Auftragsverarbeitungsvertrag (AVV)

zwischen

_____

_____

_____

im Folgenden "Auftraggeber" -

und

anonetics GmbH

Ferdinandstraße 29-33

20095 Hamburg

im Folgenden "Auftragnehmer" -

Auftraggeber und Auftragnehmer gemeinsam im Folgenden auch „Parteien“

wird folgender Auftragsverarbeitungsvertrag geschlossen.

Präambel

Im Rahmen des zur Nutzung der Softwarelösung anolink ZNA abgeschlossenen Hauptvertrags, ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers, dessen Mitarbeiterinnen und Mitarbeitern sowie durch ihn beauftragte Dritte mit diesen personenbezogenen Daten im Rahmen der Durchführung des Hauptvertrags.

Dies vorausgeschickt vereinbaren die Parteien was folgt:

1. Umfang, Gegenstand und Dauer der Auftragsverarbeitung

1.1 Der Auftragnehmer verarbeitet die personenbezogenen Daten des Auftraggebers ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DS-GVO.

1.2 Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer erfolgt gemäß Hauptvertrag. Art, Umfang und Zweck ergibt sich zudem aus **Anlage 1** zu diesem Vertrag, ebenso wie die Arten personenbezogener Daten und Kategorien betroffener Personen.

1.3 Die Dauer dieses Vertrages richtet sich in der Regel nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieses Vertrages nicht etwas anderes ergibt. Unabhängig von der Laufzeit oder

Wirksamkeit des Hauptvertrages bleibt dieser Auftragsverarbeitungsvertrag anwendbar, soweit der Auftragnehmer personenbezogene Daten für den Auftraggeber verarbeitet.

2. Weisungsbefugnisse des Auftraggebers

2.1 Der Auftraggeber bleibt für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Ziff. 7 DSGVO).

2.2 Der Auftragnehmer darf die personenbezogenen Daten nur im Auftrag und auf dokumentierte Weisung des Auftraggebers verarbeiten. Etwas anderes gilt nur dann, wenn der Auftragnehmer durch das Recht der Union oder der Bundesrepublik Deutschland verpflichtet ist, die personenbezogenen Daten auch auf andere Weise zu verarbeiten. In einem solchen Fall ist der Auftragnehmer verpflichtet, den Auftraggeber vor Beginn der jeweiligen Verarbeitung über die entsprechenden rechtlichen Anforderungen zu unterrichten, sofern das einschlägige Recht nicht eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet.

2.3 Soweit sich die dokumentierten Weisungen des Auftraggebers nicht bereits aus diesem Vertrag und seinen Anlagen ergeben, erfolgen diese durch den Auftraggeber grundsätzlich in Textform (z.B. per E-Mail). Sollte der Auftraggeber ausnahmsweise eine Weisung mündlich (z.B. telefonisch) erteilen, wird er diese entsprechend in Textform nochmals bestätigen.

2.4 Ansprechpartner des Auftragnehmers zwecks Weisungserteilung und sonstiger Mitteilungen ist/sind:

Lennox Yuma Marten

Telefon: +49 40 328906200

E-Mail: lennox@anonetics.de

2.5 Der Auftragnehmer gewährleistet, dass er die personenbezogenen im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder gegen die DSGVO oder anderweitige gesetzliche Vorschriften über den Datenschutz verstößt, wird der Auftragnehmer den Auftraggeber hierauf unverzüglich hinweisen. Der Auftragnehmer ist nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt aber nicht verpflichtet, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die Rechtskonformität der Verarbeitung der personenbezogenen Daten beim Auftraggeber liegt.

