netzlink

AUFTRAGSDATENVERARBEITUNG

Vertrag über die Auftragsverarbeitung personenbezogener Daten (AV-Vertrag),

gemäß Artikel 28 der europäischen Datenschutz-Grundverordnung (DS-GVO)

20. Juli 2020

Vertrag über die Auftragsverarbeitung personenbezogener Daten

für Dienstleistungen im Rahmen von SORMAS

zwischen

Kundenname
Adresse

vertreten durch die Geschäftsführung Herr / Frau

nachfolgend Servicenehmer genannt (Verantwortlicher im Sinne der DS-GVO)

und

Netzlink Informationstechnik GmbH
IT-Campus Westbahnhof
Westbahnhof 11
38118 Braunschweig

vertreten durch Geschäftsführer Harald Lies

nachfolgend Servicenehmer genannt (Auftragsverarbeiter im Sinne des DS-GVO)

Präambel

Dieser Auftragsverarbeitungsvertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der Bereitstellung und dem Betrieb der Softwareanwendung SORMAS als sogenannter „Managed Service“ ergeben. Sämtliche in diesem AV-Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen können.

§ 1 Definitionen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DS-GVO, § 2 BDSG, § 2 UWG und § 2 TMG. Sollten in den Artikeln bzw. Paragraphen sich widersprechende Darstellungen zu finden sein, gelten die Definitionen in der Rangfolge DS-GVO, BDSG, UWG und TMG. Weiterhin gelten folgende Begriffsbestimmungen:

(1) Unterauftragnehmer

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Auftragnehmers verarbeitet und diese Verarbeitung die Erbringung der in diesem AV-Vertrag benannten Leistungen betrifft.

(2) Verarbeitung im Auftrag

Verarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch einen Auftragnehmer im Auftrag des Auftraggebers.

(3) Weisung

Weisung ist die auf eine bestimmte Verarbeitung personenbezogener Daten des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden im AV-Vertrag konkret festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen ergänzt werden (Einzelweisung).

§ 2 Gegenstand des Auftrags

(1) Gegenstand der Auftragsverarbeitung ist die Erbringung folgender Leistungen durch den Auftragnehmer.

Auftragsdetails: Bereitstellung, Betrieb und Wartung der Softwarelösung SORMAS als Managed Service (SORMAS aaS).

Der Auftragnehmer ist verpflichtet, die Verfahren des Auftraggebers zum Datenschutz umzusetzen. Der Auftragnehmer ist verpflichtet, die Anweisungen des Auftraggebers zu befolgen, damit die Rechte aus dem Datenschutz der betroffenen Person gesichert sind.

Exemplarische Beschreibung des Zwecks der Verarbeitung: SORMAS-OEGD-COVID-19 ist eine spezielle auf den deutschen öffentlichen Gesundheitsdienst (ÖGD) angepasste Version, die in Zusammenarbeit mit den Gesundheitsämtern weiter optimiert wird. Fortlaufend ergänzte Informationen finden sich unter: sormas-oegd.de

Die wichtigsten Eigenschaften von SORMAS für die aktuelle COVID-19 Situation sind:

1. COVID-19-spezifische Prozessmodelle für Fallmeldungen, Infektionsverläufe und Diagnostik

2. Gesundheitliche Überwachung per App durch Kontaktpersonen mit voller Datenintegration

3. Auf Smartphones und Tablets mobil und offline nutzbar

4. Fortlaufend aktualisierte Dashboards mit epidemiologischen Karten, Grafiken und Prozessanalysen

(2) Folgende personenbezogene Daten werden durch den Auftragnehmer verarbeitet (im Folgenden einzeln oder gemeinsam „personenbezogene Daten" genannt):

- Personenstammdaten, Kontaktdaten
- Pseudonyme
- Kommunikationsdaten (IP-Adressen, Telefonnummern, Email Adressen)
- besondere Kategorien von personenbezogenen Daten
    - Daten über die Gesundheit
    - Daten aus Testungen
    - Daten zu Biomaterialproben

(3) Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags betroffene Personen umfasst

