Auftragsverarbeitungsvertrag (AVV)

zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

zwischen

den Gesundheitsämtern des Landes Schleswig-Holstein:

Stadt Flensburg
Gesundheitsdienste
Norderstr. 58 - 60
24939 Flensburg
(0461) 85-2602-0
FAX 85-2819
E-Mail: gesundheitsdienste@flensburg.de

Stadt Kiel
Amt für Gesundheit
Fleethörn 18 - 24
24103 Kiel
(0431) 901-0
FAX 901-62113
E-Mail: gesundheitsamt@kiel.de

Hansestadt Lübeck
Gesundheitsamt
Sophienstr. 2 - 8
23560 Lübeck
(0451) 122-5315-0
FAX 122-5390
E-Mail: gesundheitsamt@luebeck.de

Stadt Neumünster
Der Oberbürgermeister
Fachdienst Gesundheit
Meßtorffweg 8
24534 Neumünster
(04321) 942-2810-0
FAX 942-2800
E-Mail: fachdienst.gesundheit@neumuenster.de

Kreis Dithmarschen
Fachdienst Gesundheit, Betreuung und Projektplanung
Esmarchstr. 50
25746 Heide
(0481) 785-4900
FAX 785-4931
E-Mail: fd-gesundheitsschutz@dithmarschen.de

Kreis Herzogtum Lauenburg
Fachdienst Gesundheit
Barlachstr. 4
23909 Ratzeburg
(04541) 888-380-0
FAX 888-259
E-Mail: gesundheitsdienste@kreis-rz.de

Kreis Nordfriesland
Fachdienst Gesundheit
Damm 8
25813 Husum
(04841) 67-711
FAX 67-89 44 15
E-Mail: gesundheitsamt@nordfriesland.de

Kreis Ostholstein
Fachdienst Gesundheit
Holstenstr. 52
23701 Eutin
(04521) 788-0
FAX 788-188
E-Mail: gesundheitsamt@kreis-oh.de

Kreis Pinneberg
Fachdienst Gesundheit
Kurt-Wagener-Str. 11
25337 Elmshorn
(04121) 4502-0
FAX 4502-93510
E-Mail: gesundheitsamt@kreis-pinneberg.de

Kreis Plön
Amt für Gesundheit
Hamburger Straße 17-18
24306 Plön
(04522) 743-531
FAX 743-467
E-Mail: gesundheitsamt@kreis-ploen.de

Kreis Rendsburg-Eckernförde
Fachdienst Gesundheitsdienste
Kaiserstr. 8
24768 Rendsburg
(04331) 202-238-0
FAX 202-565
E-Mail: gesundheit@kreis-rd.de

Kreis Schleswig-Flensburg
Fachdienst Gesundheit
Moltkestr. 22-26
24837 Schleswig
(04621) 810-20-0
FAX 810-50
E-Mail: gesundheitsamt@schleswig-flensburg.de

Kreis Segeberg
Fachdienst Gesundheit
Hamburger Str. 30
23795 Bad Segeberg
(04551) 951-342-0
FAX 951-301
E-Mail: gesundheit@kreis-se.de

Kreis Steinburg
Gesundheitsamt
Viktoriastraße 17a
25524 Itzehoe
(04821) 69-390-0
FAX 69-403
E-Mail: gesundheitsamt@steinburg.de

Kreis Stormarn
Fachdienst Gesundheit
Reimer-Hansen-Str. 3
23843 Bad Oldesloe
(04531) 160-1282-0
FAX 160-1626
E-Mail: gesundheitsamt@kreis-stormarn.de

und

dem Ministerium für Soziales, Gesundheit, Jugend, Familie und Senioren des Landes Schleswig-Holstein
Adolf-Westphal-Straße 4
24143 Kiel
(0431) 988-0
FAX 988-5416
E-Mail Poststelle@sozmi.landsh.de

nachfolgend Auftraggeber genannt

und

der Kassenärztliche Vereinigung Schleswig-Holstein
Bismarckallee 1-6
23795 Bad Segeberg

nachfolgend Auftragnehmerin genannt

Inhaltsverzeichnis

§ 1 Definitionen

Es gelten die Begriffsbestimmungen der Datenschutz-Grundverordnung (DS-GVO), der Sozialgesetzbücher (SGB I-XII), des Gesetzes gegen den unlauteren Wettbewerb (UWG) und des Telemediengesetzes (TMG) sowie des Landesdatenschutzgesetzes (Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Daten LDSG).

Weiterhin gelten folgende Begriffsbestimmungen für in diesen Regelungen nicht enthaltene Begriffe:

(1) Weisung
Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) der Auftragnehmerin mit personenbezogenen Daten gerichtete schriftliche Anordnung der Auftraggeber.

(2) Unterauftragnehmer
Von der Auftragnehmerin beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmerin zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber den Auftraggebern benötigt wird.

(3) Verarbeitung im Auftrag
Verarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch eine Auftragnehmerin im Auftrag der Auftraggeber.

§ 2 Gegenstand und Dauer der Vereinbarung

(1) Diese Vereinbarung regelt im Folgenden die Verfahren bei von der Auftragnehmerin durchzuführenden Tätigkeit („Auftragsverarbeitung").

Art und Umfang der durchzuführenden Tätigkeit:

Zur Erfüllung des dem jeweiligen örtlich zuständigen öffentlichen Gesundheitsdienst (ÖGD) gesetzlich zugewiesenen Auftrages gemäß Infektionsschutzgesetz wird die Auftragnehmerin beauftragt, die Testungen für den Nachweis des Vorliegens einer Infektion mit dem Coronavirus SARS-COV2 zu übernehmen und die technischen Mittel zur Verwaltung der erhobenen Daten bereitzustellen. Soweit erforderlich kann die Beauftragung Dritter unter Einhaltung datenschutzrechtlicher Vorgaben zur Auftragsverarbeitung erfolgen.

(2) Auftragsverarbeitung:
Die Auftragnehmerin ist befugt personenbezogene Daten oder Sozialdaten, die die Auftraggeber als verantwortliche Stellen zur Verfügung stellen, ausschließlich zum Zwecke der Erfüllung dieser Vereinbarung und nach den Weisungen der Auftraggeber gemäß Art. 4 Nr. 2 und Art. 28 DS-GVO, den einschlägigen Bestimmungen der Sozialgesetzbücher und des Bundesdatenschutzgesetzes ("BDSG") sowie den Landesdatenschutzgesetzen ("LDSG") zu verarbeiten. Die Auftraggeber bleiben die für die Datenverarbeitung verantwortliche Stelle und sind für die Rechtmäßigkeit der vertragsgemäßen Verarbeitung der personenbezogenen Daten verantwortlich.

(3) Das Auftragsverhältnis wird mit Unterzeichnung dieses Auftragsverarbeitungsvertrages geschlossen bzw. bestätigt. Grundlage für die Testungen bildet die Rechtsverordnung des Bundes zum Anspruch auf bestimmte Testungen für den Nachweis des Vorliegens einer Infektion mit dem Coronavirus SARS-CoV2 in der jeweils aktuellen Fassung. Die Laufzeit dieses Vertrages richtet sich nach der Entwicklung des Infektionsgeschehens. Sobald die

Feststellung der epidemischen Lage von nationaler Tragweite nach § 5 Absatz 1 Satz 2 Infektionsschutzgesetz für beendet erklärt wird, erfolgt lediglich die zur Abwicklung bereits vorgenommener Testungen erforderliche Datenverarbeitung. Es gelten die gesetzlichen Regelungen, soweit sich aus den Bestimmungen dieses Vertrages nicht darüberhinausgehende Verpflichtungen ergeben. Ein Sonderkündigungsrecht aus wichtigem Grund bleibt unberührt. Die Auftraggeber können den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß der Auftragnehmerin gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, die Auftragnehmerin eine Weisung der Auftraggeber nicht ausführen kann oder will oder die Auftragnehmerin Kontrollrechte der Auftraggeber vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

(4) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

§ 3 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen (Art. 28 Abs.3 S.1 DSGVO)