3. Vertraulichkeits- und Verschwiegenheitsverpflichtung

3.1 Der Auftragnehmer gewährt den von ihm eingesetzten Personen und – vorbehaltlich Ziffer 5 – Unterauftragsverarbeitern sowie den von diesen eingesetzten Personen nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand dieses Vertrages sind, als dies für die Durchführung, Verwaltung und Überwachung des Hauptvertrages erforderlich ist. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3.2 Soweit im Rahmen des Auftrages auch Daten verarbeitet werden, die unter ein Berufs- oder Amtsgeheimnis im Sinne von § 203 StGB fallen, verpflichtet sich der Auftragnehmer, über Berufs- und Amtsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu

verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der Tätigkeit eines Berufs- und Amtsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, nach § 203 Abs. 4 S. 1 StGB strafbar machen. Diese Strafbarkeit besteht auch, wenn sich der Auftragnehmer oder die von ihm eingesetzten Personen weiterer Mitwirkender bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbaren, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

3.3 Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufs- oder Amtsgeheimnis unterliegenden Daten des Auftraggebers befassten Personen sich dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufs- oder Amtsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit des § 203 Abs. 4 StGB belehrt wurden. Ferner hat der Auftragnehmer geeignete Maßnahmen ergriffen, um die Einhaltung und Durchsetzung des Beschlagnahmeschutzes (§ 97 StPO) sowie das Auskunftsverweigerungsrecht nach § 53a StPO zu gewährleisten und sicherzustellen, dass die Entscheidung über diese Rechte allein bei dem Auftraggeber liegt.

3.4 Der Auftragnehmer wird seine Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzten Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß von dem Berufs- oder Amtsgeheimnis unterliegenden Daten des Auftraggebers in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren. Ferner wird er seine Unterauftragsverarbeiter dazu verpflichten, geeignete Maßnahmen zu ergreifen, um die Einhaltung und Durchsetzung des Beschlagnahmeschutzes (§ 97 StPO) sowie das Auskunftsverweigerungsrecht nach § 53a StPO zu gewährleisten und sicherzustellen, dass die Entscheidung über diese Rechte allein bei dem Auftraggeber liegt.

3.5 Auf Verlangen des Auftraggebers wird der Auftragnehmer den Nachweis der vorgenannten Verpflichtungen vorlegen.

3.6 Die Parteien sind verpflichtet, über alle Geschäfts- und Betriebsvorgänge sowie Datensicherheitsmaßnahmen der jeweils anderen Partei, die ihnen aufgrund der Zusammenarbeit bekannt werden, Stillschweigen zu wahren und nicht an Dritte weiterzugeben. Ausgenommen von dieser Verpflichtung zur Geheimhaltung sind lediglich diejenigen Informationen, die

(i) zum Zeitpunkt des Zugänglichmachens bereits offenkundig waren oder danach ohne Zutun der jeweils anderen Partei offenkundig wurden;
(ii) zum Zeitpunkt des Zugänglichmachens nachweislich bereits im Besitz einer Partei waren, vorausgesetzt, dass diese nicht von der jeweils anderen Partei zugänglich gemacht worden sind;
(iii) einer Partei von dritter Seite auf rechtlich zulässige Weise und ohne Rechtsverletzung gegenüber der anderen Partei zugänglich gemacht wurden; oder
(iv) zu deren Offenlegung gegenüber Behörden und Gerichten eine rechtliche Verpflichtung besteht.

Die Geheimhaltungspflicht besteht auch nach Beendigung dieses Vertrages fort.

4. Datensicherheit; Technische und Organisatorische Maßnahmen gemäß Art. 32 DSGVO

4.1 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 Aufsichtsbehörden gegenüber nachweisen. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus Art. 32 DS-GVO resultierenden Maßnahmen.

4.2 Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt im **Anlage 3** zu diesem Vertrag.

4.3 Sofern zum Leistungsumfang des Auftragnehmers die Bereitstellung eines technischen Systems bzw. einer technischen Lösung gehört, sichert der Auftragnehmer zu, dass dieses technische System bzw. die technische Lösung den Voraussetzungen der DSGVO entspricht, insbesondere Art. 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) sowie dem III. Kapitel der DSGVO (u.a. Art. 15 DSGVO [Bereitstellung der personenbezogenen Daten in einem elektronischen Format] und Art. 20 DSGVO [Datenübertragbarkeit an den Betroffenen]).