- Erkrankte und ggf. deren Kontaktpersonen
- Projektbeteiligte des Auftraggebers und der (Unter-)Auftragnehmer (z.B. in Logfiles, Berechtigungssystem)

(4) Der Zugriff auf personenbezogene Daten erfolgt durch:

- Übersendung/Transfer durch den Auftraggeber
- Verarbeitung mit potentieller Einsichtnahme in personenbezogene Daten durch den Auftragnehmer erfolgt nur, sofern dies im Einzelfall erforderlich ist, beispielsweise bei Wartungsarbeiten und zur Fehlerbeseitigung; Löschung der zugeordneten Datenbankinhalte nach Beendigung des Auftragsverhältnisses
- Verarbeitung durch den Auftraggeber, dem zuständigen Gesundheitsamt

§ 3 Verantwortlichkeit

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher" im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Auftraggeber sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dazu müssen alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Dabei ist jede Partei für die Verpflichtung des eigenen Personals zuständig. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.

(3) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

§ 4 Dauer des Auftrags

(1) Der AV-Vertrag wird mit der Unterzeichnung wirksam und gilt für die Dauer der Nutzung von SORMAS aaS.

(2) Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages z.B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

(3) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar. Ansonsten gilt eine Kündigungsfrist von 14 Tagen zum Monatsende.

(4) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

(5) Nach Ende des Vertrages können dem Auftraggeber die Datenbankinhalte auf Wunsch in geeigneter Form zur Verfügung gestellt werden, ansonsten werden die produktiven Daten datenschutzkonform gelöscht.

§ 5 Weisungsbefugnis des Auftraggebers

(1) Der Umgang und die Verarbeitung mit den personenbezogenen Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

(2) Änderungen des § 2 Absatz 1, die diese weiter konkretisieren, sie jedoch nicht maßgeblich modifizieren, sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer wesentlichen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf der Änderung, steht dem Auftragnehmer ein ordentliches Kündigungsrecht bezüglich des von der Weisung betroffenen AV-Vertrages zu. Verweigert der Auftragnehmer, die Änderung durchzuführen, steht auch dem Auftraggeber ein ordentliches Kündigungsrecht zu. Erfolgt eine Kündigung, so ist für die restliche Vertragslaufzeit weiterhin die vertraglich vereinbarte Leistung durch den Auftragnehmer zu erbringen.

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

§ 6 Leistungsort

(1) Der Auftragnehmer wird die vertraglichen Leistungen in Deutschland erbringen.

§ 7 Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Der Auftragnehmer darf in die Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers Einsicht nehmen. Eine Erhebung, Verarbeitung oder weitere Nutzung erfolgt nicht.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber nachweisen. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus Art. 32 DS-GVO resultierenden Maßnahmen.

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Verantwortliche verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiterzuleiten.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt in Anlage 1 zu diesem Vertrag.

(3) Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DS-GVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DS-GVO notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein aussagekräftiges und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsverarbeitung zur Verfügung. Anfallende Aufwände für die Erstellung und Aktualisierung dieses Datenschutz- und Sicherheitskonzeptes werden vom Auftraggeber vergütet, sofern dieses Dokument nicht Bestandteil des ursprünglichen Auftrages war.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Datenschutzfolgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.

(6) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Dies gilt auch nach Beendigung des Vertragsverhältnisses.

(7) Weiterhin sind alle Personen des Auftragnehmers bzgl. der Pflichten zur Wahrung von Geschäfts- und Betriebsgeheimnissen des Auftraggebers zu verpflichten und müssen auf §17 UWG hingewiesen werden.

(8) Kontakt Datenschutzbeauftragter
Sie erreichen den Datenschutzbeauftragten unter der E-Mail
datenschutzbeauftragter@netzlink.com
Als externer Datenschutzbeauftragter ist beim Auftragnehmer derzeit

Martin Overbeck (E-Mail: overbeck@elektro-datentechnik.de)

benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DS-GVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner.

(9) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Art. 33, 34 DS-GVO.