(1) Art der Verarbeitung:
Zum Zwecke der Durchführung von Testungen für den Nachweis des Vorliegens einer Infektion mit dem Coronavirus SARS-COV2 werden personenbezogene Daten von Testpersonen von den Beteiligten verarbeitet. Zur Erfüllung der Aufgaben der Verfolgung des Infektionsgeschehens und gemäß den Bestimmungen des Infektionsschutzgesetzes werden die erforderlichen Daten verarbeitet und soweit erforderlich an die an dem Prozess beteiligten Stellen weitergeleitet.
Die Auftraggeber bedienen sich der technischen Mittel, die durch die Auftragnehmerin zur Verfügung gestellt werden, um die notwendigen Testungen abzuwickeln. Hierzu hat die Auftragnehmerin ein „Eingabeportal" entwickelt auf das die Auftraggeber mittels sicherer Authentifizierung Zugriff nehmen. Durch die Mitarbeiter der Auftraggeber werden die Daten der Testpersonen direkt in das System eingegeben. Durch ein Rollen- und Rechtekonzept werden spezifische Berechtigungen festgelegt und systemseitig gesteuert. Die sich anschließende systemseitige Datenverarbeitung stellt die Auftragnehmerin auf Grundlage dieser vertraglichen Vereinbarung sicher. Die für die Testung eingerichteten Testzentren haben Zugriff auf die Inhalte dieses Erfassungssystems und die Mitarbeiter können die erforderlichen personenbezogenen Informationen sowie den zuständigen Auftraggeber aus diesen Daten entnehmen. Die Auftragnehmerin verantwortet den Aufbau inklusive Wahl des Ortes der Testzentren und veranlasst das Tätigwerden entsprechend qualifizierten Personals in den jeweiligen Testzentren. Ausschließlich bei Erscheinen der Testperson nehmen die Mitarbeiter des Testzentrums Zugriff auf die jeweiligen relevanten Daten zu der Testperson und führen die Testung durch. Nach durchgeführter Testung erfolgt die Weitergabe des Probenmaterials für die Diagnostik zum Erregernachweis SARS-COV2 an die von der KVSH beauftragten Labore.

Nach entsprechender Auswertung der Probenentnahme in den Laboren soll die Erfassung der Testergebnisse in einem von der Auftragnehmerin bereitgestellten „Ergebniserfassungssystem" erfolgen. Hierfür entwickelt die Auftragnehmerin ein System, dass die automatisierte Weitergabe aus den Systemen der Labore an das System der Auftragnehmerin ermöglicht. Auf die in diesem System zentral gespeicherten Daten nehmen die Auftraggeber mittels sicherer Authentifizierung Zugriff. Die Anforderungen an die für den Betrieb der technischen Systeme zu treffenden technischen und organisatorischen Maßnahmen ergeben sich aus § 9.

(2) Art der Daten:

Name, Geburtsdatum, Anschrift, Kontaktdaten: Handynummer oder sonstige telefonische Erreichbarkeit, Zeitpunkt der Testung, Ersttestung oder weitere Testung, durchführendes Testzentrum/durchführende Person, durchführendes Labor, Ergebnis der Laboruntersuchung (Befund), besondere Risikomerkmale (Gemeinschaftseinrichtung, Pflege- oder Wohneinrichtung, medizinische Einrichtung), Grund der Testung nach RVO (Klassifizierung §§ 2-4 der RVO), Angaben zu Auslandsaufenthalt, Abrechnungsgrundlage (RVO, Sondervereinbarung), Angaben zur erteilten Einwilligung in die Benachrichtigung Corona Warn-App, Kostenträger, Angabe PLZ des zuständigen Gesundheitsamtes

(3) Kategorien betroffener Personen:

a. Patienten/innen /Testpersonen
b. Ärzte/innen
c. Mitarbeiter KVSH
d. Mitarbeiter Testzentrum
e. Mitarbeiter Land SH
f. Mitarbeiter der Auftraggeber
g. Labore

§ 4 Rechte und Pflichten der Auftraggeber

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach ergänzend dokumentierter Weisung der Auftraggeber.

(2) 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 sind allein die Auftraggeber verantwortlich. Gleichwohl ist die Auftragnehmerin verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an die Auftraggeber gerichtet sind, unverzüglich an diese weiterzuleiten.

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

(4) Die Auftraggeber sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen der Auftragnehmerin vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

(5) Die Auftraggeber stellen sicher, dass die aus Art. 32 DS-GVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung eingehalten werden.

(6) Mündliche Informationen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

§ 5 Kontrollrechte der Auftraggeber

(1) Die Auftraggeber haben die Auftragnehmerin unter dem Aspekt ausgewählt, dass diese hinreichend Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen

der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Sie dokumentiert das Ergebnis ihrer Auswahl.

Hierfür kann sie beispielsweise

- datenschutzspezifische Zertifizierungen oder Datenschutzsiegel und -prüfzeichen berücksichtigen,
- schriftliche Selbstauskünfte der Auftragnehmerin einholen (vergl. auch Anlage 2),
- sich ein Testat eines Sachverständigen vorlegen lassen oder
- sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zur Auftragnehmerin stehen darf, von der Einhaltung der vereinbarten Regelungen überzeugen.

(2) Liegt ein Verstoß der Auftragnehmerin oder der bei ihr im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten der Auftraggeber oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs bei der Auftragnehmerin sollte auch hierbei weitestgehend vermieden werden.

(3) Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch die Auftraggeber im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags wird von der Auftragnehmerin unentgeltlich unterstützt. Insbesondere verpflichtet sich die Auftragnehmerin, die Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

§ 6 Weisungsbefugnisse der Auftraggeber

(1) Die Auftraggeber haben das Recht, Weisungen zu erteilen. Ergänzende Weisungen zu den technischen und organisatorischen Maßnahmen sind stets schriftlich oder in einem dokumentierten elektronischen Format zu erteilen. Die Auftragnehmerin ist verpflichtet, den Weisungen der Auftraggeber zur Verarbeitung von Daten uneingeschränkt zu folgen. Ist die Auftragnehmerin der Ansicht, dass eine Weisung gegen gesetzliche Vorschriften und/oder diesen Vertrag verstößt, so ist die Auftragnehmerin verpflichtet, die Auftraggeber hierauf unverzüglich hinzuweisen, sowie berechtigt, die Ausführung der Weisung bis zu einer schriftlichen Bestätigung der Weisung durch die Auftraggeber auszusetzen. Weisungen der Auftraggeber dürfen nur durch deren weisungsberechtigte Personen erfolgen.

(2) Mündliche Weisungen werden die Auftraggeber unverzüglich schriftlich oder in einem dokumentierten elektronischen Format (Textform) bestätigen. Die Auftragnehmerin notiert sich Datum, Uhrzeit und Person, welche die mündliche Weisung erteilte sowie den Grund der Weisung.

§ 7 Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin handelt ausschließlich im Rahmen der getroffenen Vereinbarung und nach Weisungen der Auftraggeber, sofern sie nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem die Auftragnehmerin unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt die Auftragnehmerin den Auftraggebern

diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 S. 2 lit. a DSGVO).

(2) Personenbezogene oder sonstige Daten, die im Rahmen der Erfüllung dieses Vertrages bekannt geworden sind, dürfen nur für Zwecke der Durchführung dieses Vertrages verwendet werden.

(3) Die Auftragnehmerin sichert die Wahrung der Vertraulichkeit und des Daten- sowie Sozialgeheimnisses gemäß Art. 28 Abs. 3 Satz 2 lit. b, 29, 32 Abs. 4 DS-GVO, § 35 SGB I. zu. Die Auftragnehmerin setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit und zur Geheimhaltung unter Hinweis auf die rechtlichen Folgen einer Pflichtverletzung, insbesondere nach § 203 Abs. 4 StGB, nachweisbar verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Dies umfasst die Verpflichtung zur Geheimhaltung auch über das bestehende Dienst- oder Beschäftigungsverhältnis hinaus. (Art. 28 Abs. 3 S. 2 lit. B und Art. 29 DSGVO). Die Auftragnehmerin überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in ihrem Betrieb.

(4) Die Auftragnehmerin ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der Auftraggeber geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen.

(5) Die Auftragnehmerin trennt – soweit dies technisch möglich ist - die verarbeiteten personenbezogenen Daten von sonstigen bei ihr gespeicherten eigenen Datenbeständen oder Datenbeständen Dritter. Sofern eine Trennung nicht oder nur unvollständig umsetzbar ist, trifft die Auftragnehmerin ergänzende technische und organisatorische Maßnahmen. Die Datenverarbeitung in Privatwohnungen ist nur gestattet sofern der Zugriff über hinreichend sichere, dem Stand der Technik entsprechende Anbindungen an die IT-Infrastruktur der Auftragnehmerin realisiert wird und eine Datenspeicherung ausschließlich auf Systemen der Auftragnehmerin erfolgt.

