Auftragsdatenverarbeitungsvertrag

zwischen dem

Verantwortlichen

, wie in der zwischen den Parteien geschlossenen Hauptauftragsvereinbarung („Hauptvertrag“) festgelegt

\- nachstehend Verantwortlicher genannt \-

und der

Dr. Flex GmbH
Stresemannstraße 21
10963 Berlin

\- nachstehend Auftragsverarbeiter genannt \-

– nachfolgend jeweils auch „Partei“ bzw. gemeinsam „Parteien“ genannt –

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

1) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27\. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG\] sichergestellt werden.

2) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 zu gewährleisten.

3) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

4) Die Anhänge I bis IV sind Bestandteil der Klauseln.

5) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.

6) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

1) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

2) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

1) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

2) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

3) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit

zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – fakultativ

Kopplungsklausel

1) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

2) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

3) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1 Weisungen

1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen.

Diese Weisungen sind stets zu dokumentieren.

2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.2a Weisungsgebundene Fehleranalyse und Systemstabilität

1) Zur Sicherstellung der Funktionsfähigkeit, Stabilität, Sicherheit und ordnungsgemäßen Leistungserbringung der vertraglich geschuldeten Dienste ist der Auftragsverarbeiter berechtigt, personenbezogene Daten in dem Umfang zu verarbeiten, der zur Identifikation, Analyse und Behebung technischer Fehler, Systemstörungen, Sicherheitsvorfälle oder Abweichungen in der Funktionalität der Software erforderlich ist.

2) Diese Verarbeitung erfolgt ausschließlich im Rahmen und zur Erfüllung der vom Verantwortlichen erteilten dokumentierten Anweisung und stellt keinen eigenständigen Verarbeitungszweck des Auftragsverarbeiters dar.

3) Die Fehleranalyse dient ausschließlich der Wiederherstellung der Systemintegrität, der Gewährleistung der Verfügbarkeit, der Sicherstellung einer ordnungsgemäßen Termin- und Kommunikationsabwicklung sowie der Einhaltung gesetzlicher Sicherheitsanforderungen.

4) Eine Nutzung der im Rahmen der Fehleranalyse verarbeiteten personenbezogenen Daten zu eigenen wirtschaftlichen Zwecken, insbesondere zu Marketing-, Profilbildungs- oder sonstigen nicht weisungsgebundenen Zwecken, schließt der Auftragsdatenverarbeiter aus.

5) Soweit möglich und verhältnismäßig, erfolgt die Fehleranalyse auf Grundlage pseudonymisierter oder technisch minimierter Datensätze.

7.2b Weisungsgebundene Supportleistungen

1) Der Auftragsverarbeiter ist berechtigt, personenbezogene Daten zu verarbeiten, soweit dies zur Erbringung von Support-, Beratungs- und Unterstützungsleistungen

gegenüber den Verantwortlichen erforderlich ist.

2) Hierzu zählen insbesondere die Bearbeitung von Supportanfragen, die technische Unterstützung bei der Nutzung der vertraglich geschuldeten Dienste, die Analyse gemeldeter Störungen oder Fehlfunktionen sowie die Unterstützung bei administrativen Vorgängen im Rahmen der Termin- und Kommunikationsverwaltung.

3) Die Verarbeitung erfolgt ausschließlich im Rahmen der dokumentierten Weisungen des Verantwortlichen und dient allein der ordnungsgemäßen Erfüllung der vertraglich vereinbarten Leistungen. Sie stellt keinen eigenständigen Verarbeitungszweck des Auftragsdatenverarbeiters dar.

4) Eine Nutzung der im Rahmen von Supportleistungen verarbeiteten personenbezogenen Daten zu eigenen Zwecken, insbesondere zu Marketing-, Analyse- oder Profilbildungszwecken, findet nicht statt.

5) Der Zugriff auf personenbezogene Daten erfolgt nur im erforderlichen Umfang und unter Beachtung des Prinzips der Datenminimierung sowie der internen Zugriffsbeschränkungen.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer

verarbeitet.

7.4 Sicherheit der Verarbeitung

1) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

2) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die

Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.4a Ärztliche Schweigepflicht

1) Soweit der Auftragsverarbeiter im Rahmen dieses Vertrags Kenntnis von Tatsachen erlangt, die dem ärztlichen Berufsgeheimnis unterliegen – insbesondere von personenbezogenen Daten von Patientinnen und Patienten oder bereits von dem Bestehen eines Behandlungsverhältnisses –, wird der Auftragsverarbeiter als mitwirkende Person im Sinne des § 203 Abs. 3 StGB tätig.