(10) Es erfolgt keine separate Speicherung von personenbezogenen Daten durch den Auftragnehmer.

(11) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.

(12) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(13) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichen im Sinne der DS-GVO liegen.

(14) Der Auftragnehmer bestätigt die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.
Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen und zu dokumentieren.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Verantwortlichen abzustimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren. Soweit die beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht genügen, benachrichtigt er den Verantwortlichen unverzüglich.

Die Datensicherheitsmaßnahmen beim Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Sicherheitsstandards nicht unterschreiten.

§ 8 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Person ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (Rechtmäßigkeit der Verarbeitung) vorliegen, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Dem Auftraggeber obliegen die aus Art. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten einer betroffenen Person.

(4) Der Auftraggeber kann weisungsberechtigte Personen benennen. Weisungsberechtigte Personen des Auftraggebers sind die Geschäftsführung und Personen mit entsprechender Autorisierung. Diese können auf Wunsch gesondert benannt oder eingegrenzt werden. Hierbei sind dem Auftragnehmer folgende Informationen anzugeben. (Bei mehr als einer Person, bitte Anlage 2 ausfüllen).

Vorname(n) u Nachname(n)	
und/ oder Funktion(en)	
und/oder Abteilung(en)	
Rufnummer(n)	
Emailadresse(n)	

Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich oder in Textform mitteilen.

(5) Als Datenschutzbeauftragter ist beim Auftraggeber nach Art. 37 DS-GVO derzeit benannt:

Name des Datenschutzbeauftragten

Adresse Straße

Adresse PLZ Ort

Telefon:

Email:

Ein Wechsel des Datenschutzbeauftragten ist dem Auftragnehmer unverzüglich schriftlich mitzuteilen. Der Auftraggeber gewährleistet, dass die Anforderungen an ihn bzgl. der Stellung des Datenschutzbeauftragten und seiner Tätigkeit gemäß Art. 38 DS-GVO erfüllt werden.

(6) Der Auftraggeber legt die Maßnahmen nach § 11 zur Beendigung des Auftrages durch Weisung fest.

(7) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

§ 9 Kontrollrechte des Auftraggebers

(1) Die Durchführung der Auftragskontrolle mittels Prüfungen durch den Auftraggeber oder von ihm hierzu beauftragten Personen bzw. Institutionen im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags wird vom Auftragnehmer unterstützt. Insbesondere verpflichtet sich der Auftragnehmer, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

(2) Der Auftraggeber hat das Recht zum Zweck der Auftragskontrolle vom Auftragnehmer hinreichende Garantien einzufordern:

a. schriftliche Selbstauskünfte des Auftragnehmers,

b. Überprüfung der Einhaltung der vereinbarten Regeln durch einen sachkundigen Mitarbeiter des Auftraggebers oder einen Dritten, der nicht in einem

Wettbewerbsverhältnis zum Auftragnehmer stehen darf. Hierzu ist eine rechtzeitige Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs beim Auftragnehmer erforderlich.

c. Der Verantwortliche kann die Einhaltung eines genehmigten Zertifizierungsverfahrens gem. Art. 42 DS-GVO durch den Auftragsverarbeiter als Faktor heranziehen, um die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen zu beurteilen. Der Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

(3) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(4) Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte auch hierbei möglichst vermieden werden.

§ 10 Einsichtnahme von Daten

Der Auftragnehmer darf die vertragsgegenständlichen Daten nicht eigenmächtig berichtigen, löschen oder deren Verarbeitung einschränken; insbesondere dürfen die Update- und Pflegemaßnahmen die Datenintegrität nicht verletzen. Die datenschutzkonforme Löschung, Einschränkung oder Berichtigung von Daten übernimmt der Auftraggeber.

§ 11 Unterauftragnehmer

(1) Der Auftragnehmer nimmt Unterauftragnehmer in Anspruch. Der Auftragnehmer stellt sicher, dass die beauftragten Unterauftragnehmer zur Einhaltung der in diesem AV-Vertrag vereinbarten Pflichten und Regeln verpflichtet sind.