5. Unterauftragsverarbeiter

5.1 Der Auftragnehmer ist berechtigt, zur Leistungserfüllung Unterauftragsverarbeiter in Anspruch zu nehmen (allgemeine schriftliche Genehmigung gemäß Art. 28 Abs. 2 S. 2 DSGVO). Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der **Anlage 2** aufgeführten Unternehmen als Unterauftragnehmer in Bezug auf Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Genehmigung für das Tätigwerden als erteilt.

5.2 Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung und/oder Ersetzung von Unterauftragsverarbeitern schriftlich oder in Textform (konkret, vollständig, mit Anschrift und stichwortartiger Beschreibung ihrer Aufgaben) informieren. Der Auftraggeber kann dem Einsatz eines Unterauftragsverarbeiters binnen 2 (zwei) Wochen nach Erhalt dieser Information widersprechen. Widerspricht der Auftraggeber, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen. Sofern der Auftraggeber nicht innerhalb von 2 (zwei) Wochen widerspricht, erlischt sein Widerspruchsrecht.

5.3 Unterauftragsverarbeiter dürfen für die geschuldete Leistung auch nach diesem Vertrag nur in dem Umfang eingesetzt werden, wie dies für die Durchführung, Verwaltung und Überwachung der geschuldeten Leistung erforderlich ist.

5.4 Der Auftragnehmer ist verpflichtet, seinen Unterauftragsverarbeitern die im Wesentlichen gleichen Pflichten aufzuerlegen, die für ihn aufgrund dieses Vertrages oder aufgrund gesetzlicher Vorschriften gelten. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

5.5 Ein genehmigungspflichtiges Unterauftragsnehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei Personal-, Post- und Versanddienstleistungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen

angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Die Nebenleistungen sind vorab detailliert zu benennen.

5.6 Der Auftragnehmer haftet gegenüber dem Auftraggeber für die Einhaltung der Pflichten durch die Unterauftragsverarbeiter.

6. Datentransfer in Drittländer

6.1 Die Übermittlung von Daten (inklusive der Bereitstellung oder Einrichtung von Zugriffsmöglichkeiten) in Länder außerhalb der Europäischen Union und des Europäischen Wirtschaftsraumes oder an internationale Organisationen (im Folgenden einheitlich „Drittland“) – sowohl durch den Auftragnehmer selbst als auch durch seine Unterauftragsverarbeiter – erfolgt auf Grundlage dieses Vertrages und bedarf keiner gesonderten Einwilligung des Auftraggebers, sofern die Unterauftragsverarbeiter in der **Anlage 2** benannt bzw. der Auftraggeber diesen nicht gemäß Ziffer 6.2 widersprochen hat und die geeigneten Garantien nach Art. 44 ff. DSGVO gewährleistet sind.

6.2 Sofern personenbezogene Daten aus der Europäischen Union oder dem Europäischen Wirtschaftsraum an einen Unterauftragsverarbeiter in ein Land übermittelt werden, das nicht als Land mit einem angemessenen Schutzniveau gemäß Art. 45 DSGVO von der Europäischen Kommission anerkannt ist, oder an eine internationale Organisation, verpflichtet sich der Auftragnehmer, eine Datenübermittlung nur auf Grundlage geeigneter Garantien im Sinne der Art. 44 ff. DSGVO durchzuführen.

6.3 Der Auftragnehmer wird dem Auftraggeber auf Anfrage die geeigneten Garantien, auf deren Grundlage die Übermittlung erfolgt, zur Verfügung stellen.

7. Datenschutzverletzungen

7.1 Dem Auftragnehmer ist bekannt, dass der Auftraggeber verpflichtet ist, sämtliche Verletzungen des Schutzes personenbezogener Daten umfassend zu dokumentieren und gegebenenfalls den Aufsichtsbehörden bzw. der betroffenen Person binnen 72 Stunden zu melden.