2) Der Auftragsverarbeiter verpflichtet sich hiermit ausdrücklich, sämtliche ihm im Rahmen der Auftragsverarbeitung bekannt gewordenen Informationen, die dem ärztlichen Berufsgeheimnis unterliegen, streng vertraulich zu behandeln und Dritten nicht unbefugt offenzulegen. Diese Verpflichtung gilt zeitlich unbegrenzt, auch über die Beendigung dieses Vertrags hinaus.

3) Der Auftragsverarbeiter stellt sicher, dass alle bei ihm mit der Verarbeitung betrauten Beschäftigten sowie sonstige eingesetzte Personen vor Aufnahme ihrer Tätigkeit nachweislich auf die Wahrung der ärztlichen Schweigepflicht gemäß § 203 StGB verpflichtet werden. Auf die Strafbarkeit eines Verstoßes nach §§ 203, 204 StGB wird ausdrücklich hingewiesen.

4) Der Auftragsverarbeiter verarbeitet die dem Berufsgeheimnis unterliegenden Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen und nur, soweit dies zur Erfüllung der vertraglich geschuldeten Leistungen erforderlich ist.

5) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Verlangen geeignete Nachweise über die Verpflichtung seiner Beschäftigten und sonstigen eingesetzten Personen auf die ärztliche Schweigepflicht vorzulegen.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle

Beschränkungen und/oder zusätzlichen Garantien an.

Sofern Patientenanliegen im Rahmen der VoiceAI ausnahmsweise Angaben enthalten, die besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO darstellen, erfolgt die Verarbeitung ausschließlich auf dokumentierte Weisung der Praxis als Verantwortlicher und wird durch technische Schutzmaßnahmen (z. B. Verschlüsselung, Zugriffsbeschränkung) abgesichert.
Eine eigenständige Bewertung oder Nutzung solcher Inhalte durch Dr. Flex findet nicht statt. Optimierungszwecke erfolgen ausschließlich anhand zuvor randomisierter, nicht rückführbarer Transkripte ohne Personenbezug.

7.6 Dokumentation und Einhaltung der Klauseln

1) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

2) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

3) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

4) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

5) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Tagen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten

Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

1) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten, einschließlich einer ausdrücklichen Verpflichtung zur Wahrung der ärztlichen Schweigepflicht gemäß § 203 StGB, soweit der Unterauftragsverarbeiter mit entsprechenden Daten in Berührung kommt.

2) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

3) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

4) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlungen

1) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.

2) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

2) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

3) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1\) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2\) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3\) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen

unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4\) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679

4) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

1) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

2) bei der Einholung der folgenden Informationen, die gemäß Artikel 33

Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1\) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2\) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3\) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden

können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

3) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen innerhalb von 24 Stunden unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

1) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

2) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

3) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der

Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

1) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

2) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1\) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2\) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;

3\) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.

3) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

4) Unmittelbar, spätestens jedoch 48 Stunden nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Eine Rückgabe der

Daten erfolgt nicht, es sei denn dies wurde gesondert vertraglich vereinbart. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln. Der Auftragsverarbeiter stellt mit geeigneten Löschverfahren sicher, dass die Daten unwiderruflich gelöscht werden.

ANHANG I – LISTE DER PARTEIEN

1\. Verantwortlicher:

Der Verantwortliche gemäß den im Hauptvertrag hinterlegten Stammdaten.

2\. Auftragsverarbeiter:

Dr. Flex GmbH

Stresemannstraße 21, 10963 Berlin
Ansprechpartner: Dr. med. Felix Wohlgemuth

Beitrittsdatum:
Das Datum der Unterzeichnung oder Zustimmung des Hauptvertrags durch den Verantwortlichen.

Unterschrift:
Mit der Unterzeichnung oder Zustimmung des Hauptvertrags gelten auch die Regelungen dieses Auftragsverarbeitungsvertrages gemäß Art. 28 DSGVO als vereinbart. Eine gesonderte Unterschrift oder Zustimmung ist nicht erforderlich.