(6) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch die Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen der Auftraggeber hat die Auftragnehmerin im notwendigen Umfang unentgeltlich mitzuwirken und die Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO).

(7) Die Auftragnehmerin wird die Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine von den Auftraggebern erteilte Weisung ihrer Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Die Auftragnehmerin ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bei den Auftraggebern nach Überprüfung bestätigt oder geändert wird.

(8) Die Auftragnehmerin erklärt sich damit einverstanden, dass die Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt sind, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch von den Auftraggebern beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Die Auftragnehmerin gestattet der zuständigen Rechts- und Datenschutz-aufsichtsbehörde der Auftraggeber Prüfungshandlungen, die sich auf diesen Vertrag beziehen, in ihren Geschäftsräumen vorzunehmen.

(9) Die Auftragnehmerin benennt einen Datenschutzbeauftragten nach Maßgabe des Art. 37 DS-GVO, der seine Tätigkeit entsprechend Art. 38 und 39 DS-GVO ausübt. Der derzeitige Datenschutzbeauftragte der Auftragnehmerin wird in der **Anlage 1** benannt. Sofern kein Datenschutzbeauftragter bei der Auftragnehmerin benannt ist, benennt die Auftragnehmerin den Auftraggebern einen Ansprechpartner. Ein Wechsel des Datenschutzbeauftragten oder des Ansprechpartners ist den Auftraggebern unverzüglich schriftlich mitzuteilen.

(10) Die Auftragnehmerin selbst führt für die Verarbeitung ein Verzeichnis der bei ihr stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DS-GVO. Sie stellt auf Anforderung der Auftraggeber die für die Übersicht nach Art. 30 DS-GVO notwendigen Angaben zur Verfügung. Des Weiteren stellt sie das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

§ 8 Unterauftragsverhältnisse

(1) Die Einschaltung von Unterauftragnehmern ist unter Einhaltung der nachfolgenden Bedingungen zulässig. Die Unterauftragsverhältnisse ergeben sich aus der Aufstellung der **Anlage 2**.

(2) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen, und bei denen ein Zugriff auf Sozialdaten nicht ausgeschlossen werden kann. Nicht hierzu gehören Nebenleistungen, die die Auftragnehmerin z.B. als Telekommunikationsdienstleister, dem Postgeheimnis unterliegende Post-/Transportdienstleistungen, Gebäudereinigung sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Die Auftragnehmerin ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der Daten der Auftraggeber auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(3) Die Auftragnehmerin darf Unterauftragnehmer nur beauftragen, wenn sie die Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert, wodurch die Auftraggeber die Möglichkeit erhalten, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch darf nur aus wichtigem Grund erfolgen.

(4) Die Auftragnehmerin trägt dafür Sorge, dass sie die Unterauftragnehmer unter besonderer Berücksichtigung der Eignung auswählt und technische und organisatorische Maßnahmen ergreift, die dem Grundsatz der Erforderlichkeit und der Datenminimierung hinreichend Rechnung tragen.

(5) Es erfolgt keine Beauftragung von Unterauftragnehmern in Drittstaaten außerhalb der EU/des EWR.

(6) Die Auftragnehmerin hat nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggebern und Auftragnehmerin auch gegenüber Unterauftragnehmern gelten. Insbesondere müssen die Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragnehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(7) Der Vertrag mit dem Unterauftragnehmer muss schriftlich abgefasst werden, was auch in einem dokumentierten elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

(8) Die Weiterleitung von Daten an den Unterauftragnehmer ist erst zulässig, wenn der Unterauftragnehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

(9) Die Auftragnehmerin hat die Einhaltung der Pflichten des Unterauftragnehmers zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und den Auftraggebern auf Verlangen zugänglich zu machen.

§ 9 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 S. 2 lit. c DSGVO)

(1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Einzelheiten hierzu beschreibt die **Anlage 3.**

(2) Die Auswahl der technischen und organisatorischen Maßnahmen erfolgt passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse bei der Auftragnehmerin durch Anwendung eines Datenschutz- und Informationsmanagements.

(3) Es gibt ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung.

(4) Die Maßnahmen bei der Auftragnehmerin können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Sicherheitsziele, die in **Anlage 3** beschrieben sind, nicht unterschreiten. Sofern eine Anpassung der technischen und organisatorischen Maßnahmen – auch bei Beibehaltung oder Verbesserung der vereinbarten Sicherheitsziele – die Beauftragung eines außerhalb der EU oder EWR ansässigen Unterauftragnehmers einschließt, sind die Auftraggeber über diese geplante Änderung rechtzeitig zu informieren.

(5) Der Datenfluss sowie die Spezifikationen und die Datensatzbeschreibung sind geeignet zu dokumentieren.

§ 10 Speicherung, Löschung und Rückgabe von Daten (Art. 28 Abs. 3 DSGVO)

(1) Die Auftragnehmerin hat nur nach Weisung der Auftraggeber die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an die Auftragnehmerin zwecks der Geltendmachung seiner gesetzlich vorgesehenen Betroffenenrechte wenden sollte, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeber weiterleiten. Die Auftragnehmerin speichert

die Informationen nur so lange wie dies zur Erfüllung der durch diesen Vertrag übertragenen Aufgaben erforderlich ist.

(2) Sind die Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer betroffenen Person verpflichtet, deren in der DSGVO vorgesehenen Betroffenenansprüchen nachzukommen, wird die Auftragnehmerin die Auftraggeber dabei unentgeltlich unterstützen, diese Informationen bereitzustellen, vorausgesetzt, die Auftraggeber haben die Auftragnehmerin hierzu schriftlich aufgefordert.

(3) Bei Störungen im Betriebsablauf, etwa bei Hard- und Softwareaustausch hat die Auftragnehmerin dafür zu sorgen, dass keine Daten Dritten offenbart werden.

(4) Nach Abschluss der vertraglichen Arbeiten oder zuvor nach Aufforderung durch die Auftraggeber – spätestens mit Beendigung des Auftrags – hat die Auftragnehmerin sämtliche in ihren Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, den Auftraggebern auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Gleiches gilt für Test- und Ausschussmaterial. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch die Auftragnehmerin entsprechend der jeweiligen gesetzlichen Aufbewahrungsfristen, insbesondere auch aus § 6 LDSG SH, über das Vertragsende hinaus aufzubewahren.

§ 11 Mitteilungspflichten der Auftragnehmerin bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten (Art. 28 Abs. 3 S. 2 lit. f DSGVO)

Die Auftragnehmerin teilt den Auftraggebern unverzüglich Störungen, Verstöße der Auftragnehmerin oder der bei ihr beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten im Umfang des Art. 33 III lit. a - d DSGVO mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten der Auftraggeber nach Art. 33 und Art. 34 DSGVO. Die Auftragnehmerin sichert zu, die Auftraggeber erforderlichenfalls bei ihren Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für die Auftraggeber darf die Auftragnehmerin nur nach vorheriger Weisung durchführen. Die Auftragnehmerin unterstützt die Auftraggeber im Hinblick auf Art.32-36 DSGVO bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Die Auftragnehmerin hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten der Auftraggeber mitzuwirken. Die Auftragnehmerin wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Sie hat den Auftraggebern alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen

§ 12 Anzeigepflicht bei der Aufsichtsbehörde

Voraussetzung für die Datenverarbeitung und -nutzung ist, dass die Auftraggeber sowie ggf. die Auftragnehmerin die Auftragsverarbeitung schriftlich durch Vorlage der getroffenen Vereinbarungen der zuständigen Aufsichtsbehörde anzeigt.

§ 13 Leistungsort

Die Auftragnehmerin wird die vertraglichen Leistungen in der Europäischen Union oder im Europäischen Wirtschaftsraum erbringen, etwaige Unterauftragnehmer an den mit den Auftraggebern vereinbarten Leistungsstandorten der Unterauftragnehmer in der Europäischen Union oder im Europäischen Wirtschaftsraum.

