Auftragsverarbeitungsvereinbarung

Stand dieser Vereinbarung: November 2026

Die nachfolgende Auftragsverarbeitungsvereinbarung[1] („**Vereinbarung**“) ist Bestandteil des zwischen der Simpleprax GmbH („**Auftragsverarbeiter**“) und dem Nutzer („**Verantwortlicher**“) auf Grundlage der Allgemeinen Vertragsbedingungen der Simpleprax GmbH („**AGB**“) geschlossenen Vertrags über die Simpleprax-Leistungen und die auf dieser Grundlage erbrachten Services („**Simpleprax-Vertrag**“).

Die Vereinbarung wird als gesondertes Dokument bereitgestellt, ist jedoch integraler Bestandteil des Simpleprax-Vertrags und kommt gemeinsam mit diesem zustande.

1 Zweck und Anwendungsbereich

1.1 Mit dieser Vereinbarung soll die Einhaltung von Art. 28 Abs. 3, 4 DS-GVO sichergestellt werden.

1.2 Der Verantwortliche und der Auftragsverarbeiter haben dieser Vereinbarung zugestimmt, um die Einhaltung von Art. 28 Abs. 3, 4 DS-GVO zu gewährleisten.

1.3 Diese Vereinbarung gilt für die Verarbeitung personenbezogener Daten gemäß Anhang 1.

1.4 Die Anhänge 1 bis 3 sind Bestandteil dieser Vereinbarung.

1.5 Diese Vereinbarung gilt unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der DS-GVO unterliegt.

1.6 Diese Vereinbarung stellt für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der DS-GVO erfüllt werden.

2 Unabänderbarkeit dieser Vereinbarung

2.1 Die Parteien verpflichten sich, diese Vereinbarung nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

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

3 Auslegung

3.1 Werden in dieser Vereinbarung, die in der DS-GVO definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der DS-GVO.

3.2 Diese Vereinbarung ist im Lichte der Bestimmungen der DS-GVO auszulegen.

3.3 Diese Vereinbarung darf nicht in einer Weise ausgelegt werden, die den in der DS-GVO vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

4 Vorrang

Im Falle eines Widerspruchs zwischen dieser Vereinbarung und den Bestimmungen des Simpleprax-Vertrags oder sonstiger Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, hat diese Vereinbarung Vorrang.

5 Kopplungsklausel

- entfällt -

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 1 aufgeführt.

7 Pflichten der Parteien

7.1 Weisungen

7.1.1 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.

7.1.2 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die DS-GVO oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang 1 genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang 1 angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

7.4.1 Der Auftragsverarbeiter ergreift mindestens die in Anhang 2 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 („**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.

7.4.2 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.

7.5 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 („**sensible Daten**“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6 Dokumentation und Einhaltung der Vereinbarung

7.6.1 Die Parteien müssen die Einhaltung dieser Vereinbarung nachweisen können.

7.6.2 Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß dieser Vereinbarung umgehend und in angemessener Weise.

7.6.3 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in dieser Vereinbarung festgelegten und unmittelbar aus der DS-GVO hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Vereinbarung 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.

7.6.4 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.

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

7.7 Einsatz von Unterauftragsverarbeitern

7.7.1 Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in der in Anhang 3 beigefügten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens dreißig (30) Tage im Voraus ausdrücklich in Textform 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.

7.7.2 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 dieser Vereinbarung gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend dieser Vereinbarung und der DS-GVO unterliegt.

7.7.3 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.

7.7.4 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.

7.7.5 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

7.8.1 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 DS-GVO im Einklang stehen.

7.8.2 Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Ziffer 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 DS-GVO beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der DS-GVO sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Art. 46 Abs. 2 DS-GVO erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

8 Unterstützung des Verantwortlichen

8.1.1 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.

8.1.2 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 Ziffer 8.1.1 und dieser Ziffer 8.1.2 befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

8.1.3 Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Ziffer 8.1.2 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:

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

- Verpflichtungen gemäß Art. 32 DS-GVO.

8.1.4 Die Parteien legen in Anhang 2 die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Vereinbarung sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

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 Art. 33, 34 DS-GVO 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:

9.1.1 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);

9.1.2 bei der Einholung der folgenden Informationen, die gemäß Art. 33 Abs. 3 DS-GVO 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;

9.1.3 bei der Einhaltung der Pflicht gemäß Art. 34 DS-GVO, 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 unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

9.2.1 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);

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

9.2.3 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 2 alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Art. 33, 34 DS-GVO zu unterstützen.

