Stand: 01.09.2025

Anlage: Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO

Vertrag über die Verarbeitung personenbezogener Daten

im Sinne des Art. 28 Abs. 3 der VO (EU) 2016/679 DSGVO

im Auftrag des Kunden

- Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO -

- nachfolgend „Auftraggeber“ genannt -

durch die

Privatärztliche Verrechnungsstelle Westfalen-Nord GmbH

- Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO -

- nachfolgend „Auftragnehmerin“ genannt -

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

Diese Vereinbarung zur Auftragsverarbeitung (nachfolgend "AV-Vereinbarung") konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Nutzung des digitalen Dienstes „praxisToni“. Sie ist integraler Bestandteil der Allgemeinen Geschäftsbedingungen der Auftragnehmerin (nachfolgend „Hauptvertrag“).

1. Gegenstand und Dauer der Verarbeitung

(1) Die Auftragnehmerin verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Zusammenhang mit der Nutzung der KI-gestützten Telefonassistenz praxisToni. Es handelt sich dabei um eine über das Internet zugängliche Software-as-a-Service-Anwendung. Die Verarbeitung personenbezogener Daten umfasst insbesondere die automatisierte Annahme und Verarbeitung eingehender Anrufe in medizinischen Einrichtungen, die Erfassung, Kategorisierung und Verschriftlichung der übermittelten Inhalte sowie die Erstellung und Bereitstellung entsprechender digitaler Tickets zur Bearbeitung durch die Nutzer.

(2) Die Verarbeitung erfolgt für die Dauer des zwischen den Parteien geschlossenen Hauptvertrages. Laufzeit und Kündigung dieser Vereinbarung richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrages, d.h. eine Beendigung des Hauptvertrages bewirkt automatisch auch die Beendigung dieser Vereinbarung. Die Parteien sind sich darüber einig, dass ohne das Bestehen dieser Vereinbarung keine Verarbeitung personenbezogener Daten durch die Auftragnehmerin als Auftragsverarbeiterin erfolgen darf. Eine isolierte ordentliche Kündigung dieser Vereinbarung ist ausgeschlossen.

2. Umfang, Zweck und Art der Verarbeitung sowie Kategorien betroffener Personen

(1) Die Verarbeitung umfasst insbesondere das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen und die Vernichtung von personenbezogenen Daten, die im Rahmen von eingehenden Telefonaten durch den Dienst praxisToni verarbeitet und in Form von digitalen Tickets zur Verfügung gestellt werden.

(2) Zweck der Verarbeitung ist die Erbringung der Leistungsverpflichtungen resultierend aus dem Hauptvertrag.

(3) Die Erbringung der vertraglich vereinbarten Datenverarbeitung erfolgt grundsätzlich in einem Mitgliedstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR). Eine Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation durch die Auftragnehmerin erfolgt ausschließlich auf Grundlage dokumentierter Weisungen des Kunden oder sofern dies zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem die Auftragnehmerin unterliegt, erforderlich ist. In jedem Fall muss eine solche Übermittlung im Einklang mit Kapitel V der Verordnung (EU) 2016/679 erfolgen. Der Kunde erklärt sich damit einverstanden, dass die Auftragnehmerin zur Durchführung bestimmter Verarbeitungstätigkeiten Unterauftragsverarbeiter (siehe nachfolgende Ziffer 10) einsetzt und im Rahmen dessen auch eine Drittlandsübermittlung stattfinden kann. In diesen Fällen stellen die Auftragnehmerin und der jeweilige Unterauftragsverarbeiter sicher, dass die Anforderungen des Kapitels V der Verordnung (EU) 2016/679 eingehalten werden, insbesondere durch die Verwendung der von der Europäischen Kommission gemäß Art. 46 Abs. 2 lit. c DSGVO erlassenen Standardvertragsklauseln, sofern deren Voraussetzungen erfüllt sind.

(4) Die Art (und der Umfang) der personenbezogenen Daten, die im Rahmen der Nutzung der Software verarbeitet werden, können je nach Gesprächsverlauf, der durch den Anrufer bestimmt wird, variieren. Der Anrufer entscheidet eigenständig, welche Informationen er bereitstellt. Daraus folgt, dass personenbezogene Daten unterschiedlichster Art verarbeitet werden können. Die Datenverarbeitung erfolgt ausschließlich im Auftrag und nach Weisung des Auftraggebers.
Im Einzelnen sind insbesondere folgende Daten Gegenstand der Verarbeitung:

- **Datenkategorien, die zur Erbringung der Dienstleistung zwingend erforderlich sind:**
    - Bei Nutzern: Kontakt-/Kommunikationsdaten (z. B. E-Mail-Adresse), IP-Adresse
    - Bei Anrufern: Übermittelte Telefonnummer des Anrufers, Sprachaufzeichnung des Anrufers
- **Weitere mögliche Datenkategorien:**
    - Stammdaten (z. B. Name, Vorname, ggf. Titel, Geburtsdatum)
    - Kontaktdaten (z. B. Telefonnummer, ggf. E-Mail-Adresse)
    - Versicherungsstatus (privat oder gesetzlich)
    - Gesundheitsdaten (z. B. Angaben zu Rezeptwünschen, Überweisungsanliegen)
    - Termindaten (z. B. gewünschte oder bestehende Terminvereinbarungen)

- Sonstige vom Anrufer freiwillig bereitgestellte Informationen, einschließlich solcher, die besondere Kategorien personenbezogener Daten i. S. v. Art. 9 DSGVO enthalten können

Die konkrete Datenverarbeitung richtet sich nach der Konfiguration der Software durch den Verantwortlichen sowie nach den im Rahmen des Anrufs freiwillig mitgeteilten Informationen durch die betroffene Person.

(5) Die Verarbeitung personenbezogener Daten betrifft insbesondere folgende Kategorien betroffener Personen:
- Den Auftraggeber als Kunden der Auftragnehmerin;
- Beschäftigte des Auftraggebers;
- Patienten des Auftraggebers;
- Angehörige des Patienten des Auftraggebers;
- Neue Patienten (Interessenten) und sonstige Anrufer, die telefonisch Kontakt mit der medizinischen Einrichtung aufnehmen.

3. Technische und organisatorische Maßnahmen

(1) Die Auftragnehmerin ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen. Vor Beginn der Verarbeitung hat die Auftragnehmerin die in Anhang I dieser Vereinbarung aufgelisteten technischen und organisatorischen Maßnahmen zu implementieren und während des Vertrags aufrechtzuerhalten, bzw. – soweit ein Unterauftragsverarbeiter die Verarbeitung übernimmt – sicherzustellen, dass entsprechende Maßnahmen bei dem Unterauftragsverarbeiter umgesetzt sind.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der technologischen Weiterentwicklung. Insoweit ist es der Auftragnehmerin und ihren Unterauftragsverarbeitern gestattet, alternative adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Die Auftragnehmerin wird solche Änderungen dokumentieren.

4. Rechte und Pflichten des Kunden

(1) Der Kunde ist als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO allein verantwortlich für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten, insbesondere für das Vorliegen einer gültigen Rechtsgrundlage sowie die Wahrung der Rechte der betroffenen Personen. Der Kunde stellt sicher, dass der Auftragnehmerin nur solche Daten übermittelt werden, deren Verarbeitung nach den geltenden Datenschutzvorschriften zulässig ist.

(2) Der Kunde verpflichtet sich, die betroffenen Personen gemäß Art. 13 DSGVO ordnungsgemäß zu informieren, einschließlich der Angabe der Auftragnehmerin als eingesetztem Auftragsverarbeiter sowie der wesentlichen Inhalte dieser Vereinbarung. Die Auftragnehmerin stellt dem Kunden auf Anfrage die zur Erfüllung der Informationspflichten erforderlichen Angaben zur Verfügung.

(3) Dem Kunden obliegt es, der Auftragnehmerin die Verarbeitungsdaten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für

die Qualität der Verarbeitungsdaten. Der Kunde hat die Auftragnehmerin unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse der Auftragnehmerin Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

(4) Der Kunde verpflichtet sich, die Auftragnehmerin bei der Umsetzung der in Art. 32 bis 36 DSGVO genannten Pflichten, insbesondere bei der Wahrnehmung von Betroffenenrechten, bei der Durchführung einer Datenschutz-Folgenabschätzung und bei etwaigen Konsultationen mit der Aufsichtsbehörde, zu unterstützen, soweit dies erforderlich ist.

(5) Sollten Dritte gegenüber der Auftragnehmerin wegen der Verarbeitung von personenbezogenen Daten im Rahmen dieses Vertrages Ansprüche geltend machen, stellt der Kunde die Auftragnehmerin insoweit von solchen Ansprüchen frei, als der Anspruch nicht auf ein vorsätzliches oder fahrlässiges Verhalten der Auftragnehmerin oder deren Erfüllungsgehilfen zurückzuführen ist. Die Freistellung erfolgt nicht, soweit die Auftragnehmerin gegen Bestimmungen dieses Vertrages oder gegen gesetzliche Vorschriften der DSGVO verstoßen hat. Die Auftragnehmerin hat dem Kunden auf Verlangen alle Informationen zur Verfügung zu stellen, die zur Prüfung des Anspruchs erforderlich sind.

