

NOVENTI

azh srzh zrk

# **Vertrag über eine Auftragsverarbeitung gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)**

## Präambel

Diese Vereinbarung zur Auftragsverarbeitung im Sinne von Art. 28 DSGVO regelt die Rechte und Pflichten der Vertragsparteien („**Parteien**“) aus dem Auftragsverhältnis zwischen dem Leistungserbringer als Verantwortlichem im Sinne von Art. 4 Nr. 7 DSGVO („**Auftraggeber**“) und dem Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO, der NOVENTI HealthCare GmbH („**Auftragnehmer**“). Die Vereinbarung bindet den Auftragnehmer in Bezug auf den Auftraggeber und legt entsprechend der Bestimmungen der für Leistungserbringer geltenden Nutzungsbedingungen Gegenstand und Dauer der Verarbeitung personenbezogener Daten, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen und des Auftragsverarbeiters fest.

### § 1 Inhalt der Auftragsverarbeitung

- 1.1 Der Auftragnehmer verarbeitet personenbezogene Daten ("**Daten**") als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO im Auftrag des Auftraggebers. Eine genaue Beschreibung des Gegenstands des Auftrags sowie Art und Zweck der Datenverarbeitung ergeben sich aus der **Anlage 1** (Inhalt der Auftragsverarbeitung) zu dieser Vereinbarung. Im Übrigen ergibt sich der Gegenstand des Auftrags aus der für die Datenverarbeitung ausschlaggebenden Vereinbarung ("**Hauptvertrag**"), auf den hier verwiesen wird.
- 1.2 Der Auftragnehmer verarbeitet im Rahmen des Hauptvertrags Daten für den Auftraggeber. Diese werden nur im Auftrag und nach dokumentierter Weisung des Auftraggebers gemäß Art. 28 und 29 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 Auftrags

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

### § 3 Art der personenbezogenen Daten und Kategorien betroffener Personen

- 3.1 Art der Daten: Eine Auflistung der Art der Daten, die der Auftragnehmer für den Auftraggeber verarbeitet, finden sich in der **Anlage 1** (Inhalt der Auftragsverarbeitung) zu dieser Vereinbarung.
- 3.2 Kategorien betroffener Personen: Eine Auflistung der Kategorien der betroffenen Personen findet sich in **Anlage 1** (Inhalt der Auftragsverarbeitung) zu dieser Vereinbarung.

### § 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 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.
- 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 erforderlichenfalls 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 können auch Daten verarbeitet werden, die gemäß § 203 StGB unter ein Berufsgeheimnis fallen. Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, nach § 203 Abs. 4 S. 1 StGB strafbar machen. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.
- 5.3 Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.
- 5.4 Der Auftragnehmer ist nach Ziffer 7 dieser Vereinbarung berechtigt, Unterauftragnehmer zur Vertragserfüllung heranzuziehen. Im Ausland dürfen Unterauftragnehmer zur Vertragserfüllung nur dann herangezogen werden, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist. Der Auftragnehmer wird etwaige Unterauftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zum Stillschweigen verpflichten. Der Auftragnehmer wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzte Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren. Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.

## § 6 Datensicherheit

- 6.1 Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer
- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
  - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
  - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

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

- 6.2 Die Vertragsparteien vereinbaren die in der **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 unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in den Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Person nachzukommen (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 nach Möglichkeit 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 bzw. nach Beendigung der Vereinbarung 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**

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**

- 13.1 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.
- 13.2 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**

- 14.1 Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.
- 14.2 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.
- 14.3 Im Falle eines Widerspruchs zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.
- 14.4 Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:
- Anlage 1 (Inhalt der Datenverarbeitung)
  - Anlage 2 (technische und organisatorische Maßnahmen)
  - Anlage 3 (genehmigte Subdienstleister)

# Anlage 1a

## Inhalt der Auftragsverarbeitung NOVENTI Videosprechstunde

### § 1 Gegenstand des Auftrags, Art und Zweck der Verarbeitung:

Der Auftragnehmer bietet Leistungserbringern die Nutzung eines Web-basierten Services „NOVENTI Videosprechstunde“ an. Über NOVENTI Videosprechstunde können Patienten angelegt und Termine für die Durchführung von Videosprechstunden verwaltet werden. NOVENTI Videosprechstunde bietet zudem eine Adressbuchfunktion. Über die Adressbuchfunktion kann der Auftraggeber ein Adressbuch anlegen und verwalten. Die Bereitstellung der Adressbuchfunktion bzw. die Verarbeitung personenbezogener Daten in Zusammenhang mit der Nutzung der Adressbuchfunktion ist Gegenstand dieser Vereinbarung zur Auftragsverarbeitung.

