Anlage zum NOVENTI Connect TIaaS-Vertrag: Vertrag über eine Auftrasgverarbeitung gemäß Art. 28 DS-GVO („AVV“)

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

1. Gegenstand des Auftrags, Art und Zweck der Verarbeitung

1.1. Der Auftragnehmer stellt dem Auftraggeber einen Zugang zur Telematikinfrastruktur zur Verfügung. Dies erfolgt über im Rechenzentrum gehostete Konnektoren. Eine detaillierte Beschreibung der Leistung und der Vereinbarung zu Service Leveln entnehmen Sie der Leistungsbeschreibung NOVENTI Connect TIaaS.

1.2. Im Übrigen ergibt sich der Gegenstand des Auftrags aus der Bestelltung / Auftrag für NOVENTI Connect TIaaS auf die hier verwiesen wird (im Folgenden „Hauptvertrag“). Eine Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer ist darüber hinaus nicht vorgesehen.

1.3. Die Verarbeitung der personenbezogenen 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. Art der personenbezogenen Daten, Kategorien betroffener Personen

2.1. Art der Daten:

2.2. Kommunikationsdaten und sonstige Informationen, die mit Hilfe der Konnektoren zwischen den IT-Systemen des Auftraggebers und der Telematikinfrastruktur ausgetauscht werden oder ausgetauscht werden sollen sowie Daten die im Rahmen von Support-Leistungen ausgetauscht werden.

2.3. Kreis der betroffenen Personen:
- Kundendaten
- Beschäftigtendaten
- Patientendaten

3. Dauer des Auftrages

3.1. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

3.2. Der Auftraggeber kann unabhängig von den Regelungen im Hauptvertrag diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer die Erteilung von Auskünften oder den Zutritt des Auftraggebers im Rahmen von Kontrollen vertragswidrig verweigert. Nach der Kündigung darf der Auftragnehmer keine personenbezogenen Daten des Auftraggebers mehr verarbeiten.

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.

4.2. Der Auftragnehmer verarbeitet personenbezogene Daten nur 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. 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

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

5.2. Im Rahmen der Vereinbarung werden auch Daten verarbeitet, die gemäß § 203 StGB unter ein Berufsgeheimnis fallen. Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, nach § 203 Abs. 4 S. 1 StGB strafbar machen. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

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

5.4. Der Auftragnehmer ist nach Ziffer 7 dieser Vereinbarung berechtigt, Unterauftragnehmer zur Vertragserfüllung heranzuziehen. Im Ausland dürfen Unterauftragnehmer zur Vertragserfüllung nur dann herangezogen

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

6. Datensicherheit

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

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

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

6.2. Die Vertragsparteien vereinbaren die in dem Anlage 1 „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. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber schriftlich mitzuteilen.

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.

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 und vom Auftragnehmer die Übersendung einer Kopie dieser Verträge zu verlangen.

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 2 zu diesem Vertrag aufgelistet.

7.5. Erbringt der Subunternehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

7.6. Eine weitere Auslagerung durch den Subunternehmer bedarf der ausdrücklichen Zustimmung des Auftragnehmers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Subunternehmer aufzuerlegen.

8. Unterstützung bei der Wahrung von Betroffenenrechten

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). Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen.

8.2. Soweit betroffene Personen gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit ausüben können, stellt der Aufragnehmer sicher, dass sie die Daten, die sie dem Auftraggeber bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format erhalten können.

8.3. 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.

8.4. 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 Informationspflichten 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. Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei einer vorherigen Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO.

9.5. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

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. Der Auftragnehmer weist unaufgefordert dem Auftraggeber in Textform mit Datumsangabe nach, dass er sämtliche Datenträger sowie sonstigen Unterlagen an den Auftraggeber herausgegeben oder datenschutzkonform vernichtet oder gelöscht und somit keine Daten des Auftraggebers zurückbehalten hat.

