Bedingungen Auftragsverarbeitung gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO) für NOVENTI Ora On-premise und NOVENTI Ora Cloud

NOVENTI HealthCare GmbH (Geschäftsbereich Division Sonstige Leistungserbringer),
Tomannweg 6, 81673 München

Stand November 2021

Präambel

Gegenstand der Vereinbarung ist die Regelung der Rechte und Pflichten des Verantwortlichen (nachfolgend „Auftraggeber“) und des Auftragsverarbeiters (NOVENTI HealthCare, nachfolgend „Auftragnehmer“). Der Auftragnehmer stellt dem Auftraggeber die Software „NOVENTI Ora“ entsprechend der jeweiligen Bestellung/Auftragsbestätigung und den Allgemeinen Geschäftsbedingungen NOVENTI Ora zur Verfügung. Der Auftraggeber hat die Möglichkeit, NOVENTI Ora in der eigenen IT-Infrastruktur und auf eigenen Datenträgern zu betreiben (nachfolgend: „NOVENTI Ora On-premise“) oder NOVENTI Ora über das Internet als Software-as-a-Service-Dienstleistung (nachfolgend: „NOVENTI Ora Cloud“) zu nutzen. In beiden Varianten werden personenbezogene Daten des Auftraggebers verarbeitet bzw. besteht die Möglichkeit des Zugriffs auf personenbezogene Daten des Auftraggebers. Der Auftragnehmer verarbeitet die personenbezogenen Daten des Auftraggebers in beiden Varianten als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO. 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) Der Auftragnehmer überlässt dem Auftraggeber die Software NOVENTI Ora entsprechend der jeweiligen Bestellung/Auftragsbestätigung und der Allgemeinen Geschäftsbedingungen NOVENTI Ora zur Nutzung. Bei der Software NOVENTI Ora handelt es sich um eine Praxisverwaltungssoftware. Art und Zweck der Verarbeitung unterscheiden sich je nach Art der Nutzung der Software. Die Art der Nutzung ergibt sich aus der jeweiligen Bestellung/Auftragsbestätigung.

a) NOVENTI Ora On-premise: Hat sich der Auftraggeber für die Variante NOVENTI Ora On-premise entschieden, erfolgt der Betrieb der Praxisverwaltungssoftware und eine damit einhergehende Verarbeitung personenbezogener Daten auf den Systemen des Auftraggebers. Um den ordnungsgemäßen Betrieb der Software sicherzustellen, besteht für den Auftragnehmer zum Zwecke von Wartung und Support die Möglichkeit, auf die Praxisverwaltungssoftware zuzugreifen. Dabei kann nicht ausgeschlossen werden, dass personenbezogene Daten des Auftraggebers eingesehen werden. Zudem kann es erforderlich sein, dass bestimmte Daten zum Zwecke der Fehlerbehebung an den Auftraggeber übermittelt werden.

b) NOVENTI Ora Cloud: Nutzt der Auftraggeber die Variante NOVENTI Ora Cloud, wird die Praxisverwaltungssoftware auf vom Auftragnehmer bereitgestellten Systemen betrieben. Der Auftragnehmer übernimmt in diesem Fall das Hosting der Anwendung. Um den ordnungsgemäßen Betrieb der Software sicherzustellen, besteht für den Auftragnehmer zum Zwecke von Wartung und Support zudem die Möglichkeit, auf die Praxisverwaltungssoftware zuzugreifen. Dabei kann nicht ausgeschlossen werden, dass personenbezogene Daten des Auftraggebers eingesehen werden. Zudem kann es erforderlich sein, dass bestimmte Daten zum Zwecke der Fehlerbehebung an den Auftraggeber übermittelt werden.

Im Übrigen ergibt sich der Gegenstand des Auftrags aus der jeweiligen Bestellung/Auftragsbestätigung und den Allgemeinen Geschäftsbedingungen NOVENTI Ora (im Folgenden „Hauptvertrag“).

(2) Der Auftragnehmer verarbeitet im Rahmen des Hauptvertrags personenbezogene Daten („Daten“) für den Auftraggeber. Diese werden nur im Auftrag und nach dokumentierter Weisung des Auftraggebers gemäß Art. 28 DSGVO (Auftragsverarbeitung) und den nachfolgenden Bestimmungen verarbeitet.

(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

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

3 Art der personenbezogenen Daten und Kategorien betroffener Personen

(1) Im Rahmen von NOVENTI Ora werden die folgenden personenbezogenen Daten verarbeitet:

- Versichertenstamm: Name, Geburtsdatum, Anschrift, Versichertennummer
- Kommunikationsdaten, z.B. Telefon, E-Mail
- Termindaten: Zeit, Ort; Behandler, Behandlungsgrund
- Gesundheitsdaten, z.B. Rezepte (Verordnungen), Befunde, Behandlungsdokumentation
- Beschäftigtendaten, z.B. Name, Dienstplan, Arbeitszeit, Gehälter

(2) Kreis der betroffenen Personen:

- Kunden der Auftraggeber bzw. Patienten
- Beschäftigte des Auftraggebers

4 Verantwortlichkeit und Weisungsbefugnis

(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 2 genannten Umfang. Dem Auftragnehmer ist es gestattet, die ihm übermittelten Daten zu anonymisieren, so dass keine Rückschlüsse auf natürliche Personen mehr möglich sind. Anonymisierte Daten, auf die die datenschutzrechtlichen Vorgaben entsprechend den Ausführungen aus Erwägungsgrund 26 DSGVO keine Anwendung mehr finden, kann der Auftragnehmer für eigene Zwecke verwenden.