7.2 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich nach Kenntniserlangung über Verletzungen des Schutzes personenbezogener Daten sowie bei Verdachtsfällen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen sowie zur Unterstützung des Auftraggebers bei der Erfüllung seiner Pflichten nach Art. 33, 34 DSGVO.

7.3 Der Auftragnehmer wird den Auftraggeber bei der Erfüllung seiner Meldepflichten gegenüber der jeweils zuständigen Aufsichtsbehörde und der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person mit allen erforderlichen und angemessenen Mitteln unterstützen.

8. Wahrnehmung von Betroffenenrechten

8.1 Die Wahrnehmung von Betroffenenrechten nach dem III. Kapitel der DSGVO obliegt dem Auftraggeber. Der Auftragnehmer unterstützt den Auftraggeber dabei mit allen erforderlichen und wirtschaftlich angemessenen Mitteln sowie angesichts des Stands der Technik und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen mit geeigneten technischen und organisatorischen Maßnahmen, seiner Pflicht zur Beantwortung von Anträgen der in dem III. Kapitel der DSGVO genannten Rechte der betroffenen Personen nachzukommen.

8.2 Sollte sich eine betroffene Person unmittelbar an den Auftragnehmer zur Wahrnehmung der Betroffenenrechte wenden, wird der Auftragnehmer den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer wird dem Ersuchen der betroffenen Person ohne vorherige schriftliche (Textform ist ausreichend) Weisung des Auftraggebers nicht nachkommen.

8.3 Der Auftragnehmer wird dem Auftraggeber im Rahmen des Zumutbaren und Erforderlichen ermöglichen, personenbezogene Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

8.4 Der Auftraggeber trägt die Kosten des Auftragnehmers für solche Unterstützungsleistungen im Rahmen der Wahrnehmung von Betroffenenrechten, es sei denn, dass die Unterstützung wegen Gesetzes- oder Vertragsverstoß durch den Auftragnehmer erforderlich wurde.

9. Kontrollrechte

9.1 Der Auftraggeber ist berechtigt, sich durch Kontrollen während der üblichen Geschäftszeiten, die in der Regel mit einer Frist von vier Wochen anzumelden sind, von der Einhaltung aller vertraglichen und gesetzlichen Pflichten durch den Auftragnehmer zu überzeugen.

9.2 Der Auftragnehmer ermöglicht derartige Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen vom Auftraggeber beauftragten Prüfer, der zu absoluter Verschwiegenheit verpflichtet ist, durchgeführt werden und trägt zu ihrer Durchführung bei. Derartige Kontrollen dürfen nicht zu übermäßigen Beeinträchtigungen des Geschäftsablaufs des Auftragnehmers führen. Als Nachweis dienen insbesondere Auskünfte des Auftragnehmers, vorhandene Testate von Sachverständigen, Zertifizierungen und/oder Ergebnisse interner Prüfungen.

9.3 Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten innerhalb einer angemessenen Frist zur Verfügung.

9.4 Sollten bei der Prüfung Fehler und/oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen festgestellt werden, wird der Auftraggeber den Auftragnehmer hierüber unverzüglich unterrichten.

9.5 Der Auftraggeber trägt die Kosten des Auftragnehmers im Zusammenhang mit den Kontrollen, es sei denn, dass diese wegen Gesetzes- oder Vertragsverstoß durch den Auftragnehmer erforderlich wurden.

10. Behördliche oder gerichtliche Maßnahmen

10.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch aufsichtsbehördliche Maßnahmen, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter betroffen sein, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird überdies die in diesem Zusammenhang Beteiligten unverzüglich darüber unterrichten, dass die Verfügungsbefugnisse an den Daten ausschließlich beim Auftraggeber als Verantwortlichen im Sinne der DSGVO liegen und bei Betroffenheit von durch ein Berufsgeheimnis im Sinne des § 203 StGB geschützten Daten (insb. Patientendaten) zudem auf den besonderen Beschlagnahmeschutz gemäß § 97 StPO und die beschränkten aufsichtsrechtlichen Befugnisse nach § 29 Abs. 3 BDSG hinweisen. Der Auftragnehmer wird die Daten vor Durchführung von Maßnahmen nach Möglichkeit verschlüsseln und den Schlüssel nicht ohne rechtskräftige oder sofort vollziehbare Entscheidung an Dritte herausgeben.