10 Verstöße gegen diese Vereinbarung und Beendigung

10.1 Falls der Auftragsverarbeiter seinen Pflichten gemäß dieser Vereinbarung nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der DS-GVO – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Vereinbarung einhält oder sie beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Vereinbarung einzuhalten.

10.2 Der Verantwortliche ist berechtigt, diese Vereinbarung zu kündigen, soweit sie die Verarbeitung personenbezogener Daten gemäß dieser Vereinbarung betrifft, wenn

1. der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Ziffer 10.1 ausgesetzt hat und die Einhaltung dieser Vereinbarung 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 Vereinbarung verstößt oder seine Verpflichtungen gemäß der DS-GVO nicht erfüllt;

3. der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß dieser Vereinbarung oder der DS-GVO zum Gegenstand hat, nicht nachkommt.

10.3 Der Auftragsverarbeiter ist berechtigt, diese Vereinbarung zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß dieser Vereinbarung 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 Ziffer 7.1.2 verstoßen.

10.4 Sofern der Verantwortliche nicht etwas anderes verlangt, löscht der Auftragsverarbeiter nach Beendigung dieser Vereinbarung nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Vereinbarung.

Anhang 1 – Beschreibung der Verarbeitung

Die vom Auftragsverarbeiter verarbeiteten personenbezogenen Daten werden Ende-zu-Ende verschlüsselt und sind dem Auftragsverarbeiter grds. nicht im Klartext zugänglich.

#	Information	Beschreibung
1	Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden	● Mitarbeiter des Verantwortlichen ● Patienten und ggf. Angehörige von Patienten
2	Kategorien der verarbeiteten personenbezogenen Daten	Welche Kategorien von personenbezogenen Daten im Einzelnen verarbeitet werden, bestimmt sich nach den vom Verantwortlichen genutzten Simpleprax-Leistungen. Bei den vom Auftragsverarbeiter verarbeiteten Kategorien personenbezogener Daten kann es sich insbesondere handeln um: ● Geschäftliche Kontaktdaten, z.B. Adresse, E-Mail-Adresse, Telefonnummer ● Login-Daten, z.B. Nutzername, Passwort, Zeitstempel, IP-Adresse ● Inhaltsdaten aus Dokumenten, die vom Verantwortlichen im Rahmen der Nutzung der Simpleprax-Leistungen verarbeitet werden, einschließlich Patientendaten ● Gesprächsdaten (Audioaufzeichnung) ● E-Mail-Adresse oder Telefonnummern der Patienten für Nachrichtenversand
3	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	● Siehe Ziffer 2 oben und Anhang 2
4	Art der Verarbeitung	● Bereitstellung einer SaaS-Lösung zur Nutzung durch den Verantwortlichen
5	Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden	● Erbringung der zwischen Verantwortlichem und Auftragsverarbeiter vertraglich vereinbarten Leistungen
6	Dauer der Verarbeitung	● Die Dauer der Datenverarbeitung bestimmt sich nach der Dauer des zugrundeliegenden Vertrags.

Anhang 2 – Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

Der Auftragsverarbeiter trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit im Sinne des Art. 32 DS-GVO.