5. Weisungsbefugnis des Kunden

(1) Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich im Rahmen des geschlossenen Hauptvertrages und auf dokumentierte Weisung des Kunden – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation –, sofern sie nicht durch das Recht der Union oder der Mitgliedstaaten, dem die Auftragnehmerin unterliegt, zu einer anderweitigen Verarbeitung verpflichtet ist. Im Falle einer solchen Verpflichtung teilt die Auftragnehmerin dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Kunde ist zur Erteilung von Einzelweisungen berechtigt. Solche Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung der Auftragnehmerin - etwaige dadurch bedingte Mehrkosten der Auftragnehmerin sind vom Kunden zu übernehmen.

(2) Die Auftragnehmerin gewährleistet, dass die Auftragsverarbeitung im Einklang mit den Weisungen des Kunden erfolgt. Ist die Auftragnehmerin der Ansicht, dass eine Weisung des Kunden gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, hat sie den Kunden unverzüglich darüber zu informieren; nach einer entsprechenden Mitteilung an den Kunden ist die Auftragnehmerin berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Kunden auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung beim Kunden liegt.

(3) Weisungen sind grundsätzlich in Textform zu erteilen. (Fern-)mündlich erteilte Weisungen sind unverzüglich in Textform zu bestätigen. Die vollständige Dokumentation der Weisungen hat sowohl durch den Kunden als auch die Auftragnehmerin zu erfolgen.

6. Rechte und Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin stellt sicher und kontrolliert regelmäßig, dass die Datenverarbeitung im Rahmen der Leistungserbringung nach dem Hauptvertrag in ihrem Verantwortungsbereich, der Unterauftragsverarbeiter nach Ziffer 10 dieses Vertrags einschließt, in Übereinstimmung mit den Bestimmungen dieses Vertrags erfolgt.

(2) Die Auftragnehmerin darf ohne vorherige Zustimmung durch den Kunden im Rahmen der Auftragsverarbeitung keine Kopien oder Duplikate der Verarbeitungsdaten anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Hauptvertrag (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(3) Der Auftragnehmerin bleibt es vorbehalten, Verarbeitungsdaten zu anonymisieren[1] und nachfolgend die anonymisierten Daten zum Zwecke der bedarfsgerechten Gestaltung und Leistungsoptimierung im Rahmen des Hauptvertrages, der damit verbundenen Weiterentwicklung und der Optimierung erbrachten Dienste zu verwenden. Soweit die Auftragnehmerin im Rahmen dieses Vertrages Daten anonymisiert und die so gewonnenen anonymisierten Daten zu eigenen Zwecken verarbeitet, insbesondere zur Weiterentwicklung oder Optimierung ihrer Dienstleistungen, erfolgt diese Verarbeitung nicht mehr im Auftrag des Kunden. In diesem Fall entscheidet die Auftragnehmerin allein über die Zwecke und Mittel der weiteren Datenverarbeitung und agiert in Bezug auf diese Verarbeitungen als eigenständige Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO. Die Auftragnehmerin gewährleistet, dass bei der Anonymisierung sämtliche technisch und organisatorisch erforderlichen Maßnahmen getroffen werden, um eine Re-Identifikation betroffener Personen dauerhaft auszuschließen.

(4) Die Auftragnehmerin unterstützt den Kunden bei Kontrollen durch die Aufsichtsbehörde im Rahmen des Zumutbaren und Erforderlichen, soweit diese Kontrollen die Datenverarbeitung durch die Auftragnehmerin betreffen.

7. Vertraulichkeit und Datenschutz

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Berufsgeheimnissen, Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Die Auftragnehmerin behandelt alle im Rahmen dieser Vereinbarung verarbeiteten personenbezogenen Daten vertraulich. Dies gilt auch für besondere Kategorien

[1] Eine Anonymisierung liegt dann vor, wenn sie sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen oder wenn die betroffene Person nicht oder nicht mehr identifiziert werden kann (DSGVO, Erwägungsgrund 26, S. 5). Es kann davon ausgegangen werden, dass kein Personenbezug mehr angenommen werden kann, wenn alle Mittel geprüft wurden, die vernünftigerweise eingesetzt werden können, um die betreffende Person zu identifizieren (EuGH, Urt. V. 19.10.2016, Rs-582/14, Rn. 42).

personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, insbesondere Gesundheitsdaten, soweit solche im Rahmen der Nutzung der in Ziff. 1 genannten Anwendung verarbeitet werden.