10.2 Der Auftragnehmer wird Dritten ohne rechtskräftige oder sofort vollziehbare Entscheidung oder Androhung unmittelbaren Zwangs keinen Zugriff auf die Daten ermöglichen.

10.3 Der Auftragnehmer informiert den Auftraggeber ferner unverzüglich über sonstige Kontrollen und/oder Maßnahmen durch die Aufsichtsbehörden. Dies gilt auch für Kontrollen und/oder Maßnahmen anderer Behörden, sofern diese die vertragsgegenständlichen Daten des Auftraggebers betreffen.

11. Weitere Pflichten des Auftragnehmers

11.1 Dem Auftragnehmer ist bekannt, dass er für die jeweilige Auftragsverarbeitung ein Verzeichnis von Auftragsverarbeitungen gemäß Art. 30 Abs. 2 DSGVO zu führen hat. Auf Verlangen des Auftraggebers stellt der Auftragnehmer dem Auftraggeber die für dessen Verarbeitungsverzeichnis notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

11.2 Der Auftragnehmer unterstützt den Auftraggeber nach Maßgabe des Art. 28 Abs. 3 lit. f) DSGVO bei der Datenschutzfolgeabschätzung und gegebenenfalls bei der vorherigen Konsultation der Aufsichtsbehörden (Art. 35, 36 DSGVO). Er wird dem Auftraggeber alle erforderlichen Angaben und Dokumente auf Verlangen zur Verfügung stellen.

11.3 Datenschutzbeauftragter des Auftragnehmers ist Artin Eskandari. 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 DSGVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner.

11.4 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Verpflichtungen nach Art. 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) und wird insbesondere in Bezug auf die eingesetzten Systeme, Produkte, Anwendungen und Services die Grundsätze des Art. 25 DSGVO berücksichtigen.

12. Löschung und Rückgabe personenbezogener Daten

12.1 Der Auftraggeber hat gemäß Hauptvertrag jederzeit die Möglichkeit, alle Informationen, Nachrichten und mit dem Account zusammenhängende Daten selbst zu sichern und herunterzuladen.

12.2 Der Auftragnehmer löscht die in Ziffer 13.1 benannten Daten sowie sonstige vertragsgegenständliche Daten, und Datenbestände, die in direktem Zusammenhang mit dem Vertrag stehen, vier Wochen nach Beendigung des Vertrags bzw. Abschluss der Erbringung der Verarbeitungsleistungen, sofern nicht

(i) der Auftraggeber innerhalb dieser Frist seine Wahl mitteilt, dass sämtliche personenbezogenen Daten zurückzugeben und die vorhandenen Kopien gelöscht werden sollen und

(ii) für den Auftragnehmer nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

12.3 Bis zur Löschung oder Herausgabe der Daten gewährleistet der Auftraggeber weiterhin die Einhaltung der Bestimmungen dieses Vertrages, auch wenn der Vertrag wirksam beendet wurde. Das Protokoll der erfolgten Löschung ist auf Anforderung vorzulegen.

13. Schlussbestimmungen

13.1 Werden in diesem Vertrag die in der DSGVO definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung. Diese Klauseln sind im Lichte der Bestimmungen der DSGVO auszulegen.

13.2 Im Falle eines Widerspruchs zwischen diesem Vertrag und den Bestimmungen damit zusammenhängender Vereinbarungen, insbesondere dem Hauptvertrag, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

13.3 Sollten sich einzelne Bestimmungen dieses Vertrags ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung, Rechtsprechung oder aufsichtsbehördlicher Weisung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt. Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären. Existieren mehrere wirksame und durchführbare Bestimmungen, welche die in Satz 1 dieser Ziffer genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Daten im Sinne dieses Vertrages am besten gewährleistet.