§ 14 Haftung

(1) Die Auftragnehmerin haftet gegenüber den Auftraggebern im Rahmen der gesetzlichen Bestimmungen für Schäden, die infolge schuldhaften Verhaltens gegen Datenschutzbestimmungen und gegen diese Datenschutzvereinbarung entstehen. Ebenso haftet sie für schuldhaftes Verhalten ihrer Unterauftragnehmer sowie deren Unterauftragnehmer.

(2) Auftraggeber und Auftragnehmerin haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

§ 15 Gerichtsstand und Sonstiges

(1) Es gilt deutsches Recht.

(2) Gerichtsstand ist der Sitz der Auftragnehmerin.

(3) Ist eine oder sind mehrere Bestimmungen dieser Vereinbarung unwirksam, so wird hiervon die Wirksamkeit der übrigen Vereinbarung nicht berührt. Im Falle der Unwirksamkeit einer Bestimmung dieser Vereinbarung gilt anstelle der unwirksamen eine wirksame Bestimmung als vereinbart, die so weit wie möglich dem entspricht, was die Parteien gewollt haben oder gewollt hätten, wenn sie die Unwirksamkeit erkannt hätten.

(4) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Änderungen des Verarbeitungsgegenstandes, Verfahrensänderungen sowie Abweichungen von den sonstigen getroffenen Festlegungen sind schriftlich oder ein dokumentiertes elektronisches Format zu vereinbaren.

(6) Die nachstehend aufgeführten Anlagen sind Bestandteil dieser Vereinbarung:

Anlage 1: Nennung des Datenschutzbeauftragten
Anlage 2: Aufstellung der Unterauftragsverhältnisse
Anlage 3: Technische und organisatorische Maßnahmen

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Flensburg, den

_____

Gesundheitsdienste der Stadt Flensburg

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Kiel, den

_____

Amt für Gesundheit Stadt Kiel

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Lübeck, den

_____

Gesundheitsamt der Hansestadt Lübeck

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Neumünster, den

Stadt Neumünster
Der Oberbürgermeister
Fachdienst Gesundheit

_____

(Dr. Olaf Tauras)
Oberbürgermeister

Heide, den

Fachdienst Gesundheit, Betreuung und
Projektplanung Dithmarschen

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Ratzeburg, den

_____

Fachdienst Gesundheit
Kreis Herzogtum Lauenburg

Husum, den

_____

Fachdienst Gesundheit Kreis Nordfriesland

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Eutin, den

_____

Fachdienst Gesundheit Kreis Ostholstein

Pinneberg, den

_____

Fachdienst Gesundheit Kreis Pinneberg

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Plön, den

_____

Amt für Gesundheit Kreis Plön

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Rendsburg, den

_____

Fachdienst Gesundheitsdienste
Kreis Rendsburg-Eckernförde

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Schleswig, den

_____

Fachdienst Gesundheit
Kreis Schleswig-Flensburg

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Bad Segeberg, den

_____

Fachdienst Gesundheit Kreis Segeberg

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Itzehoe, den

_____

Gesundheitsamt Kreis Steinburg

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Bad Oldesloe, den

_____

Fachdienst Gesundheit Kreis Stormarn

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Kiel, den

_____

Ministerium für Soziales, Gesundheit,
Jugend, Familie und Senioren des Landes
Schleswig-Holstein

Auftragsverarbeitungsvertrag (AVV) zur Durchführung der Testungen von COVID-19 Patientinnen/Patienten und zur Bereitstellung der technischen Mittel

Bad Segeberg, den

_____

Kassenärztliche Vereinigung
Schleswig-Holstein

Anlage 1:

Nennung des Datenschutzbeauftragten der Auftragnehmerin

zum Auftragsverarbeitungsvertrag

zwischen

den Gesundheitsämtern des Landes Schleswig-Holstein:

Stadt Flensburg
Gesundheitsdienste
Norderstr. 58 - 60
24939 Flensburg
(0461) 85-2602-0
FAX 85-2819
E-Mail: gesundheitsdienste@flensburg.de

Stadt Kiel
Amt für Gesundheit
Fleethörn 18 - 24
24103 Kiel
(0431) 901-0
FAX 901-62113
E-Mail: gesundheitsamt@kiel.de

Hansestadt Lübeck
Gesundheitsamt
Sophienstr. 2 - 8
23560 Lübeck
(0451) 122-5315-0
FAX 122-5390
E-Mail: gesundheitsamt@luebeck.de

Stadt Neumünster
Der Oberbürgermeister
Fachdienst Gesundheit
Meßtorffweg 8
24534 Neumünster
(04321) 942-2810-0
FAX 942-2800
E-Mail: fachdienst.gesundheit@neumuenster.de

Kreis Dithmarschen
Fachdienst Gesundheit, Betreuung und Projektplanung
Esmarchstr. 50
25746 Heide
(0481) 785-4900
FAX 785-4931
E-Mail: fd-gesundheitsschutz@dithmarschen.de

Kreis Herzogtum Lauenburg
Fachdienst Gesundheit
Barlachstr. 4
23909 Ratzeburg
(04541) 888-380-0
FAX 888-259
E-Mail: gesundheitsdienste@kreis-rz.de

Kreis Nordfriesland
Fachdienst Gesundheit
Damm 8
25813 Husum
(04841) 67-711
FAX 67-89 44 15
E-Mail: gesundheitsamt@nordfriesland.de

Kreis Ostholstein
Fachdienst Gesundheit
Holstenstr. 52
23701 Eutin
(04521) 788-0
FAX 788-188
E-Mail: gesundheitsamt@kreis-oh.de

Kreis Pinneberg
Fachdienst Gesundheit
Kurt-Wagener-Str. 11
25337 Elmshorn
(04121) 4502-0
FAX 4502-93510
E-Mail: gesundheitsamt@kreis-pinneberg.de

Kreis Plön
Amt für Gesundheit
Hamburger Straße 17-18
24306 Plön
(04522) 743-531
FAX 743-467
E-Mail: gesundheitsamt@kreis-ploen.de

Kreis Rendsburg-Eckernförde
Fachdienst Gesundheitsdienste
Kaiserstr. 8
24768 Rendsburg
(04331) 202-238-0
FAX 202-565
E-Mail: gesundheit@kreis-rd.de

Kreis Schleswig-Flensburg
Fachdienst Gesundheit
Moltkestr. 22-26
24837 Schleswig
(04621) 810-20-0
FAX 810-50
E-Mail: gesundheitsamt@schleswig-flensburg.de

Kreis Segeberg
Fachdienst Gesundheit
Hamburger Str. 30
23795 Bad Segeberg
(04551) 951-342-0
FAX 951-301
E-Mail: gesundheit@kreis-se.de

Kreis Steinburg
Gesundheitsamt
Viktoriastraße 17a
25524 Itzehoe
(04821) 69-390-0
FAX 69-403
E-Mail: gesundheitsamt@steinburg.de

Kreis Stormarn
Fachdienst Gesundheit
Reimer-Hansen-Str. 3
23843 Bad Oldesloe
(04531) 160-1282-0
FAX 160-1626
E-Mail: gesundheitsamt@kreis-stormarn.de

und

dem Ministerium für Soziales, Gesundheit, Jugend, Familie und Senioren des Landes Schleswig-Holstein
Adolf-Westphal-Straße 4
24143 Kiel
(0431) 988-0
FAX 988-5416
E-Mail Poststelle@sozmi.landsh.de

(Auftraggeber)

und

Kassenärztliche Vereinigung Schleswig-Holstein
Bismarckallee 1-6
23795 Bad Segeberg

(Auftragnehmerin)

Der derzeitige Datenschutzbeauftragte der Auftragnehmerin wird im Folgenden benannt. Die Auftragnehmerin gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DS-GVO erfüllt werden.