### § 2 Art der personenbezogenen Daten und Kategorien betroffener Personen

Art der Daten:

- Stammdaten: Name, Geschlecht
- Kommunikationsdaten: E-Mail-Adresse, Telefon,

Kategorien der betroffenen Personen:

- Kunden bzw. Patienten des Auftraggebers

# Anlage 1b

## Inhalt der Auftragsverarbeitung NOVENTI Borino

### § 1 Gegenstand des Auftrags, Art und Zweck der Verarbeitung:

Der Auftragnehmer bietet Leistungserbringern die Nutzung eines Web-basierten Services „NOVENTI Borino“ an. Über NOVENTI Borino können Patienten und sonstige Nutzer online einen Termin bei dem jeweiligen Leistungserbringer vereinbaren. Neben der Möglichkeit der Terminbuchung bietet NOVENTI Borino dem Leistungserbringer weitere Möglichkeiten, wie die Veröffentlichung bestimmter Informationen zum Leistungsspektrum oder zu den Öffnungszeiten. Für die Wartung und den Support der Anwendung ist der Auftragnehmer verantwortlich. Im Übrigen ergibt sich der Gegenstand des Auftrags aus dem Hauptvertrag, auf den hier verwiesen wird.

### § 2 Art der personenbezogenen Daten und Kategorien betroffener Personen

Art der Daten:

- Stammdaten: Name, Geburtsdatum, Anschrift
- Kommunikationsdaten, z.B. Telefon, E-Mail-Adresse
- Terminiindaten. Zeit, Ort, Dauer; behandelnder Leistungserbringer, Behandlungsgrund
- Gesundheitsdaten, z.B. Rezepte (Verordnungen), Befunde, Behandlungsdokumentation
- Beschäftigtendaten, z.B. Namen von Beschäftigten des Auftraggebers

Kategorien der betroffenen Personen:

- Kunden bzw. Patienten des Auftraggebers
- Beschäftigte des Auftraggebers

# Anlage 2

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

### 1 Maßnahmen zu Gewährleistung der Vertraulichkeit

<b>1.1 Zutrittskontrolle</b>	<b>Zutreffend (falls ja, bitte ankreuzen)</b>
Soll verhindern, dass Unbefugte räumlich Zugang zu Datenverarbeitungsanlagen erhalten. Maßnahmen zur Gebäude- und Raumsicherung.	
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"/>
Videüberwachung 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"/>

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: <a href="#">Klicken Sie hier, um Text einzugeben.</a>	<input type="checkbox"/>

1.3 Zugriffskontrolle	Zutreffend (falls ja, bitte ankreuzen)
Soll unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen verhindern.	
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: <a href="#">Klicken Sie hier, um Text einzugeben.</a>	<input type="checkbox"/>

<b>1.4 Auftragskontrolle</b>	<b>Zutreffend</b>
Soll sicherstellen, dass Daten, die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftraggebers verarbeitet werden.	(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: <a href="#">Klicken Sie hier, um Text einzugeben.</a>	<input type="checkbox"/>

<b>1.5 Trennungskontrolle</b> 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: <a href="#">Klicken Sie hier, um Text einzugeben.</a>	<input type="checkbox"/>

## 2 Maßnahmen zu Gewährleistung der Integrität

<b>2.1 Weitergabekontrolle</b> 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: Klicken Sie hier, um Text einzugeben.	<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"/>
Dezidierter 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: Klicken Sie hier, um Text einzugeben.	<input type="checkbox"/>

### 3 Maßnahmen zu Gewährleistung der der Verfügbarkeit & Belastbarkeit

<b>3.1 Verfügbarkeitskontrolle</b> Soll Daten gegen zufällige Zerstörung oder Verlust schützen.	<b>Zutreffend</b> <b>(falls ja, bitte ankreuzen)</b>
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: <a href="#">Klicken Sie hier, um Text einzugeben.</a>	<input type="checkbox"/>

<b>3.2 Belastbarkeit (Widerstandsfähigkeit und Ausfallkontrolle)</b> Soll Systeme befähigen, mit risikobedingten Veränderungen umgehen zu können und Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufzuweisen.	<b>Zutreffend (falls ja, bitte ankreuzen)</b>
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"/>
Unverzügliche 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: <a href="#">Klicken Sie hier, um Text einzugeben.</a>	<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 Soll die Wirksamkeit der Datensicherheitsmaßnahmen gewährleisten.	Zutreffend (falls ja, bitte ankreuzen)
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: Klicken Sie hier, um Text einzugeben.	<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/Verfahrensanweisungen	<input checked="" type="checkbox"/>
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	<input type="checkbox"/>

# Anlage 3 - Unterauftragnehmer

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

<b>Unterauftragnehmer</b>	<b>Aufgabenfeld</b>
NOVENTI HEALTH SE Tomannweg 6 81673 München	IT Services
Kronsoft Development SRL Bulevardul Saturn 41-T Braşov 500440, 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