13.4 Änderungen und Ergänzungen dieses Vertrages und aller ihrer Bestandteile bedürfen der Schriftform sowie eines ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses Vertrages handelt. Dies gilt auch für das Schriftformerfordernis selbst.

13.5 Dieser Vertrag und sämtliche sich aus diesem Vertrag ergebenden Rechtsbeziehungen unterliegen dem Recht der Bundesrepublik Deutschland unter Ausschluss jeglicher Kollisionsnormen, welche die Anwendung einer anderen Rechtsordnung anordnen. Als Gerichtsstand wird Hamburg vereinbart.

13.6 Die folgenden Anlagen sind wesentlicher Bestandteil dieser Vereinbarung:

- **Anlage 1** – Umfang und Gegenstand der Auftragsverarbeitung
- **Anlage 2** – Liste der Unterauftragsverarbeiter
- **Anlage 3** – Technische und organisatorische Maßnahmen (TOMs)

Hamburg, _____ Ort, Datum

_____ _____

anonetics GmbH _____

Anlage 1 - Umfang und Gegenstand der Auftragsverarbeitung

Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer erfolgt in der nachfolgend spezifizierten Art, dem Umfang und dem Zweck in Bezug auf die ebenfalls nachfolgend bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen.

Gegenstand der Auftragsverarbeitung / des Hauptvertrages	Die Verarbeitung von personenbezogenen Daten erfolgt im Rahmen der Bereitstellung und Nutzung der Webanwendung anolink ZNA. Die Anwendung dient der digitalen Erfassung, Verarbeitung und Übermittlung von patientenbezogenen Daten im Kontext von Notaufnahmen. Dies umfasst insbesondere die strukturierte Erhebung von Patienteninformationen, die digitale Abbildung von Aufnahmeprozessen (z. B. Behandlungsverträge, Wahlleistungen, Einwilligungen) sowie die sichere Übertragung der Daten an nachgelagerte Systeme wie Krankenhausinformationssysteme (KIS) oder Patientenportale.
Zwecke der Datenverarbeitung	• Digitale Erfassung und Verarbeitung von Patientendaten im Rahmen der Notaufnahme • Überwachung und Koordinierung von Patienten im Rahmen der Notaufnahme • Bereitstellung von Nutzungsübersichten und -analysen • Gewährleistung von IT- und Datensicherheit • Fehlerdiagnose und -behebung • bedarfsgerechte Gestaltung, Optimierung und Weiterentwicklung von anolink ZNA
Art(en) der Verarbeitung	• Speicherung • Erfassen • Löschen / Vernichtung • Offenlegung • Ordnen • Einschränkung • Organisation
Betroffene Personen und Daten	**Betroffene Personen** • Nutzer von anolink ZNA (insbesondere Ärzte, Pflegepersonal, Verwaltungspersonal und sonstige Beschäftigte des Kunden) • Patienten des Kunden • Ansprechpartner des Kunden • Sonstige Dritte, auf die in den eigens erstellten Abfragen Bezug genommen wird

	<u>Betroffene Daten</u> **Benutzerdaten** • Personenstammdaten (z.B. Mitarbeiter, Nutzer des Kunden) • Kontaktdaten (insbesondere Anschriften) • Kommunikationsdaten (z.B. IP-Adressen, Telefon, E-Mail) **Verarbeitete Inhaltsdaten (Patienten- und Dokumentendaten)** • Gesundheitsbezogene und patientenbezogene Daten (z. B. Befunde, Diagnosen, Anamnesen, Behandlungsinformationen) • Daten aus individuell erstellten Formularen (strukturierte und unstrukturierte Eingaben) • Inhalte hochgeladener oder generierter Dokumente (z. B. PDF-Dateien, Formulare, Scans) • Dokumenten- und Dateiinformationen (z. B. Dateinamen, Dateitypen, Versionen) **System- und Nutzungsdaten** • Metadaten zu erfassten Daten und Dokumenten (z. B. Erstellungszeitpunkt, Zuordnung zu Patienten, Nutzer) • Informationen über Verarbeitungsvorgänge (z. B. Erstellung, Bearbeitung, Übermittlung) • Zugriffsdaten (z. B. Zeitpunkte von Zugriffen, Aktionen innerhalb der Anwendung) • Technische Protokolldaten (z. B. Systemlogs, Fehlerprotokolle)