Name	Standort	Telefon	E-Mail-Adresse
Tom Brümmer	Bismarckallee 1-6, 23895 Bad Segeberg	04551/883-474	datenschutz@kvsh.de

Anlage 2:

Unterauftragsverhältnisse

zum Auftragsverarbeitungsvertrag

zwischen

den Gesundheitsämtern des Landes Schleswig-Holstein:

Stadt Flensburg
Gesundheitsdienste
Norderstr. 58 - 60
24939 Flensburg
(0461) 85-2602-0
FAX 85-2819
E-Mail: gesundheitsdienste@flensburg.de

Stadt Kiel
Amt für Gesundheit
Fleethörn 18 - 24
24103 Kiel
(0431) 901-0
FAX 901-62113
E-Mail: gesundheitsamt@kiel.de

Hansestadt Lübeck
Gesundheitsamt
Sophienstr. 2 - 8
23560 Lübeck
(0451) 122-5315-0
FAX 122-5390
E-Mail: gesundheitsamt@luebeck.de

Stadt Neumünster
Der Oberbürgermeister
Fachdienst Gesundheit
Meßtorffweg 8
24534 Neumünster
(04321) 942-2810-0
FAX 942-2800
E-Mail: fachdienst.gesundheit@neumuenster.de

Kreis Dithmarschen
Fachdienst Gesundheit, Betreuung und Projektplanung
Esmarchstr. 50
25746 Heide
(0481) 785-4900
FAX 785-4931
E-Mail: fd-gesundheitsschutz@dithmarschen.de

Kreis Herzogtum Lauenburg
Fachdienst Gesundheit
Barlachstr. 4
23909 Ratzeburg
(04541) 888-380-0
FAX 888-259
E-Mail: gesundheitsdienste@kreis-rz.de

Kreis Nordfriesland
Fachdienst Gesundheit
Damm 8
25813 Husum
(04841) 67-711
FAX 67-89 44 15
E-Mail: gesundheitsamt@nordfriesland.de

Kreis Ostholstein
Fachdienst Gesundheit
Holstenstr. 52
23701 Eutin
(04521) 788-0
FAX 788-188
E-Mail: gesundheitsamt@kreis-oh.de

Kreis Pinneberg
Fachdienst Gesundheit
Kurt-Wagener-Str. 11
25337 Elmshorn
(04121) 4502-0
FAX 4502-93510
E-Mail: gesundheitsamt@kreis-pinneberg.de

Kreis Plön
Amt für Gesundheit
Hamburger Straße 17-18
24306 Plön
(04522) 743-531
FAX 743-467
E-Mail: gesundheitsamt@kreis-ploen.de

Kreis Rendsburg-Eckernförde
Fachdienst Gesundheitsdienste
Kaiserstr. 8
24768 Rendsburg
(04331) 202-238-0
FAX 202-565
E-Mail: gesundheit@kreis-rd.de

Kreis Schleswig-Flensburg
Fachdienst Gesundheit
Moltkestr. 22-26
24837 Schleswig
(04621) 810-20-0
FAX 810-50
E-Mail: gesundheitsamt@schleswig-flensburg.de

Kreis Segeberg
Fachdienst Gesundheit
Hamburger Str. 30
23795 Bad Segeberg
(04551) 951-342-0
FAX 951-301
E-Mail: gesundheit@kreis-se.de

Kreis Steinburg
Gesundheitsamt
Viktoriastraße 17a
25524 Itzehoe
(04821) 69-390-0
FAX 69-403
E-Mail: gesundheitsamt@steinburg.de

Kreis Stormarn
Fachdienst Gesundheit
Reimer-Hansen-Str. 3
23843 Bad Oldesloe
(04531) 160-1282-0
FAX 160-1626
E-Mail: gesundheitsamt@kreis-stormarn.de

und

dem Ministerium für Soziales, Gesundheit, Jugend, Familie und Senioren des Landes Schleswig-Holstein
Adolf-Westphal-Straße 4
24143 Kiel
(0431) 988-0
FAX 988-5416
E-Mail Poststelle@sozmi.landsh.de

(Auftraggeber)

und

Kassenärztliche Vereinigung Schleswig-Holstein
Bismarckallee 1-6
23795 Bad Segeberg

(Auftragnehmerin)

Gemäß § 8 des Auftragsverarbeitungsvertrages zur Durchführung der Testungen von COVID-19 Patientinnen und Patienten und zur Bereitstellung der technischen Mittel bestehen folgende Unterauftragsverhältnisse:

1. DRK-Landesverband Schleswig-Holstein e.V., Klaus-Groth-Platz 1, 24105 Kiel
   - vertreten durch den alleinvertretungsberechtigten Vorstand Ralph Schmieder

2. Medizinische Klinik Borstel, Leibniz Lungenzentrum, Parkallee 35, 23845 Borstel
   - vertreten durch den Medizinischen Direktor

3. RKiSH, Rettungskooperation Schleswig-Holstein

4. Johanniter-Unfall-Hilfe e.V. Berlin, vertreten vom Regionalverband Schleswig-Holstien Süd/Ost, Bei der Gasanstalt 12, 23560 Lübeck
   - vertreten durch den hauptamtlichen Regionalvorstand Kai-Uwe Preuß

5. Labor Dr. Krause & Kollegen MVZ GmbH, Steenbeker Weg 23, 24106 Kiel
   - vertreten durch den vertretungsberechtigten Geschäftsführer Dr. med. Thomas Lorentz

Anlage 3:

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 S. 2 lit. c DSGVO

zum Auftragsverarbeitungsvertrag

zwischen

den Gesundheitsämtern des Landes Schleswig-Holstein:

Stadt Flensburg
Gesundheitsdienste
Norderstr. 58 - 60
24939 Flensburg
(0461) 85-2602-0
FAX 85-2819
E-Mail: gesundheitsdienste@flensburg.de

Stadt Kiel
Amt für Gesundheit
Fleethörn 18 - 24
24103 Kiel
(0431) 901-0
FAX 901-62113
E-Mail: gesundheitsamt@kiel.de

Hansestadt Lübeck
Gesundheitsamt
Sophienstr. 2 - 8
23560 Lübeck
(0451) 122-5315-0
FAX 122-5390
E-Mail: gesundheitsamt@luebeck.de

Stadt Neumünster
Der Oberbürgermeister
Fachdienst Gesundheit
Meßtorffweg 8
24534 Neumünster
(04321) 942-2810-0
FAX 942-2800
E-Mail: fachdienst.gesundheit@neumuenster.de

Kreis Dithmarschen
Fachdienst Gesundheit, Betreuung und Projektplanung
Esmarchstr. 50
25746 Heide
(0481) 785-4900
FAX 785-4931
E-Mail: fd-gesundheitsschutz@dithmarschen.de

Kreis Herzogtum Lauenburg
Fachdienst Gesundheit
Barlachstr. 4
23909 Ratzeburg
(04541) 888-380-0
FAX 888-259
E-Mail: gesundheitsdienste@kreis-rz.de

Kreis Nordfriesland
Fachdienst Gesundheit
Damm 8
25813 Husum
(04841) 67-711
FAX 67-89 44 15
E-Mail: gesundheitsamt@nordfriesland.de

Kreis Ostholstein
Fachdienst Gesundheit
Holstenstr. 52
23701 Eutin
(04521) 788-0
FAX 788-188
E-Mail: gesundheitsamt@kreis-oh.de

Kreis Pinneberg
Fachdienst Gesundheit
Kurt-Wagener-Str. 11
25337 Elmshorn
(04121) 4502-0
FAX 4502-93510
E-Mail: gesundheitsamt@kreis-pinneberg.de

Kreis Plön
Amt für Gesundheit
Hamburger Straße 17-18
24306 Plön
(04522) 743-531
FAX 743-467
E-Mail: gesundheitsamt@kreis-ploen.de

Kreis Rendsburg-Eckernförde
Fachdienst Gesundheitsdienste
Kaiserstr. 8
24768 Rendsburg
(04331) 202-238-0
FAX 202-565
E-Mail: gesundheit@kreis-rd.de

Kreis Schleswig-Flensburg
Fachdienst Gesundheit
Moltkestr. 22-26
24837 Schleswig
(04621) 810-20-0
FAX 810-50
E-Mail: gesundheitsamt@schleswig-flensburg.de

Kreis Segeberg
Fachdienst Gesundheit
Hamburger Str. 30
23795 Bad Segeberg
(04551) 951-342-0
FAX 951-301
E-Mail: gesundheit@kreis-se.de

Kreis Steinburg
Gesundheitsamt
Viktoriastraße 17a
25524 Itzehoe
(04821) 69-390-0
FAX 69-403
E-Mail: gesundheitsamt@steinburg.de

Kreis Stormarn
Fachdienst Gesundheit
Reimer-Hansen-Str. 3
23843 Bad Oldesloe
(04531) 160-1282-0
FAX 160-1626
E-Mail: gesundheitsamt@kreis-stormarn.de

und

dem Ministerium für Soziales, Gesundheit, Jugend, Familie und Senioren des Landes Schleswig-Holstein
Adolf-Westphal-Straße 4
24143 Kiel
(0431) 988-0
FAX 988-5416
E-Mail Poststelle@sozmi.landsh.de

(Auftraggeber)

und

Kassenärztliche Vereinigung Schleswig-Holstein
Bismarckallee 1-6
23795 Bad Segeberg

(Auftragnehmerin)

Inhaltsverzeichnis

1. Einleitung

Das vorliegende Dokument beschreibt die technischen und organisatorischen Maßnahmen zur Datensicherheit gem. Artikel 32 EU-Datenschutzgrundverordnung (DSGVO) für die automatisierte Verarbeitung oder Nutzung personenbezogener Daten.