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

1. Personen, die einen Termin über das Dr. Flex Booking Widget oder telefonisch über das KI-gestützte Sprachassistenzsystem (VoiceAI) buchen, verschieben, stornieren, einen Rückruf vereinbaren oder ein Anliegen übermitteln (Patient:innen).
2. Behandler:innen
3. Personen, die einen Termin in der medizinischen Einrichtung des Verantwortlichen vereinbart haben (Patient:innen) und dieser in den digitalen Kalender der medizinischen Einrichtung eingetragen wurde.
4. Personen, die sich in Dr. Flex einen Verwaltungs-Account anlegen.

Kategorien personenbezogener Daten, die verarbeitet werden

* Stammdaten (z. B. Name, Geburtsdatum)
* Kontaktdaten (z. B. Telefonnummer, E-Mail-Adresse)
* Termindaten (z. B. Terminart, Behandler, Zeitpunkt, Praxisstandort)
* Kommunikations- und Anliegeninhalte (frei formuliert), soweit zur organisatorischen Bearbeitung oder Weiterleitung im Auftrag erforderlich – beispielsweise Rezeptwunsch, Befundanforderung, Krankschreibung, Rückrufbitte, Fragen zu Rechnungen oder sonstige praxisorganisatorische Anliegen
* Kommunikationsdaten (z. B. automatisierte Benachrichtigungen wie Terminbestätigungen, Terminerinnerungen, Wartelisten-Hinweise, Stornierungs- und Änderungsbestätigungen, SMS-Antworten auf Anliegen sowie sonstige systemgestützte Patientenkommunikation)
* Daten zur Außendarstellung von medizinischen Einrichtungen und Behandler:innen (z. B. Fachrichtung, Qualifikationen, Spezialisierungen, Leistungsangebote, Bild- und Videodaten, Praxisportrait)
* Log-Daten (z. B. Zugriffs-, Änderungs- und Versandprotokolle; Ereignis- und Systemlogs zur Nachvollziehbarkeit)
* Technische Metadaten (z. B. IP-Adresse, Zeitstempel, Browser-/Geräteinformationen, Sitzungs-/Token-IDs, Fehlercodes zur Betriebs- und Sicherheitssicherung)
* Transkripte und Audioverarbeitung (VoiceAI) Audio: ausschließlich flüchtige Verarbeitung zur Spracherkennung; automatisierte Löschung unmittelbar nach Transkription, keine dauerhafte Speicherung. Transkripte: Erzeugte Transkripte werden noch am Erfassungstag oder spätestens innerhalb von 24 h randomisiert (Entfernung/Ersetzung sämtlicher Identifikatoren wie Name, Telefonnummer, Geburtsdatum, Praxis-/Termin-IDs). Nur die randomisierte Fassung wird dauerhaft zu Trainings- und Optimierungszwecken (Erkennungsqualität, Dialogführung, Fehlerratenreduktion) genutzt. Keine Zuordnung zu Patienten, Terminen oder Praxen. Metadaten: technische Prozess-/Nutzungsdaten (z. B. Dauer, Abbrüche, Fehlerraten, Zustell-/Weiterleitungsstatus) pseudonymisiert/anonymisiert für Systemanalyse und Qualitätssicherung.

> Hinweis: Dr. Flex wertet Inhalte nicht medizinisch aus und verarbeitet keine Gesundheitsdaten zu eigenen Zwecken. Anliegen- und Kommunikationsinhalte werden ausschließlich technisch entgegengenommen, strukturiert (z. B. als „Rezeptwunsch“ oder „Terminbestätigung“) und an den Verantwortlichen (Praxis) weitergeleitet.

Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder

zusätzliche Sicherheitsmaßnahmen

Vorhaltung und Speicherdauer auf Weisung des Verantwortlichen

Der Verantwortliche weist den Auftragsverarbeiter hiermit an, personenbezogene Daten im Zusammenhang mit Terminorganisation, Kommunikationsabwicklung, Systemprotokollierung sowie technischer Fehleranalyse für den Zeitraum vorzuhalten, der zur ordnungsgemäßen Durchführung dieser administrativen und organisatorischen Aufgaben erforderlich ist.