10.3. 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. Kontrollrechte des Auftraggebers

11.1. Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistungen und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen sowie die Einhaltung des AVV 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 des AVV 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 des AVV 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

12.2. 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.

12.3. Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen, wenn der Auftraggeber einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist.

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. Alle Leistungen des Auftragnehmers in Zusammenhang mit der Erfüllung seiner Pflichten aus dieser Vereinbarung sind mit der Vergütung aus dem Hauptvertrag abgegolten.

14.5. Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:

- Anlage 1 „Technische und organisatorische Maßnahmen“
- Anlage 2 „Genehmigte Subunternehmer“

Anlage 1 – Technische und organisatorische Maßnahmen

Die im Einzelfall einschlägigen technischen und organisatorischen Maßnahmen sind abhängig vom jeweiligen Verarbeitungsvorgang:

- Das Hosting der Konnektoren sowie die Erbringung von 3rd-Level Support erfolgt über den Subdienstleister Secunet **(Anlage 1a).**
- Der Betrieb der Konnektoren sowie die Erbringung von 2nd-Level Support erfolgt durch den Subdienstleister Samhammer **(Anlage 1b).**
- Der Subdienstleister Kronsoft erbringt 1st-Level und 2nd-Level Support **(Anlage 1c)**

Anlage 1a – TOM secunet

Organisatorische Maßnahmen:
Lieferkette und Einsatzumgebung:

- Alle Rechenzentrumskonnektoren werden unter Berücksichtigung der sicheren Lieferkette an die oben benannten Rechenzentren geliefert.
- Die Rechenzentrumskonnektoren werden nach dem 4-Augen-Prinzip in einem abschließbaren Serverschrank montiert und in Betrieb genommen.
- Während der Inbetriebnahme werden lediglich die Grundfunktionalitäten, wie z.B. der Zugriff auf die GUI (Graphic User Interface) und das Einspielen einer gültigen Lizenz zur Funktionsfreischaltung getestet.
- Während dieser Phase kommt keiner der Konnektoren mit Produktivdaten in Berührung.
- Der Serverschank wird im Anschluss an den erfolgreichen Test verschlossen.
- Ort: Rechenzentren der Unterauftragnehmer (Unterauftragnehmer secunet: 23M GmbH, Kleyerstr. 75-87, 60326 Frankfurt; SysEleven GmbH, Boxhagener Str. 80, 10245 Berlin).

Technische Maßnahmen:
Inbetriebnahme

- Mit der Inbetriebnahme des Konnektors wird sich der Auftraggeber per Fernzugriff auf den Konnektor aufschalten und noch bevor der Leistungserbringer angebunden wird, neue und eigene Login-Daten vergeben.
- Die Login-Daten werden der secunet nicht mitgeteilt und sind für secunet auch nicht zugänglich. Dadurch hat secunet zu keinem Zeitpunkt die Möglichkeit auf den Konnektor zuzugreifen und somit keinen Zugriff auf Daten der Produktivumgebung.
- Die Administration der Konnektoren im Rahmen des Hauptvertrages erfolgt ausschließlich durch den Auftraggeber oder von von ihm beauftragte Dritte.
- Die über den Konnektor laufenden Daten sind gemäß der Vorgaben der gematik GmbH verschlüsselt und secunet hat keinen Zugriff auf das Schlüsselmaterial.

Außerbetriebnahme:

- Mit der Außerbetriebnahme eines Konnektors (z. B. wegen eines Defekts), wird der Konnektor mit Hilfe seiner Seriennummer von secunet zuerst gesperrt und dann durch secunet entsorgt.

