" type="checkbox"/>
Erteilung von Weisungen zur Verbesserung des Datenschutzes ggü. Auftragnehmer	<input checked="" type="checkbox"/>
Sonstige Maßnahmen: --	<input type="checkbox"/>

1.5 Trennungskontrolle Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt voneinander zu verarbeiten.	Zutreffend (falls ja, bitte ankreuzen)
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)	<input checked="" type="checkbox"/>
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)	<input checked="" type="checkbox"/>
Datensicherungen der Auftraggeber-Daten auf separaten Datenträgern (ohne Daten anderer Kunden)	<input checked="" type="checkbox"/>
Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt	<input checked="" type="checkbox"/>
Trennung von Entwicklungs-, Test- und Produktivsystem	<input checked="" type="checkbox"/>
Sonstige Maßnahmen: --	<input type="checkbox"/>

2 Maßnahmen zur 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	<input checked="" type="checkbox"/>
• Secure File Transfer Protocol (sftp)	<input checked="" type="checkbox"/>
• Citrix-Verbindung	<input checked="" type="checkbox"/>
• E-Mail-Verschlüsselung	<input checked="" type="checkbox"/>

• SMIME	<input type="checkbox"/>
• OpenPGP	<input checked="" type="checkbox"/>
• E-Mail Versand mit verschlüsselten ZIP-Dateien	<input checked="" type="checkbox"/>
• Datenaustausch über https-Verbindung	<input checked="" type="checkbox"/>
• verwendetes Verschlüsselungsprotokoll:	
- TLS 1.3	<input checked="" type="checkbox"/>
Sonstige Versendungsart: Gem. SGB V	<input checked="" type="checkbox"/>
• verwendete Verschlüsselungsalgorithmen:	
- AES (128/256 bit)	<input checked="" type="checkbox"/>
- RSA (1024/2048 bit)	<input type="checkbox"/>
- Diffie-Hellmann	<input type="checkbox"/>
- Sonstiges:	<input type="checkbox"/>
Nutzung von Signaturverfahren	<input type="checkbox"/>
Verwendetes Signaturverfahren:	
- RSA	<input type="checkbox"/>
- ElGamal	<input type="checkbox"/>
- DSA	<input type="checkbox"/>
- Sonstige: PGP, eigene	<input checked="" type="checkbox"/>
Digitales Signieren von Makros	<input type="checkbox"/>
Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle	<input type="checkbox"/>
Verschlüsselung vertraulicher Datensätze	<input checked="" type="checkbox"/>
Verschlüsselung mobiler Datenträger (z.B. Laptop-Festplatten, externe Festplatten, USB-Sticks)	<input checked="" type="checkbox"/>
Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken sowie Mobiltelefonen in Sicherheitsbereiche	<input type="checkbox"/>
Regelung zur Anfertigung von Datensatz-Kopien	<input type="checkbox"/>
Erstellen von Sicherungskopien von Datenträgern, die transportiert werden müssen	<input type="checkbox"/>
Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege	<input checked="" type="checkbox"/>
Direktabholung, Kurierdienst, Transportbegleitung	<input checked="" type="checkbox"/>
Vollständigkeits- und Richtigkeitsprüfung	<input checked="" type="checkbox"/>
Sonstige Maßnahmen: --	<input type="checkbox"/>

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	<input checked="" type="checkbox"/>
Manuelle oder automatisierte Auswertung der Protokolle	<input checked="" type="checkbox"/>
Differenzierte Benutzerberechtigungen:	<input checked="" type="checkbox"/>
• Einzelne Benutzernamen, keine Benutzergruppen	<input checked="" type="checkbox"/>
• Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	<input checked="" type="checkbox"/>
• Feldzugriff bei Datenbanken	<input checked="" type="checkbox"/>

Organisatorische Festlegung von Eingabezuständigkeiten	<input checked="" type="checkbox"/>
Verpflichtung auf das Datengeheimnis	<input checked="" type="checkbox"/>
Über OS-Standard hinausgehendes Log-Konzept	<input checked="" type="checkbox"/>
Dezidiertes Logserver	<input checked="" type="checkbox"/>
Regelung der Zugriffsberechtigungen für Logserver (LogAdmin)	<input checked="" type="checkbox"/>
Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke	<input checked="" type="checkbox"/>
Sonstige Maßnahmen: --	<input type="checkbox"/>

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

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

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

5.2 Sonstiges Datenschutzmanagement	Zutreffend (falls ja, bitte ankreuzen)
Einsatz einer Datenschutzmanagement-Software	<input type="checkbox"/>
Datenschutzbeauftragter benannt	<input checked="" type="checkbox"/>
IT-Sicherheitsbeauftragter benannt	<input checked="" type="checkbox"/>
Dokumentierter Prozess zum Umgang mit Datenschutzvorfällen	<input checked="" type="checkbox"/>
Klare Verantwortlichkeiten bei der Handhabung von Datenschutz- und Sicherheitsvorfällen	<input checked="" type="checkbox"/>
Dokumentierter Prozess zur Sicherstellung von Betroffenenrechten	<input checked="" type="checkbox"/>
Zentrale, für alle Mitarbeiter zugängliche Ablage von Richtlinien/Verfahrensweisungen	<input checked="" type="checkbox"/>
Sonstige Maßnahmen: --	<input type="checkbox"/>

**- Anlage 4 –
Unterauftragnehmer**

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

Unterauftragnehmer	Aufgabenfeld
NOVENTI HEALTH SE Tomannweg 6 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