Die Vorhaltung dient insbesondere:

- der Abwicklung und Nachvollziehbarkeit von Terminbuchungen, Terminänderungen und Stornierungen
- der Bearbeitung von Rückfragen seitens der Praxis oder von Patienten
- der Dokumentation technischer Versand- und Zustellprozesse
- der Sicherstellung der Systemsicherheit und Missbrauchsprävention
- der Fehleranalyse und Supportbearbeitung
- der Erfüllung vertraglicher und gesetzlicher Nachweis- und Rechenschaftspflichten

Der Auftragsverarbeiter überprüft regelmäßig die Erforderlichkeit der weiteren Speicherung. Sobald der jeweilige Zweck entfällt und keine gesetzlichen Aufbewahrungspflichten bestehen, werden die Daten gelöscht oder anonymisiert.

Eine darüber hinausgehende Speicherung zu eigenen Zwecken ist ausgeschlossen.

Verarbeitung sensibler Daten und angewandte Beschränkungen

Die Verarbeitung personenbezogener und praxisbezogener Daten erfolgt ausschließlich zu den vertraglich definierten Zwecken, insbesondere zur Terminverwaltung, Außendarstellung, Praxisorganisation und Systemverwaltung. Dies umfasst:

Verarbeitung sensibler Daten und angewandte Beschränkungen

Die Verarbeitung personenbezogener und praxisbezogener Daten erfolgt ausschließlich zu den vertraglich definierten Zwecken, insbesondere zur Terminverwaltung, Außendarstellung, Praxisorganisation und Systemverwaltung. Dies umfasst:

1. Erhebung, Speicherung und Verarbeitung:

* Erhebung und Speicherung erforderlicher personenbezogener Daten zur Terminorganisation, Außendarstellung, Kommunikation und Verwaltung von

Benutzerrechten.
* Synchronisation und Verwaltung relevanter Daten mit dem Praxisverwaltungssystem.
* Automatisierte und individuelle Kommunikation im Rahmen der Terminorganisation.
* Anonymisierte Verarbeitung für statistische Analysen und Optimierung.
* Einsatz eines KI-gestützten Sprachassistenten (VoiceAI) zur telefonischen Terminorganisation und Anliegenbearbeitung. Dazu zählen insbesondere die Vereinbarung, Verschiebung und Stornierung von Terminen, die Koordination von Rückrufen, Anrufdienste wie Recall- oder Terminerinnerungen, die strukturierte Aufnahme von Anliegen sowie die Beantwortung häufiger Fragen.

* VoiceAI – Zweckbindung der Verarbeitung:
Die Verarbeitung im Rahmen der Nutzung des KI-gestützten Sprachassistenzsystems („Dr. Flex VoiceAI“) erfolgt ausschließlich zur organisatorischen Unterstützung der Praxis bei der Entgegennahme, Weiterleitung und Bearbeitung von Patientenanliegen, insbesondere:
- Annahme, Vereinbarung, Verschiebung oder Stornierung von Terminen,
- Koordination von Rückrufen und sonstigen organisatorischen Anliegen,
- Entgegennahme allgemeiner Patientenanfragen im Rahmen der Praxisorganisation.
Die Verarbeitung durch Dr. Flex erfolgt hierbei ausschließlich als technischer Dienstleister auf dokumentierte Weisung des Verantwortlichen.
Eine inhaltliche Auswertung, Klassifizierung oder Nutzung der Gesprächsinhalte zu medizinischen oder diagnostischen Zwecken findet nicht statt.
Rechtliche Einordnung: Soweit Anliegenangaben ausnahmsweise besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO) enthalten, erfolgt deren Verarbeitung ausschließlich im Auftrag und auf dokumentierte Weisung der Praxis (Verantwortlicher) gemäß Art. 28 DSGVO. Dr. Flex nimmt keine medizinische Interpretation vor und verwendet Inhalte nicht zu eigenen Zwecken. Die rechtliche Zulässigkeit nach Art. 9 Abs. 2 DSGVO stellt der Verantwortliche sicher.