Anlage 1b – TOM Samhammer

Nr.	Gebiet	Beschreibung
0	**Organisation**	
	Wie ist die Umsetzung des Datenschutzes organisiert?	Ein externer Datenschutzbeauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus dem BDSG (neu DSGVO) eingesetzt.
	Nennen Sie uns bitte den Namen und die Kontaktdaten Ihres Datenschutzbeauftragten.	Christian Volkmer +49-941-2986930 Projekt 29 GmbH & Co. KG Ostengasse 14 93047 Regensburg
	In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit, als auch eine konstante Sensibilisierung durch monatliche Datenschutznewsletter, fachbezogene Webschulungen und persönliche Sensibilisierung durch den externen Datenschutzbeauftragten.
	Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Im Rahmen des internen Verfahrens-verzeichnisses sind die Datenströme dokumentiert und die Zulässigkeit der Verarbeitung und Nutzung nach BDSG nachgewiesen. Eventuell notwendige Vorabkontrollen werden schon im Planungsstadium integriert.
1	**Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**	
1.1	**Zutrittskontrolle**	
	Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Das Gebäude ist mit einem Zutrittskontrollsystem gesichert (personalisierte Karte + PIN).
	Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Die Räume werden, wenn gefordert, durch das Zutrittskontrollsystem gesichert.
	Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?	Die Verarbeitungsanlagen werden ebenfalls durch das Zutrittskontrollsystem gesichert (Nur IT-Personal und Vorstand hat Zutritt).
	Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?	Im Rahmen der Kontrollen durch den externen Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft.
1.2	**Zugangskontrolle**	
	Wie erfolgt die Vergabe von Benutzerzugängen?	Benutzerzugänge werden nur sehr selektiv und nach Genehmigung durch die IT-Abteilung vergeben. Rechtevergabe und Änderung sind dokumentiert.
	Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Eine regelmäßige Revision der vergebenen Rechte ist Teil der Prüfungen der Maßnahmen und wird zusammen mit dem externen Datenschutzbeauftragten durchgeführt und von diesem dokumentiert.
	Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert?	Die Anlage und Veränderung von Benutzerzugängen wird im firmeneigenen Ticketsystem dokumentiert.
	Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird?	Die Entscheidungen zur Rechtevergabe halten sich streng an die entsprechenden Vorgaben. Nur der interne IT-Service verfügt über Administratorenzugänge
	Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.) und wie ist der Zugang gestaltet?	Der Zugriff von außerhalb des Unternehmens wurde mit SSL-VPN umgesetzt. Hier hat jeder Mitarbeiter ein personalisiertes Profil.
1.3	**Zugriffskontrolle**	
	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Die Passwörter werden vom jeweiligen Mitarbeiter selbst vergeben. Die strengen Systemvoreinstellungen zwingen zu einer hohen Passwortkomplexität. Passwörter werden nicht gespeichert.
	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	Die Vorgaben und Empfehlungen des BSI dienen als Vorbild für die o. g. Systemeinstellungen. Diese wurden per Group-Policies definiert.
	Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss?	Die Aufforderung zur Änderung ist in der Group Policy definiert. Jeder Benutzer kann sein Passwort jederzeit selbst nach definierten Regeln ändern. Nach 90 Tagen muss das Passwort geändert werden
	Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	Schulung und Sensibilisierung der Mitarbeiter. Einweisungen und regelmäßige Schulungen zu den verwendeten Geräten
	Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?	Siehe auch Punkt „Vergabe von Benutzerzugängen“ Punkt 1.2; die IT-Abteilung prüft in regelmäßigen Abständen die Rechte und Benutzerstruktur
	Wie erfolgt die Dokumentation von Zugriffsberechtigungen?	Alle freigeschalteten Berechtigungen werden im hauseigenen Ticketsystem festgehalten
	Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?	Stichprobenartige Durchsicht der Systemprotokolle durch die IT-Abteilung