Anlage 2 – Liste der Unterauftragsverarbeiter

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung
Microsoft Ireland One Microsoft Place South County Business Park, Carmanhall And Leopardstown, Dublin, D18 P521 Ireland	Bereitstellung von Cloud-Infrastruktur für Betrieb und Skalierung der Anwendung, einschließlich Speicherung und Verarbeitung von Daten (z. B. Blob Storage und Datenbanken wie PostgreSQL), Ausführung von Backend-Funktionen sowie Nutzung von Sicherheits- und Schlüsselmanagementdiensten (z. B. Azure Key Vault)	Deutschland
IONOS SE Elgendorfer Str. 57 56410 Montabaur Deutschland	Hosting der Domains (anonetics.de, anonetics.com, anolink.de) und zugehöriger Subdomains. Speicherung von Metadaten wie IP-Adressen und andere technische Daten	Deutschland
Vercel Inc. 340 S Lemon Ave #4133 Walnut, CA 91789 USA	Hosting und Bereitstellung der Webanwendung anolink ZNA sowie Sicherstellung von Verfügbarkeit und Systembetrieb	Deutschland
Auth0 (Okta, Inc.) 10800 NE 8th Street, Suite 600, Bellevue, WA 98004 USA	Verwaltung von Authentifizierung und Kontodaten, einschließlich E-Mail-Adressen, Passwörter und andere benutzerbezogene Daten	EU
DeepL SE Maarweg 165 50825 Köln Deutschland	Automatisierte Übersetzung von Texten und Dokumenten sowie Verarbeitung sprachbezogener Daten zur Bereitstellung und Verbesserung von Übersetzungsdiensten	Deutschland
LINK Mobility Poland sp. z o. o. Toszecka 101 44-117 Gliwice Polen	Versand von SMS-Nachrichten zur Benachrichtigung und Kommunikation mit Empfängern	EU

Anlage 3 – Technische und organisatorische Maßnahmen (TOMs) gem. Art. 32 DSGVO

anonetics GmbH | Stand 12.02.2025

Hinweis

Dieses Dokument enthält Informationen, welche Geschäftspartnern, Kunden sowie weiteren externen Stellen, die ein gesetzliches oder sonstig begründetes Einsichtsrecht haben, zur Verfügung gestellt werden. Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt, nichtsdestoweniger beziehen sich die Angaben auf Angehörige aller Geschlechter.

Präambel

Der Verantwortliche hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert.

Der **allgemeine Teil (Grundsätzliche Maßnahmen)** beschreibt technische und organisatorische Maßnahmen, die unabhängig von den jeweiligen Dienstleistungen und Services, Standorten und Kunden gelten.
In den darauf folgenden Abschnitten sind Maßnahmen beschrieben, die über die im allgemeinen Teil dokumentierten Maßnahmen hinausgehen.

1. Grundsätzliche Maßnahmen

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung systematisch überwacht sowie anlassbezogen und mindestens halbjährlich evaluiert wird.
- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und alle notwendigen Umsetzungsverfahren.
- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe und Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren.
- Die an Mitarbeiter erteilten Berechtigungen sowie ausgegebenen Schlüssel, Zugangskarten oder Codes werden nach deren Ausscheiden aus dem Unternehmen bzw. Wechsel der Zuständigkeiten gemäß eines Berechtigungskonzeptes entzogen.
- Alle Dienstleister werden sorgfältig ausgewählt, und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten. Dies gilt auch für vergleichbare Situationen mit einem Datentransfer in Drittstaaten.
- Mitarbeiter werden im Hinblick auf den Datenschutz geschult und auf Verschwiegenheit verpflichtet. Spezielle Regelungen gelten für Tätigkeiten außerhalb betriebsinterner Räumlichkeiten.
- Der Schutz personenbezogener Daten wird nach dem Prinzip des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) gewährleistet.
- Die eingesetzte Software wird stets auf dem aktuellen Stand gehalten, ebenso wie Virenscanner und Firewalls.