* VoiceAI – Systemanalyse und Optimierung
Zur Aufrechterhaltung und Verbesserung der Funktionsfähigkeit, Benutzerfreundlichkeit und Erkennungsqualität des Sprachassistenzsystems („Dr. Flex VoiceAI“) verarbeitet Dr. Flex ausschließlich randomisierte Transkripte sowie anonymisierte/pseudonymisierte Interaktions- und Metadaten. Originale Audiodateien und nicht-randomisierte Transkripte werden nicht dauerhaft gespeichert.
* Audioverarbeitung (flüchtig):
Audiodateien werden nur für die technische Sprachverarbeitung genutzt und unmittelbar nach Transkription automatisiert gelöscht. Es erfolgt keine dauerhafte Speicherung der Audiodaten.
* Transkripte (randomisiert, dauerhaft für Optimierung):
Unmittelbar nach Erstellung werden Transkripte randomisiert (Entfernung/Ersetzung aller Personenbezüge wie Name, Telefonnummer, Geburtsdatum sowie Praxis-/Termin-IDs). Die so nicht rückführbaren Transkripte dürfen dauerhaft zu Trainings- und Optimierungszwecken (z. B. Erkennungsqualität, Dialogführung, Fehlerratenreduktion) genutzt werden. Eine Analyse personenbezogener Gesprächsinhalte findet nicht statt; keine Zuordnung zu einzelnen Patienten, Terminen oder Praxen.

* Metadaten (anonymisiert/pseudonymisiert):
Verarbeitet werden technische Verbindungs- und Prozessdaten (z. B. Gesprächsdauer, Abbruchstellen, Fehlerraten, Antwortklassifizierungen, Zustell-/Weiterleitungsstatus) sowie aggregierte Nutzungsstatistiken (z. B. Häufigkeit bestimmter Anliegen, Dialogverläufe ohne Personenbezug). Personenbezüge werden vor der Analyse technisch ausgeschlossen; keine Re-Identifizierbarkeit.
* Rechtsgrundlage & Zweckbindung:
Die Auswertung dient ausschließlich der Verbesserung der Dienstleistungsqualität (Systemanalyse, Performance-Optimierung) und erfolgt auf Grundlage des berechtigten Interesses von Dr. Flex gemäß Art. 6 Abs. 1 lit. f DSGVO. Eine Nutzung zu anderen Zwecken (z. B. Marketing, Profilbildung) erfolgt nicht.

2. Protokollierung und Nachverfolgbarkeit:

* Erfassung von Änderungen, Zugriffen und Nutzeraktivitäten zur Sicherstellung der Systemintegrität und Nachvollziehbarkeit.
* Speicherung technischer und sicherheitsrelevanter Daten zur Gewährleistung der Funktionalität und Schutz vor unbefugtem Zugriff.

3. Sicherheitsmaßnahmen und Zweckbindung:

* Strikte Zweckbindung auf die erforderlichen Anwendungsbereiche (z. B. Terminorganisation, Außendarstellung, Systemverwaltung).
* Zugriffsbeschränkung auf autorisierte Personen mit entsprechenden Berechtigungen und erforderlicher Schulung.
* Protokollierung aller relevanten Systemaktivitäten zur Nachvollziehbarkeit und Sicherheit.
* Einsatz geeigneter Schutzmaßnahmen (z. B. Verschlüsselung, Zugriffskontrollen, Audit-Trails).
* Beschränkung der Weitergabe von Daten auf die vertraglich und gesetzlich zulässigen Fälle.

Art der Verarbeitung

Die Verarbeitung personenbezogener und praxisbezogener Daten erfolgt ausschließlich zu den im Vertrag festgelegten Zwecken und unter Beachtung der geltenden Datenschutzvorschriften, insbesondere der DSGVO. Die Verarbeitung umfasst insbesondere folgende Tätigkeiten:

1. Erhebung und Speicherung: Verarbeitung personenbezogener und praxisbezogener Daten zur Terminverwaltung, Außendarstellung und Systemverwaltung. Speicherung und Synchronisation mit dem Praxisverwaltungssystem sowie Verwaltung von Benutzer- und