#	Kategorie	Maßnahme	Beschreibung
1	**Vertraulichkeit**		
1.1		Zutrittskontrolle	● Da die Simpleprax GmbH anstelle eigener Rechenzentren die Dienste von Amazon Web Services und Hetzner in Anspruch nimmt, findet sich eine Auflistung der Sicherheitsmaßnahmen bei dem jeweiligen Anbieter: AWS: https://aws.amazon.com/de/security/ Hetzner: https://www.hetzner.com/assets/Uploads/downloads/Sicherheit.pdf
1.2		Zugangskontrolle	● Berechtigungen werden nur auf begründete Anfrage hin nach Überprüfung erteilt. Berechtigungen werden in den jeweiligen Systemen dokumentiert und wöchentlich auf weiteres Erfordernis überprüft. ● In allen eingesetzten Simpleprax Systemen wird, wenn verfügbar, eine Zwei-Faktor-Authentisierung vorausgesetzt und ebenso die vom Bundesamt für Sicherheit in der Informationstechnik empfohlenen Passwortrichtlinien angewandt. Ein regelmäßiger Passwortwechsel wird nicht erzwungen, da dies zu unsicheren Passwörtern führt. ● Mobile IT-Systeme und Datenträger müssen verschlüsselt werden. Alle eingesetzten Systeme werden, soweit technisch anwendbar, durch geeignete Schutzsoftware gegen Schadprogramme geschützt.
1.3		Zugriffskontrolle	● Berechtigungen sind strikt nach den verschiedenen möglichen Bereichen eingeteilt. Einem Mitarbeiter, der verschiedenen Berechtigungen benötigt, werden dann alle einzelnen Berechtigungen, die zur Ausübung notwendig sind, vergeben. Somit ist es auch möglich, einzelne Berechtigungen wieder zu entziehen, wenn sich die Aufgabe der Person ändert. Im Fall des Ausscheidens aus dem Unternehmen werden alle Berechtigungen entzogen und der Mitarbeiterzugang gelöscht. ● Alle Papierunterlagen mit personenbezogenen Daten müssen unwiderruflich vernichtet werden, nachdem sie nicht mehr benötigt werden. ● Nicht mehr verwendete Datenträger werden nicht an Dritte weitergegeben oder vorher nach gängigen Standards gelöscht, damit keine Daten wiederherstellbar sind.
1.4		Trennung	● Die technische Umsetzung der Simpleprax-Plattform gewährt nur Zugriff auf die jeweiligen für den Kunden zugängliche Bereiche. Somit ist von technischer Seite ein unbefugter Zugriff auf fremde Kundendaten unterbunden. ● Test- und Produktivsysteme laufen auf getrennten Servern mit jeweils getrennten Datenbanken, um eine effektive Trennung zu gewährleisten.
1.5		Pseudonymisierung & Verschlüsselung	● Daten werden nicht pseudonymisiert, jedoch verschlüsselt. Zusätzlich zur üblichen TLS-Verschlüsselung bei der Kommunikation mit den Servern, werden alle Gesundheitsdaten, wo möglich, Ende-zu-Ende verschlüsselt. Dadurch werden vertrauliche Patientendaten bereits auf dem Endgerät der Praxis oder des Patienten verschlüsselt und können erst in der empfangenden Praxis oder Klinik entschlüsselt werden (mit Ausnahme von Voice).
2	Integrität		
2.1		Eingabekontrolle	● Änderungen der personenbezogenen Daten werden in einem Log erhoben. Neben einem Zeitstempel, einer Nutzerkennung (wenn vorhanden) und weiteren Metadaten wird somit sichergestellt, dass unberechtigte Änderungen erkannt werden können und dementsprechend dagegen vorgegangen werden kann. Diese Logdaten werden 6 Monate nach Kündigung gelöscht. ● Die Protokolle können in erster Linie nur von Administratoren eingesehen werden, einige Protokolldaten werden aber auch zum Zweck der Kundenbetreuung eingesehen.