(2) Der Auftragnehmer setzt den folgenden Unterauftragnehmer ein. Der Einsatz erfolgt ausschließlich im Falle von Fehlerbehebung und Wartung, wenn dies nicht vom Auftragnehmer selbst erfüllt werden kann.

Firmenname	Ort
symeda GmbH (Softwareentwicklung)	38114 Braunschweig (Deutschland)

(3) Die nachfolgenden Regelungen finden sowohl für den Unterauftragnehmer als auch für alle in der Folge eingesetzten weiteren Unterauftragnehmer entsprechende Anwendung.

(4) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht, soweit diese den Bedingungen dieses AV-Vertrags genügen. Beabsichtigt der Auftragnehmer Ersetzungen oder Erweiterungen von Unterauftragnehmern, so wird er die Auftraggeber hierzu informieren.

Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

(5) Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.

(6) Unterauftragnehmern werden im Wege eines Vertrags dieselben Pflichten auferlegt, die in diesem AV-Vertrag zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit sowie den beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. Hierbei müssen ferner hinreichend Garantien dafür vereinbart werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO und diesem AV-Vertrag erfolgt.

Die beschriebenen Verfahren der Nachweisführung datenschutzrechtlicher Anforderungen durch den Auftragnehmer betreffen gleichermaßen auch dessen Unterauftragnehmer.

(7) Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten.

§ 12 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an personenbezogenen Daten sowie an Unterlagen, Datenträgern, Verarbeitungsergebnissen wird ausgeschlossen.

§ 13 Haftung

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

(2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

a. er den aus der DS-GVO resultierenden und speziell für den Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
b. er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
c. er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

(3) Soweit der Auftraggeber zum Schadensersatz gegenüber der betroffenen Person verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten. Dies gilt für Schäden durch Bußgeldfestsetzungen entsprechend.

(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er

a. seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
b. unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

§ 14 Schriftformklausel

Andere als die in diesem AV-Vertrag getroffenen Vereinbarungen bestehen nicht. Mündliche Nebenabreden sind nicht getroffen. Änderungen und Ergänzungen bedürfen der Schriftform. Dies gilt auch für die Schriftformklausel

§ 15 Salvatorische Klausel

(1) Sollten sich einzelne Bestimmungen dieses AV-Vertrages ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des AV-Vertrages im Ganzen hiervon unberührt.

(2) Auftraggeber und Auftragnehmer verständigen sich im Falle einer unwirksamen oder undurchführbaren Bestimmung darüber, ob und wie diese durch eine rechtsgültige Bestimmung ersetzt werden kann, die der ungültigen oder undurchführbaren Bestimmung sowie dem ursprünglich Gewollten möglichst nahekommt. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich der AV-Vertrag als lückenhaft erweist.

(3) Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter Abs. 2 genannte unwirksame Bestimmung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Rechte und Freiheiten natürlicher Personen am besten gewährleistet.

§ 16 Rechtswahl, Gerichtsstand

(1) Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts.

(2) Gerichtsstand ist Braunschweig (Deutschland).

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Geschäftsführer/in	Unterschrift Zeichnungsberechtigte/r
Netzlink Informationstechnik GmbH	des Auftraggebers
Stempel	Stempel

Anlage 1

Nachweis der allgemeinen technischen und organisatorischen Maßnahmen

Nachstehende Punkte beschreiben den Mindestinhalt der technischen und organisatorischen Maßnahmen.

1 Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen in personenbezogene Daten Einsicht genommen werden.

Es existieren folgende Maßnahmen zur Zutrittskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Alarmanlage	Schlüsselregelung / Liste
Automatisches Zugangskontrollsystem	Empfang / Rezeption / Pförtner
Biometrische Zugangssperren	Besucherbuch / Protokoll der Besucher
Chipkarten / Transpondersysteme	Mitarbeiter- / Besucherausweise
Manuelles Schließsystem	Besucher in Begleitung durch Mitarbeiter
Sicherheitsschlösser	Sorgfalt bei Auswahl des Wachpersonals
Schließsystem mit Codesperre	
Absicherung der Gebäudeschächte	
Türen mit Knauf Außenseite	
Klingelanlage mit Kamera	
Videoüberwachung der Eingänge	

Auf die Datenverarbeitungsanlagen, mit denen in personenbezogene Daten Einsicht genommen werden, darf ausschließlich vom lokalen IT-System, das der angegebenen Zutrittskontrolle unterliegt, zugegriffen werden. Eine Einsichtnahme von Fernarbeitsplätzen ist ausgeschlossen.