Zugriffsrechten.
2. Verarbeitung und Kommunikation: Nutzung der Daten zur Bereitstellung von Termindiensten, Benutzerverwaltung und Praxisorganisation. Automatisierte Kommunikation, einschließlich Terminbestätigungen, Erinnerungen und individueller Nachrichten. Darüber hinaus erfolgt die automatisierte sprachbasierte Kommunikation über den KI-gestützten Sprachassistenten VoiceAI zur Terminorganisation, strukturierte Aufnahme von Anliegen, Rückrufannahme und zur Beantwortung praxisbezogener Fragen. Benachrichtigungen im Auftrag (SMS/Telefon): Dr. Flex versendet terminbezogene Benachrichtigungen (z. B. Bestätigungen, Erinnerungen, Nachrücker-Hinweise, Storno-/Änderungsbestätigungen) im Namen und auf Weisung der Praxis.
* Rechtsgrundlage/Informationspflichten gegenüber Patienten verantwortet die Praxis; Dr. Flex handelt als Auftragsverarbeiter.
* Sperrlisten/Opt-out: Die Praxis kann Sperrlisten pflegen; Opt-outs der Patienten werden technisch unverzüglich umgesetzt und systemweit beachtet.
* Datenminimierung: Versand erfolgt nur mit erforderlichen Feldern (Telefonnummer/Mobilnummer, Terminzeitpunkt).
3. Protokollierung und Nachverfolgbarkeit: Logging von relevanten Systemaktivitäten (z. B. Änderungen, Zugriffen, Nachrichtenversand) zur Sicherstellung der Nachvollziehbarkeit und Integrität der Daten.
4. Technische Verarbeitung und Anonymisierung: Verarbeitung technischer Daten zur Gewährleistung der Systemfunktionalität und Sicherheit sowie Nutzung anonymisierter Daten für statistische Analysen und Optimierung.
5. Schutzmaßnahmen und Zweckbindung: Zugriffsbeschränkung auf autorisierte Personen, strikte Zweckbindung auf die jeweiligen Verarbeitungszwecke (Terminverwaltung, Außendarstellung, Benutzerverwaltung) sowie Einsatz geeigneter Sicherheitsmaßnahmen (z. B. Verschlüsselung, Zugriffskontrollen).

Dauer der Verarbeitung und Löschung von Daten

Die Speicherung und Verarbeitung personenbezogener und praxisbezogener Daten erfolgt ausschließlich zweckgebunden und im Rahmen der gesetzlichen und vertraglichen Vorgaben gemäß den Grundsätzen der Datenminimierung und Speicherbegrenzung (Art. 5 Abs. 1 lit. c und e DSGVO).

1. Speicherung und Verarbeitung:
* Personenbezogene Daten werden nur so lange verarbeitet, wie dies für die Erfüllung der jeweiligen Zwecke erforderlich ist.
* Protokolldaten werden zur Sicherstellung der Systemintegrität und Nachvollziehbarkeit gespeichert.
2. Rechtsgrundlagen:
* Verarbeitung erfolgt auf Basis von Einwilligung (Art. 6 Abs. 1 lit. a DSGVO), Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) oder rechtlicher Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO).

* Verarbeitung von Behandler- und Praxisdaten basiert auf vertraglicher Verpflichtung oder Einwilligung, insbesondere bei der Veröffentlichung von Medien (Art. 6 Abs. 1 lit. a DSGVO).
3. Löschung auf Anfrage oder nach Zweckerfüllung:
* Eine Löschung erfolgt nach Zweckerfüllung oder auf Anfrage gemäß Art. 17 DSGVO, es sei denn, gesetzliche oder vertragliche Aufbewahrungspflichten stehen entgegen.
* Behandler- und Praxisdaten können auf Widerruf oder auf Anfrage der Einrichtung gelöscht werden.

Spezialregelungen VoiceAI:
* Audio: Löschung unmittelbar nach Transkription.
* Transkripte: sofortige Randomisierung; dauerhafte Nutzung in nicht rückführbarer Form für Qualitätsverbesserung.

Die Einzelheiten zur Verarbeitung durch (Unter-)Auftragsverarbeiter, einschließlich Gegenstand, Art und Dauer der Verarbeitung sowie Empfänger und besondere Regelungen für Drittländer, sind in Anhang 4 dieses Vertrags geregelt. Anhang 4 ist integraler Bestandteil dieses Vertrags und ergänzt die Bestimmungen zur Verarbeitung personenbezogener Daten durch Dritte.

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN, EINSCHLIESSLI ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Die Dr. Flex GmbH implementiert technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 DSGVO. Diese Maßnahmen gewährleisten die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten und berücksichtigen die Risiken für die Rechte und Freiheiten der betroffenen Personen.

1\. Zutrittskontrolle (Schutz vor unbefugtem physischen Zugriff)

* Server befinden sich in gesicherten Rechenzentren innerhalb der EU.
* Unternehmensräume sind durch Zutrittskontrollsysteme, abschließbare Türen und Videoüberwachung gesichert.
* Zutritt nur für befugte Personen, dokumentiert durch ein Zutrittsmanagement.