Die KVSH verarbeitet in großem Umfang Gesundheitsdaten. Standardmäßig werden für alle Datenverarbeitungsprozesse die Datenschutzvorkehrungen für Daten mit hohem Schutzbedarf getroffen. In der Konsequenz erfolgt bei der Verarbeitung von Daten keine Unterscheidung in allgemeine und spezielle technische und organisatorische Maßnahmen. Bei der Modellierung des Datensicherheitsprozesses wird der BSI IT-Grundschutzstandard zugrunde gelegt. Ein dem Risiko angemessenes Schutzniveau wird unter Zugrundelegung vielfältiger Berücksichtigungsfaktoren sowie der Eintrittswahrscheinlichkeit und der Schwere der Risiken festgelegt.

Der Vorstand der KVSH hat sich in einer Leitlinie zur Anwendung des IT-Grundschutzstandards verpflichtet und hat die damit im Zusammenhang stehenden Aufgaben dem sogenannten Datenschutz und Informationssicherheits-Team übertragen. Hierüber ist ein Konzept erstellt worden und in Richtlinien werden die Einzelheiten der zu treffenden Maßnahmen festgelegt.
Die zentrale Kennwortverwaltung erfolgt im Active-Directory. Das Kennwort wird durch Admins auf Anforderung des Nutzers zurückgesetzt. Rücksetzung wird Protokolliert.

Private Geräte dürfen/können nicht mit dem Netzwerk verbunden werden. (Überwachung mit System MacMon)

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Die Verpflichtung zur Wahrung der Vertraulichkeit personenbezogener Daten ergibt sich aus Art. 5 Abs. 1 lit. f DS-GVO. In Bezug auf die zur Verarbeitung eingesetzten Systeme und Dienste sowie für die Auftragsverarbeiter und die Personen, die dem Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind, ergibt sie sich aus Art. 32 Abs. 1 lit. b DS-GVO. Ferner ergibt sie sich aus der Bindung an die Weisungen des Verantwortlichen (Art. 29, 32 Abs. 4 DSGVO), einer gesonderten Vertraulichkeitsverpflichtung gemäß Art. 28 Abs. 3 lit. b DSGVO und ggf. gesetzlichen Verschwiegenheitspflichten. Für Datenschutzbeauftragte ergibt sie sich zudem aus der Geheimhaltungspflicht nach Art. 38 Abs. 5 DSGVO. Unbefugte dürfen keinen Zugang zu den Daten haben und weder die Daten noch Geräte, mit denen diese verarbeitet werden, benutzen können (Art. 32 Abs. 1 lit. b DS-GVO, siehe auch ErwGr.39 Satz 12). Eine Verletzung der Vertraulichkeit ist insbesondere dann anzunehmen, wenn eine Verarbeitung personenbezogener Daten unbefugt erfolgt.

Die Mitarbeiter werden nach dem Verpflichtungsgesetz zur Geheimhaltung verpflichtet und die Vertraulichkeit wird durch Abgabe einer gesonderten Erklärung, die den Anforderungen der DS-GVO entspricht, sichergestellt.

2.1 Zutrittskontrolle

Ziel: Verhinderung unbefugten Zutritts zu Datenverarbeitungsanlagen

Das Rechenzentrum der KVSH befindet sich in Räumen, die von einem Überwachungsdienst betreut werden. Der technische Schutz ist gegeben durch eine Einbruchmeldeanlage, die auf die Alarmzentrale der Polizei aufgeschaltet ist.

Die Schließanlage hat mechatronische Schlüssel, sodass neben der mechanischen auch eine elektronische Steuerung der Schlösser erfolgt. Im Fall eines Schlüsselverlustes kann dadurch ein einzelner Schlüssel schnell aus der Schließberechtigung der Anlage herausgenommen und die notwendige Sicherheit wiederhergestellt werden. Die Mitarbeiter haben mit ihrem persönlichen Schlüssel ausschließlich dort Zutritt, wo sie ihn für ihre Tätigkeiten benötigen. Über die Elektronik in den Schlüsseln können diese Berechtigungen bei Bedarf angepasst werden.

Die Mitarbeiter sind durch eine Dienstanweisung zum Verschluss der Bürotüren verpflichtet. Externe Besucher werden zentral in Empfang genommen und Veranstaltungen finden in gesonderten Sitzungsräumen statt.

Alle Server sind in einem Serverraum mit zusätzlicher Zugangskontrolle und Alarmanlage untergebracht. Zutritt zu diesem Raum haben nur die IT-Administratoren, der Vorstand, sowie in Notfällen der Wachdienst und Einsatzkräfte der Feuerwehr; die Gewährleistung dafür bietet die Schlüsselkontrolle. Der Serverraum befindet sich im Erdgeschoss. In einem Protokollbuch werden Betretungen des Serverraums externer Dienstleister festgehalten. Bei jeder Türöffnung wird elektronisch in den Schlössern protokolliert, welcher Schlüssel wann die Tür geöffnet hat.

Die Datensicherung befindet sich in einem anderen Gebäudeabschnitt. Für das physikalische Löschen sensibler Daten wird ein spezielles Tool eingesetzt. Konkrete Vorgaben zur Datenlöschung sind in einem Konzept Datenvernichtung definiert.

Große zusammenhängende Datenmengen werden auf dem Speichersystem in eigenen Volumes angelegt. Für deren Löschung erfolgt eine Verschlüsselung der Datenblöcke mit einem temporären und nicht gespeicherten digitalen Schlüssel, der danach vernichtet wird. Anschließend werden die (verschlüsselten) Datenblöcke zur Überschreibung freigegeben.

Einzelne Dateien werden durch das Programm Secure Eraser (ASCOMP Software GmbH) oder ein gleichwertiges Programm gelöscht.

Ausgesonderte Festplatten werden von einem zertifizierten Entsorger vernichtet. Für die datenschutzgerechte Entsorgung von Ausdrucken mit personenbezogenen Daten gibt es ein bestimmtes Verfahren, das in dem Sicherheitskonzept „Sichere Datenvernichtung" geregelt ist.

Unterlagen, die personenbezogene Daten enthalten, werden in von einem Dienstleister bereitgestellten sicheren Behältern gesammelt und vom Gebäudemanagement zur Abholung durch den Dienstleister bereitgestellt.

Vor der Entsorgung eines Gerätes wird die Festplatte entnommen und vernichtet. Das Gerät wird durch den Servicepartner fachgerecht entsorgt.

2.2 Zugangskontrolle

Ziel: Verhinderung des Zugangs Unbefugter zu Datenverarbeitungssystemen

Der Zugang zu den Arbeitsplatzrechnern bzw. den Laptops der Mitarbeiter und damit zum Netzwerk erfolgt durch ein Passwort. Die Richtlinie Authentifizierung hat folgende Vorgaben: Mindestens 8 Zeichen, komplex (d.h. es müssen Groß- und Kleinbuchstaben, Zahlen und Zeichen verwendet werden), die letzten drei verwendeten Passwörter dürfen nicht wiederverwendet werden.