#	Kategorie	Maßnahme	Beschreibung
2.2		Weitergabekontrolle	● Jegliche Kommunikation läuft über eine SSL- bzw. TLS-Verschlüsselung. Durch die aktivierte SSL- bzw. TLS-Verschlüsselung, können die Daten, die an uns übermittelt werden oder die wir an andere übermitteln, nicht von Dritten mitgelesen werden. ● Eine Weitergabe oder sonstige Übermittlung personenbezogener Daten an Dritte erfolgt nicht. Etwas anderes gilt nur, wenn dies zur Abwicklung der mitgeteilten bzw. vereinbarten Zwecke erforderlich und nach geltendem Datenschutzrecht ohne Einwilligung erlaubt ist, die betreffende Person ausdrücklich eingewilligt hat oder wir gesetzlich dazu verpflichtet sind.
3	Verfügbarkeit und Belastbarkeit		
			● Die eingesetzten Rechenzentren verfügen über Klimaanlagen zur Kontrolle der Betriebstemperatur für Server und andere Hardware, um eine Überhitzung zu vermeiden und das Risiko von Serviceausfällen zu verringern. Temperatur und Luftfeuchtigkeit werden in angemessener Weise vom Personal und den technischen Systemen überwacht und geregelt. ● Die Rechenzentren sind mit automatischen Geräten zur Branderkennung und -bekämpfung ausgestattet. Die Branderkennungssysteme setzen Rauchsensoren in vernetzten, mechanischen und Infrastrukturbereichen ein. Diese Bereiche sind darüber hinaus durch Brandbekämpfungssysteme geschützt. ● Die elektrischen Anlagen unserer Rechenzentren wurden so entwickelt, dass sie vollständig redundant sind und ohne Beeinträchtigung des Betriebs gewartet werden können – und das rund um die Uhr. Die Rechenzentrumsbetreiber stellen sicher, dass die Rechenzentren mit einer Notstromversorgung ausgestattet sind, damit im Fall eines Stromausfalls der Betrieb von kritischen Lasten der Anlage gewährleistet ist. ● Die Betreiber kennen alle kritischen Systemkomponenten, die erforderlich sind, um die Verfügbarkeit unseres Systems zu erhalten und den Betrieb im Fall eines Ausfalls wieder aufzunehmen. Kritische Systemkomponenten werden an mehreren, voneinander isolierten Standorten (Availability Zones genannt) gesichert. Jede Availability Zone ist auf einen unabhängigen Betrieb mit hoher Zuverlässigkeit ausgelegt. Die Availability Zones sind vernetzt. Dies ermöglicht Ihnen die Nutzung von Anwendungen, für die ein automatischer, unterbrechungsfreier Failover zwischen den Availability Zones eingerichtet ist. Extrem ausfallsichere Systeme und eine daraus resultierende Serviceverfügbarkeit sind Bestandteil des Systemdesigns. Kunden profitieren durch den Einsatz von Availability Zones und Datenreplikation von extrem kurzen Wiederherstellungszeiträumen und Wiederherstellungspunktzielen sowie höchstmöglicher Serviceverfügbarkeit. ● Weitere Sicherheitsmaßnahmen, die die Verfügbarkeit und Belastbarkeit der Server gewährleisten finden Sie hier: https://aws.amazon.com/de/compliance/data-center/controls/
4	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung		
			● Simpleprax hat eine Datenschutzrichtlinie, die dazu beitragen soll, alle Datenschutzstandards zu erfüllen. Diese Richtlinie beschreibt die im Unternehmen eingerichteten Maßnahmen zur Umsetzung der Vorgaben der Datenschutzgrundverordnung und findet Anwendung im gesamten Unternehmen. Alle Mitarbeiter und an der Verarbeitung personenbezogener Daten direkt oder indirekt beteiligten externen Dienstleister (Auftragsverarbeiter) sind zur Einhaltung der gesetzlichen Vorgaben nach der DS-GVO beim Umgang mit personenbezogenen Daten verpflichtet. Eine Abweichung davon ist nur nach einer dokumentierten Freigabe durch die Geschäftsleitung zulässig. ● Alle Beschäftigten werden bei Beginn der Tätigkeit und danach regelmäßig zum Datenschutz geschult. Zertifikate für diese Schulungen sind auf Anfrage einsehbar. Alle Beschäftigten werden zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet.

#	Kategorie	Maßnahme	Beschreibung
			● Jeder Mitarbeiter muss eine Verpflichtung zum Datenschutz unterzeichnen, die eine Übersicht über alle für die Verpflichtung relevanten Vorschriften enthält und den Mitarbeiter über Regelungen, Anweisungen und Verhaltensvorschriften im Umgang mit personenbezogenen Daten informiert. ● Wir haben für unser Unternehmen einen Datenschutzbeauftragten bestellt: IITR Datenschutz GmbH Dr. Sebastian Kraska Marienplatz 2 80331 München Deutschland Telefon: +49 (0)89 1891 7360 E-Mail: email@iitr.de ● Auf der Plattform der IITR Datenschutz GmbH haben wir ein Datenschutzmanagementsystem (DSMS) implementiert. Im DSMS wird ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DS-GVO geführt. ● Wird eine Datenschutzverletzung festgestellt, gibt es interne Richtlinien, die den Prozess des Vorgehens detailliert beschreiben. Wird eine Datenschutzverletzung festgestellt ist zu prüfen, ob diese ggfs. Meldepflichten gegenüber den Betroffenen und der Datenschutz-Aufsichtsbehörde nach sich zieht. Die Meldung hat in der Regel binnen 72 Stunden zu erfolgen. Für die interne und externe Meldung von Datenschutzverletzungen stehen Templates zur Verfügung. ● Bergen neue Verarbeitungssysteme besondere Risiken für die Betroffenen, sind diese einer detaillierten Datenschutzprüfung im Rahmen einer so genannten Datenschutz-Folgenabschätzung zu unterziehen. Für die Datenschutzfolgenabschätzung gibt es eine genaue Prozessbeschreibung, die allen Mitarbeitern zur Verfügung steht.