2\. Zugangskontrolle (Schutz vor unbefugtem Zugriff auf IT-Systeme)

* Zugang zu Systemen ist passwortgeschützt und basiert auf rollenbasierten Berechtigungen.
* Zwei-Faktor-Authentifizierung (2FA) ist für sicherheitskritische Systeme implementiert.

* Fernzugriff nur über gesicherte Verbindungen (VPN, SSH).

3\. Zugriffskontrolle (Steuerung und Einschränkung von Benutzerrechten)

* Zugriff auf Daten erfolgt nach dem Prinzip der minimalen Rechtevergabe (Least Privilege Principle).
* Administratorrechte sind beschränkt und werden nach dokumentierten Verfahren vergeben.
* Beim Ausscheiden von Mitarbeitern werden Zugriffsrechte sofort entzogen.

4\. Datenträgerkontrolle (Schutz vor unbefugtem Zugriff auf Speichermedien)

* Verschlüsselung von Datenträgern mit BitLocker und FileVault.
* Protokollierung und Zugriffsbeschränkung für Datenträger mit personenbezogenen Daten.
* Sichere Löschung nach anerkannten Standards (z. B. softwarebasierte Löschung, Schreddern von Papierakten).

5\. Pseudonymisierung und Verschlüsselung

* Falls erforderlich, erfolgt die Pseudonymisierung personenbezogener Daten, sodass eine Identifizierung nur mit zusätzlichen Informationen möglich ist.
* Alle sensiblen Daten werden verschlüsselt gespeichert und übertragen.
* Transkripte aus VoiceAI werden vor jeglicher Speicherung außerhalb des flüchtigen Verarbeitungsschritts randomisiert (Entfernung/Ersetzung sämtlicher Personenbezüge wie Name, Telefonnummer, Geburtsdatum, Praxis-/Termin-IDs). Nicht-randomisierte Originaltranskripte werden nicht gespeichert.

6\. Datenintegrität und Übertragungskontrolle

* Datenübertragungen erfolgen verschlüsselt über TLS, VPN oder SSH.
* Firewalls und Monitoring-Systeme verhindern unbefugte Netzwerkzugriffe.
* Automatische Protokollierung von Änderungen an personenbezogenen Daten.

7\. Transportkontrolle

* Keine physische Weitergabe von Datenträgern mit personenbezogenen Daten.

8\. Benutzerkontrolle (Schutz vor missbräuchlicher Nutzung)

* Benutzeridentitäten werden zentral verwaltet, Authentifizierung erfolgt über ein IAM-System.

* Regelmäßige Datenschutzschulungen für autorisierte Nutzer.

9\. Maßnahmen zur Sicherstellung der Datenqualität

* Plausibilitätsprüfungen in den Systemen verhindern fehlerhafte Dateneingaben.
* Datenvalidierungsmethoden sorgen für Konsistenz in gespeicherten Datensätzen.

10\. Auftragskontrolle (Sicherstellung weisungsgebundener Verarbeitung)

* Alle Auftragsverarbeiter sind durch vertragliche Vereinbarungen zur DSGVO-Compliance verpflichtet.
* Dokumentierte Prozesse für die Auswahl und Kontrolle von Auftragsverarbeitern.

11\. Speicherkontrolle und Datenminimierung

* Speicherung personenbezogener Daten erfolgt nur in gesicherten IT-Systemen mit Zugriffskontrolle.
* Beschränkung der Datenspeicherung auf das erforderliche Minimum.
* Möglichkeit zur Sperrung oder Löschung personenbezogener Daten auf Anfrage.
* VoiceAI-Audiodateien werden ausschließlich flüchtig bis zur Transkription verarbeitet und anschließend automatisiert gelöscht; eine Speicherung erfolgt nicht.
* Temporäre Termin-Spiegel/Cache-Daten zur Praxisorganisation werden automatisch gelöscht (spätestens 12 Monate nach letztem Termin, sofern kein Folgetermin besteht).

12\. Verfügbarkeitskontrolle (Schutz vor Datenverlust)

* IT-Systeme sind gegen Datenverluste und Ausfälle abgesichert.
* Kritische Infrastruktur ist redundant ausgelegt.
* Recovery Time Objective (RTO): Im Falle eines Datenverlustes beträgt die maximale Wiederherstellungszeit 6 Stunden.