Diese Vorgaben sind durch die Konfiguration einer Sicherheitsrichtlinie der auf allen Rechnern installierten Standardsoftware (Betriebssysteme Windows Server 2012 bzw. 2016 und Windows 7/10) und durch die detaillierte Rechtevergabe für den Zugriff auf einzelne Ordner und Programme garantiert. Hinweise zum sicheren Umgang mit Passwörtern sind in die Richtlinie Authentifizierung aufgenommen und durch die Sicherheitsrichtlinien der Arbeitsplatz PCs technisch umgesetzt.
Nach einer gewissen Zeit werden die Zugänge sowohl bei Arbeitsplatzrechnern als auch bei Notebooks nach Ablauf einer definierten Zeitspanne automatisch gesperrt, sofern keine Aktivität des Benutzers erfolgt. Die Entsperrung erfordert die erneute Eingabe des Passworts.
Zugangsberechtigungen zu (Projekt-)Laufwerken werden ausschließlich in einem festgelegten Autorisierungsprozess mithilfe eines Software-Tools freigegeben. Freigaben durch die zuständige Abteilungsleitung als Fachverantwortliche erfolgen nur, wenn ein Mitarbeiter die entsprechende Befugnis für seine Tätigkeiten benötigt.
Die Notebooks der Mitarbeiter verfügen über einen Zugriffsschutz. Die Notebooks ermöglichen eine Speicherung auf den Serverlaufwerken.

Jeder Netzwerkzugriff von und nach außen wird durch eine dreistufige P-A-P- Topologie (Paketfilter-Application Gateway-Paketfilter) gemäß den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) realisiert und stellt somit einen weitestgehend zuverlässigen Schutz gegen ein Eindringen in das Netzwerk dar. Die Anbindung erfolgt über redundant ausgelegte Firewalls und DMZ gemäß BSI-Vorgabe in P-A-P-Topologie.

Personenbezogene und projektbezogene Daten werden nur auf Servern im Rechenzentrum gespeichert und verarbeitet. Damit ist eine Zutritts- und Zugangskontrolle gewährleistet. Der Zugriff wird auf Netzwerkebene und auf Applikationsebene durch passwortgebundene Authentifikationsmechanismen kontrolliert. Dadurch wird eine zentrale strukturierte Datenhaltung ermöglicht und eingehalten. Auf den Servern werden regelmäßig Security Scans durchgeführt, um eventuelle Sicherheitslücken zu entdecken und ihnen mit geeigneten Maßnahmen begegnen zu können.

2.3 Zugriffskontrolle

Ziel: Verhinderung unbefugten Lesens, Kopierens, Veränderns oder Entfernens innerhalb des Systems, also des Zugriffs Unbefugter auf personenbezogene Daten

Die Berechtigungsvergabe für Laufwerke und die Dokumentation erfolgt ausschließlich und automatisiert durch die Beantragung in einem Softwaretool. Werden Dienstleistungen extern vergeben, die potenziell den Zugriff auf personenbezogene Daten ermöglichen (z.B. Pflege und Wartung der Firewall oder des E-Mail-Servers), so erfolgt dies unter Abschluss entsprechender Verträge zur Auftragsverarbeitung.

Für das physikalische Löschen sensibler Daten wird ein spezielles Tool eingesetzt. Ausgesonderte Festplatten werden von einem zertifizierten Entsorger vernichtet.

Vergebene Zugriffsberechtigungen werden regelmäßig kontrolliert. Es existiert ein Authentisierungskonzept.

Die spezifische Verschlüsselung besonders zu sichernden Daten ist in Planung sowie teilweise umgesetzt auf FileServer-Ebene. Die verschlüsselte Datenübertragung von und zu Webservern ist, sofern Dienste oder Anwendungen angeboten werden, Pflicht. Für die Nutzer gilt nach den Regelungen einer Dienstanweisung die bevorzugte Nutzung der Verschlüsselung.
Standardmäßig wird die höchst mögliche, den BSI-Empfehlung folgende, TLS Transportverschlüsselung benutzt.
Wenn Mails beim Versand als "vertraulich" gekennzeichnet sind und keine geeignete TLS-Verschlüsselung möglich ist, wird eine PGP oder S/MIME-Verschlüsselung durchgeführt, wenn das Schlüsselmaterial vorliegt. Wenn diese nicht vorliegen, wird die gesamte E-Mail gezipt und mit einem Einmalkennwort verschlüsselt zu versenden. Das Kennwort geht an den Absender, der es telefonisch dem Empfänger mitteilt.

2.4 Trennungskontrolle

Ziel: Getrennte Verarbeitung von personenbezogenen Daten, die zu unterschiedlichen Zwecken erhoben wurden

Vertragsgemäß werden die Daten nur zu einem Zweck erhoben und verarbeitet. Zugriffs- und Benutzerkontrolle stellen sicher, dass keine Verbindung zu Daten anderer Auftraggeber erfolgen kann. Anderweitige als die im Vertrag beschriebenen Nutzungszwecke bedürfen der Einwilligung des Auftraggebers.

Entwicklungs- und Testumgebungen werden getrennt. Für Entwicklungsarbeiten werden ausschließlich Testdaten verwendet. Datensätze einzelner Projekte werden in voneinander getrennten Datenbankbereichen gespeichert und verarbeitet.
Technisch und organisatorisch wird dies über die Zutritts-, Zugangs- und Zugriffs- und Eingabekontrolle umgesetzt (siehe Abschnitte 2.1, 2.2, 2.3 und 3.2).

2.5 Pseudonymisierung

Die Möglichkeit einer Verarbeitung personenbezogener Daten in pseudonymisierter Form wird projektbezogen geprüft. Im Falle einer tatsächlichen Möglichkeit der Pseudonymisierung, wird diese durchgeführt. Die ggf. angewendeten technischen Verfahren werden jeweils in den projektspezifischen Vereinbarungen zur Auftragsverarbeitung personenbezogener Daten beschrieben.

3 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Personenbezogene Daten werden nur in einer Weise verarbeitet werden, die einen weitestgehenden Schutz vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen gewährleistet. Veränderungen an den gespeicherten Daten durch unberechtigte Dritte sind auszuschließen oder werden durch Protokollierung so erkennbar gemacht werden, dass sie korrigiert werden können.

3.1 Weitergabekontrolle

Ziel: Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens personenbezogener Daten bei der Übertragung oder der Speicherung auf Datenträgern sowie Überprüfbarkeit, welche Personen oder Stellen personenbezogene Daten erhalten haben

Die Daten werden ausschließlich gemäß dem Vertrag mit dem Auftraggeber verarbeitet. Format und Übertragungsweg personenbezogener Daten werden dabei projektbezogen überprüft, in Zusammenarbeit mit dem jeweiligen Auftraggeber festgelegt und in den jeweiligen Vereinbarungen zur Auftragsverarbeitung personenbezogener Daten beschrieben. In der Regel erfolgt die Übergabe personenbezogener Daten mittels SFTP-Server, auf den nur eine zuvor freigegebene IP-Adresse des Auftraggebers Zugriff (sog. White List-Verfahren) und sich durch ein Zertifikat authentifiziert hat, verschlüsselte Datenträger oder aber direkt über durch den Auftraggeber gesicherte Zugänge zu den Systemen des Auftraggebers. Andere Zugänge können nach vorheriger Überprüfung der Sicherheitsstandards vereinbart werden.

3.2 Eingabekontrolle

Ziel: Überprüfbarkeit, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen verarbeitet (eingegeben, verändert oder entfernt) worden sind

Sämtliche Datenübertragungen werden auf den Übertragungsservern protokolliert.

Änderungen von Datenbankinhalten können auf Anforderung und in Absprache mit dem Personalrat protokolliert werden.
Änderungen von Dateien können auf Anforderung und in Absprache mit dem Personalrat protokolliert werden.

3.3 Nichtverkettung und Zweckbindung

Nach Möglichkeit werden Daten getrennt gehalten mit zweckspezifischen Zugriffsrechten bei papierbasierten und elektronischen Daten. Projektbezogene Daten sind - sofern möglich - von den sonstigen Daten getrennt zu verarbeiten.

Soweit möglich erfolgt eine zweckspezifische Kennzeichnung von Daten, sofern diese nicht getrennt verarbeitet werden.

4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

4.1 Verfügbarkeitskontrolle und Wiederherstellbarkeit

Ziel: Schutz personenbezogener Daten gegen zufällige Zerstörung oder Verlust sowie deren stetige Verfügbarkeit für den Auftraggeber

Die Datenspeicherung erfolgt ausschließlich im gesicherten Netzwerk. Datensicherungen der relevanten Systeme werden täglich automatisch außerhalb der regulären Arbeitszeiten durchgeführt. Näheres ist in einem Backup-Konzept festgelegt.