1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen, mit denen in personenbezogene Daten Einsicht genommen werden kann.

Es existieren folgende Maßnahmen zur Zugangskontrolle:

Technische Maßnahmen	**Organisatorische Maßnahmen**
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen
Login mit biometrischen Daten	Erstellen von Benutzerprofilen
Anti-Viren-Software Server	Zentrale Passwortvergabe
Anti-Virus-Software Clients	Richtlinie „Sicheres Passwort"
Anti-Virus-Software mobile Geräte	Richtlinie „Löschen/Vernichten“
Firewall	Richtlinie „Clean Desk" (CDP)
Intrusion Detection Systeme	Allg. Richtlinie Datenschutz und/oder Sicherheit
Mobile Device Management	Mobile Device Policy
Kein Remote-Zugriff im Projekt zugelassen	Anleitung „Manuelle Desktopsperre“
Verschlüsselung von Datenträgern	
BIOS Schutz (separates Passwort)	
Sperre externer Schnittstellen (USB)	
Automatische Desktopsperre	
Verschlüsselung von Notebooks/Tablet	

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können.

Es existieren folgende Maßnahmen zur Zugriffskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
Aktenschredder (mind. P-4)	Einsatz Berechtigungskonzepte
Externer Aktenvernichter (DIN 66399)	Minimale Anzahl an Administratoren
Physische Löschung von Datenträgern	Datenschutztresor
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	Verwaltung Benutzerrechte durch Administratoren

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Es existieren folgende Maßnahmen zur Trennungskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung von Produktiv- und Testumgebung	Steuerung über Berechtigungskonzept
Physikalische Trennung (Systeme/Datenbanken/Datenträger)	Festlegung von Datenbankrechten
Mandantenfähigkeit relevanter Anwendungen	Datensätze sind mit Zweckattributen versehen

1.5 Pseudonymisierung

Es existieren folgende Maßnahmen zur Pseudonymisierung:

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt)	Die Datenweitergabe an die berechtigten Parteien, dies sind das zugehörige Landesgesundheitsamt und das Robert-Koch-Institut, erfolgt ausschließlich in anonymisierter Form. Das entsprechende Datentransferobjekt enthält lediglich die ersten drei Zeichen der Postleitzahl sowie das Alter und Geschlecht der betroffenen Person.

2. Integrität

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

Technische Maßnahmen	**Organisatorische Maßnahmen**
Email-Verschlüsselung	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
Einsatz von VPN	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
Protokollierung der Zugriffe und Abrufe	Weitergabe in anonymisierter oder pseudonymisierter Form
Sichere Transportbehälter	Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	Persönliche Übergabe mit Protokoll
Nutzung von Signaturverfahren	

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht, mit welchen Rollen welche Daten eingegeben, geändert oder gelöscht werden können
Manuelle oder automatisierte Kontrolle der Protokolle	Nachvollziehbarkelt von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind: Beispiele sind insbesondere: Backup- Verfahren.

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

Technische Maßnahmen	**Organisatorische Maßnahmen**
Feuer- und Rauchmeldeanlagen	Backup & Recovery-Konzept (ausformuliert)
Löschanlage und Feuerlöscher im Rechenzentrum	Kontrolle des Sicherungsvorgangs
Serverraumüberwachung Temperatur und Feuchtigkeit	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
Rechenzentrum redundant klimatisiert	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
Unabhängige redundante Stromversorgung	Keine sanitären Anschlüsse im oder oberhalb des Rechenzentrums
Aktive überwachte Schutzsteckdosenleisten im Rechenzentrum	Pflege eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
Datenschutztresor (S60DIS. S120DIS, andere geeignete Normen mit Quelldichtung etc.)	Getrennte Partitionen für Betriebssysteme und Daten
RAID System/Festplattenspiegelung	
Videoüberwachung des Rechenzentrums	
Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutzmanagement

Es existieren folgende Maßnahmen zum Datenschutzmanagement

Technische Maßnahmen	Organisatorische Maßnahmen
Software-Lösungen für Datenschutzmanagement im Einsatz	Internes Datenschutzteam, externer Datenschutzbeauftragter (siehe § 7)
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung (z. B. Wiki, Intranet)	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
Sicherheitszertifizierung bzw. ISMS gemäß ISO 27001, BSI IT-Grundschutz oder VdS 10000	Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich
Technische Maßnahmen aus Sicherheitskonzepten werden gemäß ISMS gesteuert, überprüft und regelmäßig angepasst	Interner Informationssicherheitsbeauftragter, Internes Informationssicherheitsteam
Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DS-GVO nach
	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Es existieren folgende Maßnahmen zur lncident-Response-Management:

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Firewalls und regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
Einsatz von Spamfiltern und regelmäßige Aktualisierung	Aktualisierung Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
Einsatz von Virenscannern und regelmäßige Aktualisierung	Einbindung von DSB in Sicherheitsvorfälle und Datenpannen
Intrusion Detection System (lDS)	Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
Intrusion Prevention System (IPS)	Prozess und Verantwortlichkeilen zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen

Privacy by Design/Default

Es existieren folgende Maßnahmen zu datenschutzfreundlichen Voreinstellungen Management:

Technische Maßnahmen	Organisatorische Maßnahmen
Es werden keine nicht erforderlichen personenbezogene Daten erhoben	Es findet keine zweckfremde Verarbeitung statt
Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

4.4 Auftragskontrolle (Outsourcing an Dritte)

Der Auftragnehmer setzt keine Dienstleister im Sinne einer Auftragsverarbeitung ein.

4.5 Durchführung der Fernwartung

Die Datenschutzkonformität der Fernwartung ist dadurch sichergestellt, dass:

- der direkte Zugriff auf die Systeme aus dem Internet nicht möglich ist,
- alle Kommunikationskanäle über SSL verschlüsselt sind,
- ein Benutzer- und Rollenkonzept vorhanden ist, das auf dem Least Privilege Prinzip basiert,
- die einzelnen Services in Docker keinen Shell bzw. Konsolenzugriff erlauben,
- der Zugriff auf das lokale IT-System ausschließlich über ein VPN möglich ist

und

- der Zugriff über VPN nur mit personalisierten RSA-Token möglich ist.
- in der VPN-Verbindung ist nur das SSH-Protokoll freigeschaltet
- in der SSH-Session ist nur ein Server der Umgebung erreichbar.
- Der SSH-Zugriff auf den Server ist nur mit personalisierten SSH-Key möglich.

Weiter werden Zugriffe zur Fernwartung wie folgt protokolliert:

- Die Zeiträume der Zugriffe auf das VPN-Portal werden durch Speicherung der Login- und Logout-Zeiten, dem zugehörigen VPN-Profil und der IP-Adresse des VPN-Users auf einem Syslogserver protokolliert.

Anlage 2
Weitere weisungsberechtigte Personen des Auftraggebers

Vorname(n) u Nachname(n)	
und/ oder Funktion(en)	
und/oder Abteilung(en)	
Rufnummer(n)	
Emailadresse(n)	

Vorname(n) u Nachname(n)	
und/ oder Funktion(en)	
und/oder Abteilung(en)	
Rufnummer(n)	
Emailadresse(n)	

Vorname(n) u Nachname(n)	
und/ oder Funktion(en)	
und/oder Abteilung(en)	
Rufnummer(n)	
Emailadresse(n)	

Vorname(n) u Nachname(n)	
und/ oder Funktion(en)	
und/oder Abteilung(en)	
Rufnummer(n)	
Emailadresse(n)	

(bitte ausfüllen oder streichen!)