13\. Wiederherstellbarkeit

* Tägliche, verschlüsselte Backups, Speicherung an getrennten Standorten.
* Wiederherstellungsmöglichkeiten sind getestet und dokumentiert.
* Recovery Point Objective (RPO): Der maximal tolerierbare Datenverlust (Zeitspanne seit der letzten Datensicherung) beträgt 8 Stunden.

14\. Trennbarkeit

* Daten unterschiedlicher Kunden und Praxen werden mandantenfähig getrennt gespeichert.

* Produktiv-, Test- und Entwicklungsumgebungen sind strikt voneinander getrennt.

15\. Betriebssystemsicherheit

* Passwortschutz und Benutzerkontenverwaltung verhindern unbefugten Zugriff.
* Initialpasswörter müssen bei Erstnutzung geändert werden.

16\. Maßnahmen für (Unter-)Auftragsverarbeiter

* Auftragsverarbeiter müssen technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten nachweisen.
* Datenübermittlungen an Auftragsverarbeiter erfolgen ausschließlich über gesicherte Verbindungen.
* Verpflichtung zur Einhaltung der Datensicherheitsmaßnahmen über AVVs.

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Genehmigte Unterauftragsverarbeiter

Die folgenden Unterauftragsverarbeiter wurden durch den Verantwortlichen genehmigt. Sie unterstützen die Verarbeitung personenbezogener Daten im Rahmen der vertraglichen Leistungen und sind zur Einhaltung der DSGVO verpflichtet.

Name des Unterauftragsverarbeiters	Anschrift	Kontaktperson & E-Mail	Beschreibung der Verarbeitung	Standort der Datenverarbeitung
IONOS SE	Elgendorfer Str. 57, 56410 Montabaur, Deutschland	Kundensupport, support@ionos.de	Hosting von Serverinfrastruktur und Datenbanken innerhalb der EU	DE
Strato AG	Pascalstraße 10, 10587 Berlin, Deutschland	Strato Support, kontakt@strato.de	Backup-Management	DE
centron GmbH	Heganger 29, 96103 Hallstadt, Deutschland	Support Team, info@centron.de	Hosting und Ausführung von KI-Modellen (VoiceAI)	DE
Sendinblue GmbH	Köpenicker Str. 126, 10179 Berlin, Deutschland	Support Team, support@sendinblue.com	Versand von E-Mails und Marketingkommunikation	EU
Retarus GmbH	Aschauer Str. 30, 81549 München, Deutschland	Retarus Support, service@retarus.com	SMS- und E-Mail-Dienstleistungen für Kunden- und Patientenkommunikation	DE
websms (LINK Mobility GmbH)	Sternwartestraße 8, 5020 Salzburg, Österreich	Support Team, support@websms.at	SMS-Dienstleistungen für Kunden- und Patientenkommunikation	EU
Spryng B.V.	Hogehilweg 8, 1101 CC Amsterdam, Niederlande	Spryng Support,

support@spryng.nl | SMS-Dienstleistungen für Kunden- und Patientenkommunikation | EU |
sipgate GmbH	Gladbacher Str. 74, 40219 Düsseldorf, Deutschland	sipgate Support, kontakt@sipgate.de	VOIP- und Telefondienste zur Kommunikation	DE
ccn Services GmbH	Adi-Maislinger-Str. 7, 81373 München, Deutschland	ccn Support, service@ccn.net	Bereitstellung von SIP-Trunk-Telefonanschlüssen für VoiceAI	DE
telinform GmbH	Fruchtbahnhofstr. 3, 68169 Mannheim, Deutschland	Support Team, kontakt@telinform.de	Kundensupport- und Telefoniedienstleistungen	DE
Google LLC (Google Business Suite)	Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland	Google Support, support@google.com	Bereitstellung von Cloud-Diensten, E-Mail und Videokonferenzen	EU
enuvo GmbH	Riedstr. 3, 8953 Dietikon, Schweiz	enuvo Support, info@enuvo.ch	Erstellung und Hosting von Umfragen und Datenerhebungen	Schweiz (Angemessenheitsbeschluss)
Atlassian PTY, Ltd	Level 6, 341 George Street, Sydney, NSW 2000, Australien	Atlassian Support, support@atlassian.com	Projektmanagement und Kollaborationstools (z. B. Jira, Confluence)	Australien (Standardvertragsklauseln)

Stand: März 2026