Anhang 3 – Liste der Unterauftragsverarbeiter

Zum Zeitpunkt des Abschlusses dieser Vereinbarung hat der Verantwortliche die Beauftragung folgender Unterauftragsverarbeiter genehmigt:

Nr.	Unterauftragnehmer (Firma, Adresse, Ansprechpartner)	Verarbeitungsschritte / Zweck der Unterauftragsverarbeitung	Umfang der Auftragsverarbeitung	Zertifiziert nach
1	**Amazon Web Services EMEA SARL (AWS)** 38 avenue John F. Kennedy, L-1855 Luxemburg	Server-Infrastruktur für Simpleprax inkl. Website, Datenbanken, Backups, Logs, automatisierter E-Mail-Versand	Verarbeitung von Patientendaten und E-Mail-Versand (im Rechenzentrum in Frankfurt, für das Amazon Web Services HIPAA-Compliance zum Schutz von Gesundheitsdaten bestätigt	BSI C5, ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3, PCI DSS, HITRUST CSF, CSA STAR, FIPS 140-2 und weitere
2	**Hetzner Online GmbH** Industriestr. 25 91710 Gunzenhausen Deutschland	Bereitstellung und Betrieb der Server-Infrastruktur für KI-gestützte Funktionen und Anwendungen von Simpleprax, insbesondere zur Verarbeitung und Analyse medizinischer Daten	Verarbeitung von personenbezogenen Daten, insbesondere Patientendaten, Audioaufzeichnungen, Transkriptionen und medizinischen Dokumentationen, im Rahmen KI-gestützter Anwendungen auf Servern in deutschen Rechenzentren	ISO/IEC 27001:2022, BSI C5:2020 Typ 2, Prüfung gemäß § 8a BSIG (KRITIS), EMAS
3	**Team Viewer Germany GmbH** Jahnstr. 30 73037 Göppingen Deutschland	Tool für Fernwartung und Fernzugriff	Verarbeitung der Video- und Audioübertragung während der Fernwartung	BSI C5, ISO 27001, ISO 9001, SOC 2, HIPAA/HITECH
4	**Google Ireland Limited** Gordon House Barrow Street Dublin 4 Ireland	Interne und externe Kommunikation	E-Mail-Verkehr, Online-Meetings, Google Drive, Kalender	BSI C5, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 und SOC 3, FedRAMP, PCI DSS, FISC Compliance, Esquema Nacional de Sequridad (ENS)
5	**Stripe Payments Europe, Ltd.** C/O A&L Goodbody, Ifsc, North Wall Quay Dublin 1 Irland	Zahlungsabwicklung	Verarbeitet Name, des Karteninhabers, E-Mail-Adresse, Unique Customer Identifier, Order ID, Bank Account Details, Payment Card Details, Card Expiration date, CVC code, Datum/Zeit/Menge der Transaktion, Merchant name / ID, Standort	PCI-DSS, SSAE18/SOC 1 Typ 1 und Typ 2, SSAE18/SOC 2 Typ 1 und Typ 2, PSD2, SCA
6	**Sentry Inc** 45 Fremont Street, 8th Floor, San Francisco, CA 94105 USA	Automatisierte Fehlererkennung, Fehleranalyse und Überwachung der technischen Funktionsfähigkeit der Simpleprax-Anwendungen.	Verarbeitung von technischen Nutzungs-, Diagnose- und Fehlerdaten zur Erkennung, Analyse und Behebung von Softwarefehlern. Speicherung der Daten in Rechenzentren in Frankfurt am Main, Deutschland (EU-Datenregion).	ISO 27001, SOC2 Type I, SOC2 Type II, HIPAA Attestation