(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.

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

(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

(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.

(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.

(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.

(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

(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.

(2) Die Vertragsparteien vereinbaren die in der **Anlage 1 „Technische und organisatorische Maßnahmen“** zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen.

(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)

(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.

(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.

(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.

(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 sowohl für die Variante NOVENTI Ora Cloud als auch für die Variante NOVENTI Ora On-premise sind in der **Anlage 2** zu diesem Vertrag aufgelistet.

8 Unterstützung bei der Wahrung der Betroffenenrechte

(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).

(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.

(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

(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.

(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.

(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.

(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

(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.

(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

(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.

(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.

(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

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 Datenschutz bei kirchlichen Einrichtungen

(1) Soweit es sich beim Auftraggeber um eine kirchliche Einrichtung im Sinne des § 3 des Gesetzes über den Kirchlichen Datenschutz (KDG) oder um eine Einrichtung im Sinne des § 3 der Kirchlichen

Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) handelt, ist dem Auftragnehmer bekannt, dass der Auftraggeber den datenschutzrechtlichen Bestimmungen des KDG bzw. der KDR-OG unterliegt. Der Auftragnehmer bestätigt die Kenntnis dieser Regelungen und deren Beachtung.

(2) Soweit es sich beim Auftraggeber um eine kirchliche Stelle im Sinne des § 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) handelt, ist dem Auftragnehmer bekannt, dass der Auftraggeber den datenschutzrechtlichen Bestimmungen des DSG-EKD unterliegt. Der Auftragnehmer unterwirft sich gemäß § 30 Absatz 5 Satz 3 DSG-EKD der kirchlichen Datenschutzaufsicht. Die Unterwerfung erstreckt sich auf die Aufgaben und Befugnisse der kirchlichen Datenschutzaufsicht nach §§ 43, 44 EKD-Datenschutzgesetz.

14 Schlussbestimmungen

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(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.

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

(4) Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:
- Anlage 1 (technische und organisatorische Maßnahmen)
- Anlage 2 - Unterauftragnehmer

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 zur 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 Dateizugriffen	☐
Protokollierung von Dateilöschungen	☐
Protokollierung von Dateiveränderungen	☐
• 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 von 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)	☒
Vorabkontrollen 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 (Mandantenfähigkeit 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 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	☒
• 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	☐
- ElGamal	☐

- 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 Sicherheitsbereiche	☐
Regelung zur Anfertigung von Datensatz-Kopien	☐
Erstellen von Sicherungskopien von Datenträgern, die transportiert werden müssen	☐
Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege	☒
Direktabholung, Kurierdienst, Transportbegleitung	☒
Vollständigkeits- und Richtigkeitsprüfung	☒
Sonstige Maßnahmen:	☐

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 Protokolle	☒
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	☒
Über OS-Standard hinausgehendes Log-Konzept	☒
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 Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten	☒
Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert	☒
Prüfung der Wirksamkeit getroffener Sicherheitsmaßnahmen 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 2 - Unterauftragnehmer

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

NOVENTI Ora Cloud

Unterauftragnehmer	**Aufgabenfeld**
NOVENTI HEALTH SE Tomannweg 6 81673 München	IT Services
Kronsoft Development SRL Bulevardul Saturn 51, Brașov 505600, Rumänien	Applikations-Entwicklung, -wartung, -support, -betrieb
T-Systems International GmbH, Hahnstr. 43d, 60528 Frankfurt am Main	Rechenzentrumsbetrieb
Retarus GmbH, Global Headquarters, Aschauer Straße 30, 81549 München, Germany	SMS-Versand
Reisswolf GmbH Ziegeleistr. 7 86368 Gersthofen	Datenträgervernichtung
DF Deutsche Fiskal GmbH Friedrichstraße 204 10117 Berlin	Zurverfügungstellung der „Fiskal Cloud“ (TSE)

NOVENTI Ora On-premise

Unterauftragnehmer	**Aufgabenfeld**
NOVENTI HEALTH SE Tomannweg 6 81673 München	IT Services
Kronsoft Development SRL Bulevardul Saturn 51, Brașov 505600, Rumänien	Applikations-Entwicklung, -wartung, -support, -betrieb
Retarus GmbH, Global Headquarters, Aschauer Straße 30, 81549 München, Germany	SMS-Versand
Reisswolf GmbH Ziegeleistr. 7 86368 Gersthofen	Datenträgervernichtung
DF Deutsche Fiskal GmbH Friedrichstraße 204 10117 Berlin	Zurverfügungstellung der „Fiskal Cloud“ (TSE)