Nr.	Gebiet	Beschreibung
	Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet?	Keine festgelegten Fristen, meist Systemparameter, ausschließlich der interne IT-Service
1.4	**Trennungskontrolle**	
	Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden?	Alle Kundensysteme sind getrennt voneinander. Sollte eine Systemtrennung physikalisch nicht möglich sein, werden die Daten über die Mandantenfähigkeit der Systeme voneinander getrennt.
1.5	**Pseudonymisierung**	
	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Alle mit der Verarbeitung von personenbezogenen Daten betrauten Personen wurden entsprechend verpflichtet. Ein Datenschutzkonzept wird im Unternehmen eingesetzt und ist allen Mitarbeitern bekannt gemacht. Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit, als auch eine konstante Sensibilisierung durch monatliche Datenschutznewsletter, fachbezogene Webschulungen und persönliche Sensibilisierung durch den externen Datenschutzbeauftragten.
	Wie werden personenbezogene Daten verarbeitet /aufbewahrt, sodass diese nicht den betroffenen Personen zugeordnet werden können?	Daten werden nicht pseudonymisiert
2	**Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**	
2.1	**Weitergabekontrolle**	
	Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?	Daten werden verschlüsselt über VPN / SFTP / TLS / HTTPS weitergegeben
	Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche?	HTTPS / SFTP / VPN (AES256)
	Wie wird die Weitergabe personenbezogener Daten dokumentiert?	Über die Systemhistorie
	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff.
	Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?	Nicht vorhanden
2.2.	**Eingabekontrolle**	
	Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?	n/a
	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Rollen-/Rechtekonzepte/Systemhistorie
	Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß der Weisungen des Auftraggebers erfolgen kann?	Zugriffskontrolle anhand des Rollen-/Rechte-konzepts zur ordnungsgemäßen Datenbear-beitung und Speicherung
	Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers durchführt?	Sämtliche Unterauftragnehmer unterliegen den gleichen Vorgaben wie der Auftragnehmer. Entsprechende Verträge sind geschlossen. Die Pflichten zur Überprüfung der Unterauftrag-nehmer übernimmt der Datenschutzbeauftrage des Unternehmens. Er ist auch bei der Auswahl der beauftragten Firmen maßgeblich beteiligt.
	Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?	Festlegung durch Vertragsbindung, bei Wegfall des Zweckes ist ebenfalls eine Löschung der Daten indiziert.
3	**Verfügbarkeit und Belastbarkeit**	
3.1.	**Verfügbarkeitskontrolle**	
	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?	Gesicherte Daten sind räumlich getrennt von Produktivdaten; ältere Bänder werden in Safe verwahrt
	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?	Ständig aktuelle Virenscanner und Spamfilter finden Einsatz. Die Systeme werden regelmäßig upgedatet.
	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Physische Löschung bei funktionsfähigen Datenträgern und mechanische Zerstörung defekter Datenträger vor der Entsorgung. Die datenschutzkonforme Entsorgung erfolgt durch einen zertifizierten externen Dienstleister
3.2.	**Wiederherstellbarkeit**	
	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DS-GVO)	Eingerichtetes 2-stufiges Backup-Verfahren. Wiederherstellung Datenstände der vergangenen 30 Tage auf Zuruf; Sicherung älterer Datenstände durch Einspielen von Bändern

Nr.	Gebiet	Beschreibung
4.	**Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)**	
	Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)?	Der externe Datenschutzbeauftragte überprüft regelmäßig und teilweise auch unangekündigt, die Einhaltung der technisch-organisatorischen Maßnahmen.
	Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)?	Einsatz eines Ticketsystems (1stAnswer) zweistufig (1st und 2nd Level); zusätzlich 24x7 telefonische Bereitschaft und automatisierte Überwachung und Alarmierung (PRTG)
	Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)?	Keine Vorbelegung durch Checkboxen; bei Anmeldung im System erfolgen keine Vorbelegungen; Benutzer muss die Anmeldeinformationen jeweils eintragen
4.1	**Auftragskontrolle**	
	Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenverarbeitung (Datenschutz-Management)?	Das Vertragswerk wurde entsprechend den neuen Richtlinien zur Auftragsdatenverarbeitung gestaltet. Der externe Datenschutzbeauftragte nimmt entsprechende Beratungs- und Kontrollpflichten wahr.