Die Datensicherungen erfolgen automatisiert. Die Datenrekonstruktion und das Wiedereinspielen der Daten bei einem eventuellen Datenverlust darf nur von den berechtigten Personen und auf Antrag durchgeführt werden. Im Rahmen der täglichen Komplettsicherung der VMs über das allgemeine Backup wird auch der jeweilige Systemstatus gesichert, sodass bei einem Serverausfall alle relevanten Konfigurationsdateien des Betriebssystems wiederhergestellt werden können.

Der Serverraum ist klimatisiert und verfügt neben den Bewegungs- und Einbruchsmeldern über eine gesonderte Überwachung hinsichtlich Rauches, Wärme und Wassereinbruch. Diese Sensoren werden automatisiert überwacht, sodass im Alarmfall rund um die Uhr ein entsprechende Alarmierung erfolgt.

Alle Server im Rechenzentrum sind an eine unterbrechungsfreie Stromversorgung angeschlossen, die die Energieversorgung aufrechterhalten kann. Diese USV ist an eine Netzersatzanlage (Notstromgenerator) angeschlossen, so dass die Serverlandschaft im Betrieb gehalten werden kann.

Alle wichtigen Server laufen in einer virtualisierten Umgebung auf einem ESX-Cluster. Serverausfälle können von diesem System sofort ausgeglichen werden. Sämtliche Festpatten mit schützenswerten Bewegungsdaten (Produktion und Sicherung) auf den zentralen Speichersysteme sollen soweit möglich verschlüsselt werden. Die zugrundeliegende Hardware ist derart konstruiert, dass alle wichtigen Komponenten redundant vorliegen. Im Fall eines Ausfalls einer solchen Komponente wird eine automatische Benachrichtigung ausgelöst. Da die Virtualisierungs-Hardware vollständig redundant aufgebaut ist, kann in so einem Fall die Hardware ohne Service-Ausfall repariert werden. Defekte Server können für Reparatur und Wartung geregelt heruntergefahren werden.

Das Antivirus-System beruht auf verschiedenen Systemen. Auf dem Proxy, der den Internetkontakt ermöglicht (Surfen), wird der gesamte Verkehr auf schädliche Dateien überprüft. Der gleiche Vorgang wird von einer anderen Software noch einmal auf den Arbeitsstationen vorgenommen. Der Mailverkehr wird ebenfalls auf schädliche Daten und Spam geprüft. Der Fund schädlicher Dateien führt zu einem automatischen Alarm.

Es existiert ein Mailarchiv. Alle aus- und eingehenden E-Mails werden für 90 Tage in einem Mailarchiv gespeichert.

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)

5.1 Datenschutz-Management

Die KVSH hat einen Datenschutzbeauftragten bestellt. Die Bestellung ist dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein gemeldet worden. Bei Bedarf wird diese

Meldung aktualisiert. Es existiert eine Dienstanweisung zum Datenschutz und zur Informationssicherheit, die die Grundlage für das Datenschutzmanagement bildet.

Als Grundlage des Datenschutzmanagements dienen die vorliegenden TOMs, die in internen Audits überprüft und in Absprache mit dem Datenschutzbeauftragten ggf. angepasst werden. Notwendige Änderungen führen in keinem Fall zu einer Unterschreitung des notwendigen Schutzniveaus. Sofern es sich um umfangreiche Änderungen handelt, werden Auftraggeber, die diese Änderungen betreffen, darüber informiert.

Zudem finden quartalsweise Treffen des DISM-Teams mit dem Vorstand statt. Dem Team gehören der IT-Leiter, der Informationssicherheitsbeauftragte sowie der Datenschutzbeauftragte an. Bei Bedarf (s. insbesondere Abschnitt 5.2) werden ad hoc-Treffen einberufen und weitere Betroffene hinzugezogen.

Grundsätzlich folgt das Datenschutz-Management dem Vorgehen, das eine stetige Verbesserung der Prozesse und Abläufe verfolgt.

Die Mitarbeiter werden auf die Vertraulichkeit (Datengeheimnis) verpflichtet und werden bei wesentlichen Neuerungen geschult. Administratoren mit Zugriff auf TK- und E-Mail-Systeme werden explizit auf die Einhaltung gemäß BDSG und TKG verpflichtet.

Eine Übersicht über die Verarbeitungstätigkeiten gem. Art. 30 DSGVO wird geführt, soweit erforderlich werden in Abstimmung mit dem Datenschutzbeauftragten Datenschutzfolgeabschätzungen gem. Art. 35 DSGVO als Ergebnis einer vorangegangenen Risikoanalyse bei der Verarbeitung personenbezogener Daten durchgeführt.

5.2 Incident-Response-Management

Meldungen jeglicher tatsächlicher oder angenommener Verstöße bzw. Auffälligkeiten hinsichtlich Datenschutzes oder IT-Sicherheit sind von den Mitarbeitern an den Datenschutz- und Informationssicherheitsbeauftragten zu melden. Soweit erforderlich werden im DISM-Team die Vorgänge besprochen und ggf. weitergehende Maßnahmen nach Entscheidung des Vorstandes eingeleitet. In jedem Fall werden entsprechende Vorkommnisse sowie ggf. erfolgende weitere Maßnahmen dokumentiert.

Je nach Art und Schwere des Vorkommnisses können im konkreten Einzelfall unterschiedliche Maßnahmen erforderlich werden. Handelt es sich um Maßnahmen aufgrund von Verletzungen des Schutzes personenbezogener Daten gem. Art. 4 Ziffer 12 DSGVO, werden die in Art. 33 bzw. Art. 34 DSGVO beschriebenen Maßnahmen geprüft und ggf. ergriffen.

Das Verfahren ist in einer vom Vorstand beschlossenen Richtlinie zum Datenschutzvorfallmanagement sowie der Dienstanweisung zum Datenschutz und zur Informationssicherheit verbindlich geregelt.

5.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSG-VO)

Nach dem Grundsatz der Datenvermeidung und Datensparsamkeit sind Datenverarbeitungssysteme an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Mit Privacy by Default (datenschutzfreundliche Voreinstellungen) wird deshalb die Absicht verfolgt, dass sich IT-Systeme durch Voreinstellungen auf das zur Erfüllung des Vertragszwecks erforderliche Maß beschränken und dementsprechend nur diejenigen personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck auch erforderlich sind. Wesentliche Elemente der Datensparsamkeit sind, soweit möglich, die Trennung personenbezogener Identifi-

zierungsmerkmale und der Inhaltsdaten, die Verwendung von Pseudonymen und Anonymisierung sowie die Löschung personenbezogener Daten, sobald diese zur Erreichung des verfolgten Zwecks nicht mehr benötigt werden.

Auf Protokollierungen von Datenverarbeitungsvorgängen, soweit dies nicht gesetzlich vorgeschrieben ist, dem Integritätsschutz dient oder aus Sicherheitsgründen erforderlich ist, wird verzichtet.

5.4 Auftragskontrolle

Ziel: Verarbeitung personenbezogener Daten nur entsprechend der Weisungen

Die festgelegten Berechtigungsprofile gestatten nur den mit der Auftragsbearbeitung betrauten Mitarbeitern den Zugriff auf die projektbezogenen Daten, der zudem auf den zur Auftragsbearbeitung erforderlichen Umfang begrenzt ist.

In den Verträgen und/oder den Vereinbarungen zur Auftragsverarbeitung werden die Regelungen bezüglich Rechten und Pflichten des Auftragnehmers und der Auftraggeber ebenso festgehalten wie der zuständige Ansprechpartner und/oder projektverantwortliche Mitarbeiter. Weisungen des Auftraggebers an die Auftragnehmerin werden ausschließlich über den genannten Ansprechpartner oder dessen Vertretung übermittelt und durch den Ansprechpartner an die mit dem Projekt befassten Mitarbeiter kommuniziert.

Alle Mitarbeiter erhalten Schulungen zum Datenschutz nach DSGVO und geben Verpflichtungserklärungen zum Datenschutz ab.

5.5 Transparenz

- Information über Verarbeitungstätigkeiten der Dienststelle auf der Webseite
- Information bei der Datenerhebung mittels Webformularen
- Dokumentation

5.6 Intervenierbarkeit

- Mechanismen zur Änderung und Löschung in Dateisystemen und Datenbanken und E-Mail-Systemen
- Prozesse zur Wahrnehmung von Betroffenenrechten