2. Zutrittskontrolle

Alle Maßnahmen, die dazu geeignet sind, den Zutritt für Unbefugte zu den Datenverarbeitungsanlagen zu verhindern.

Umgesetzte Maßnahmen:

- Alarmanlage
- Absicherung der Gebäudeschächte
- Türen mit Knauf Außenseite
- Fenstersicherung dauerhaft
- Personal anwesend
- Videoüberwachung der Eingänge
- Regelung der Schlüsselausgabe
- Besucher in Begleitung durch Mitarbeiter
- Manuelles Schließsystem
- Sicherheitsschlösser
- Zutrittsregelungen für Besucher
- Besucherliste

3. Zugangskontrolle / Zugriffskontrolle

Alle Maßnahmen, die geeignet sind, die Nutzung der Datenverarbeitungssysteme durch Unbefugte zu verhindern.

Umgesetzte Maßnahmen:

- Login mit Benutzername + Passwort
- Login mit biometrischen Daten
- Stets aktueller Virenschutz
- Stets aktuelle Softwareversionen
- Verschlüsselter Datentransfer über HTTPS/TLS
- Netzwerk-Firewall
- Mobile Device Management
- Verschlüsselung von Datenträgern und Smartphones
- Einsatz von Intrusion-Detection-Systemen
- Automatische Desktopsperre
- Verschlüsselung von Notebooks/Tablets
- Verwaltung von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Richtlinien wie „Sicheres Passwort“, „Löschen/Vernichten“, „Clean Desk“
- Physische Löschung von Datenträgern
- Protokollierung von Zugriffen auf Anwendungen
- Minimale Anzahl an Administratoren

4. Weitergabekontrolle

Alle Maßnahmen, die gewährleisten, dass personenbezogene Daten bei Übertragung, Transport oder Speicherung nicht unbefugt gelesen, kopiert oder entfernt werden können.

Umgesetzte Maßnahmen:

- Protokollierung der Zugriffe und Abrufe
- Daten werden nur an autorisierte Dritte weitergegeben
- Pseudonymisierung
- Verschlüsselung von Datenträgern und Verbindungen
- Bereitstellung über verschlüsselte Verbindungen wie SFTP, HTTPS

- Nutzung von Signaturverfahren

5. Eingabekontrolle

Alle Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden.

Umgesetzte Maßnahmen:

- Protokollierung von Dateneingaben, Änderungen und Löschungen
- Übersicht, mit welchen Programmen welche Daten eingegeben werden
- können
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten
- Klare Zuständigkeiten für Löschungen
- Administratoren- und Stellvertreterkonzept
- Nachvollziehbarkeit von Änderungen durch individuelle Benutzernamen

6. Auftragskontrolle

Alle Maßnahmen, die gewährleisten, dass personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Umgesetzte Maßnahmen:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Abschluss notwendiger Vereinbarungen zur Auftragsverarbeitung
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

7. Verfügbarkeitskontrolle / Integrität

Alle Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Umgesetzte Maßnahmen:

- Feuer- und Rauchmeldeanlagen
- Unterbrechungsfreie Stromversorgung (USV)
- Backup & Recovery-Konzept
- Notfallkonzept durch interne IT und externe Dienstleister
- Regelmäßige Tests zur Datenwiederherstellung
- Ständige Kontrolle des Backup- und Recoverykonzepts

8. Gewährleistung des Zweckbindungs-/Trennungsgebotes

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

Umgesetzte Maßnahmen:

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung von Systemen, Datenbanken und Datenträgern
- Steuerung über Berechtigungskonzept

- Festlegung von Datenbankrechten
- Datensätze mit Zweckattributen versehen