Anlage 1c – TOM Kronsoft

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	☒
Biometrische Zutrittskontrolle	☐
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: Klicken Sie hier, um Text einzugeben.	☐

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: Klicken Sie hier, um Text einzugeben.	☐

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:	
Shredder (Cross-Cut, mindestens Stufe 3, DIN 66399)	☐
Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister	☒
Datenträgerentsorgung - Sichere Löschung von Datenträgern (DIN 66399):	☐
Peter-Gutmann-Algorithmus – 35-faches Überschreiben	☒
Physikalische Zerstörung (z.B. Shredder bei Partikelgrößen bis max. 1000 Quadrat-Millimeter)	☐
Entmagnetisierung durch thermische Zerstörung (Erhitzung der Magnetplattenoberfläche über die Curie-Temperatur der verwendeten Beschichtung hinaus)	☐
Entmagnetisierung mittels eines Degaussers	☐
Sonstiges Vernichtungsverfahren:	☐
Richtlinie zur Datenvernichtung	☐
Clean Desk-Policy	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

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: Klicken Sie hier, um Text einzugeben.	☐

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)	☒
Physikalische Datentrennung (z.B. unterschiedliche Systeme oder Datenträger)	☒
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	☒
Zuordnung von Datensätzen zu Zweckattributen	☒
Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei & Speicherung auf einem anderen System	☐
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

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: Klicken Sie hier, um Text einzugeben.	☐

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: Klicken Sie hier, um Text einzugeben.	☐

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	☒
Feuerfeste Schränke	☐
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: Klicken Sie hier, um Text einzugeben.	☐

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?):	☐
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: Klicken Sie hier, um Text einzugeben.	☐

Cloudlösungen bei Partnerunternehmen

Unsere Partner sind sorgfältig ausgewählt und verfügen über entsprechende Zertifizierungen.

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: Klicken Sie hier, um Text einzugeben.	☐

5.2 Sonstiges Datenschutzmanagement	Zutreffend (falls ja, bitte ankreuzen)
Verwenden datenschutzfreundlicher Softwareeinstellungen	☐
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: Klicken Sie hier, um Text einzugeben.	☐

Anlage 2 – Genehmigte Subunternehmer

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Subunternehmer zu, jedoch nur unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO:

Firma (Subunternehmer), Adresse	Verarbeitungsstandort	Art der Dienstleistung
secunet Security Networks AG Kurfürstenstraße 58, 45138 Essen	Deutschland	Bereitstellung und Hosting der Konnektoren, Erbringung von Wartungs- und Supportleistungen
Samhammer AG Zur Kesselschmiede 3 92637 Weiden	Deutschland	Betrieb der Konnektorfarm, Erbringung von Wartungs- und Supportleistungen
Kronsoft Development SRL Bd. Saturn 51, 500440, Brasov, Rumänien	Rumänien	Erbringung von Entwicklungs- sowie Wartungs- und Supportleistungen
CompuGroup Medical Deutschland AG **Business Area Connectivity** **Maria Trost 21** **D-56070 Koblenz**	Deutschland	Bereitstellung KIM-Client, KIM-Mailserver, KIM-Fachdienst. Die CGM unterhält diesen seitens gematik zugelassenen Dienst für einen sektorübergreifenden Daten- und Informationsaustausch ausschließlich für Beteiligte im Gesundheitswesen und explizit für Beteiligte der Telematikinfrastruktur (nachfolgend „TI“)
Arvato Systems GmbH **Riebeckstraße 62** **04317 Leipzig** **Germany**	Deutschland	Bereitstellung VPN-Zugangdienst, dieser verbindet medizinische Einrichtungen über den Konnektor mit dem zentralen Netz der Telematik-Infrastruktur.