(3) Die Auftragnehmerin stellt sicher, dass ihre zur Verarbeitung eingesetzten Mitarbeiter und sonstigen Beauftragten zur Vertraulichkeit verpflichtet wurden und mit den datenschutzrechtlich relevanten Anforderungen vertraut sind.

(4) Die Auftragnehmerin trifft angemessene technische und organisatorische Maßnahmen zur Wahrung der Vertraulichkeit entsprechend Art. 32 DSGVO. Der Umfang dieser Maßnahmen richtet sich nach dem jeweiligen Stand der Technik, dem mit der Verarbeitung verbundenen Risiko sowie der praktischen Umsetzbarkeit im Rahmen des Dienstleistungsmodells.

(5) Eine Offenlegung oder Weitergabe von Daten an Dritte erfolgt ausschließlich im Rahmen dieser Vereinbarung, im Hauptvertrag oder auf dokumentierte Weisung des Kunden, es sei denn, die Auftragnehmerin ist gesetzlich hierzu verpflichtet. In einem solchen Fall wird der Kunde – soweit rechtlich zulässig – vorab über die Verpflichtung informiert.

(6) Die Pflicht zur Vertraulichkeit besteht auch nach Beendigung dieses Vertrages fort.

8. Mitzuteilende Verstöße der Auftragnehmerin

(1) Die Auftragnehmerin informiert den Kunden unverzüglich, wenn sie feststellt, dass sie oder ein Beschäftigter bei der Verarbeitung von Verarbeitungsdaten gegen datenschutzrechtliche Vorschriften oder gegen Festlegungen aus diesem Vertrag verstoßen haben, sofern deshalb die Gefahr besteht, dass Verarbeitungsdaten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.

(2) Soweit den Kunden aufgrund eines Vorkommnisses nach Ziffer 8 Absatz 1 gesetzliche Informationspflichten wegen einer unrechtmäßigen Kenntniserlangung von Verarbeitungsdaten treffen, hat die Auftragnehmerin den Kunden bei der Erfüllung der Informationspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen zu unterstützen.

9. Kontrollrechte des Kunden

(1) Der Kunde ist berechtigt, die Einhaltung der in dieser Vereinbarung sowie in den einschlägigen gesetzlichen Vorschriften festgelegten datenschutzrechtlichen Anforderungen durch die Auftragnehmerin zu überprüfen. Die Überprüfung kann in Form von Stichproben, durch Einsichtnahme in relevante Unterlagen erfolgen. Die Kontrollrechte des Kunden erstrecken sich ausschließlich auf den Bereich der Auftragnehmerin, in dem personenbezogene Daten im Auftrag des Kunden verarbeitet werden.

(2) Der Kunde ist berechtigt, im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen der Auftragnehmerin die Geschäftsräume der Auftragnehmerin, in denen Verarbeitungsdaten verarbeitet werden, zu betreten, um sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anhang I zu diesem Vertrag zu überzeugen.

(3) Die Auftragnehmerin gewährt dem Kunden die zur Durchführung der Kontrollen nach Ziffer 9 Absatz 2 erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.

(4) Die Auftragnehmerin ist berechtigt, bestimmte Informationen von der Offenlegung im Rahmen von Kontrollen auszunehmen, soweit deren Offenlegung Geschäfts- oder Betriebsgeheimnisse, den Schutz von Daten Dritter oder gesetzliche bzw. vertragliche Pflichten der Auftragnehmerin verletzen würde. Die Einschränkung darf nur insoweit erfolgen, wie dies erforderlich ist und den Kontrollzweck nicht vereitelt.

(5) Der Kunde hat der Auftragnehmerin rechtzeitig (mindestens vier (4) Wochen im Voraus) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Kunde darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Kunden, weitere Kontrollen im Falle eines konkreten, nachweisbaren Verdachts auf schwerwiegende Datenschutzverstöße durchzuführen. Wenn und soweit darüber hinausgehende (zusätzliche) Kontrollen zu erheblichem Mehraufwand bei der Auftragnehmerin führen, ist die Auftragnehmerin berechtigt, den hierfür anfallenden Aufwand dem Kunden zu marktüblichen Stundensätzen in Rechnung zu stellen.

(6) Beauftragt der Kunde einen Dritten mit der Durchführung der Kontrolle, hat der Kunde den Dritten schriftlich ebenso zu verpflichten, wie auch der Kunde aufgrund von dieser Ziffer 9 dieses Vertrags gegenüber der Auftragnehmerin verpflichtet ist. Zudem hat der Kunde den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen der Auftragnehmerin hat der Kunde diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Kunde darf keinen Konkurrenten der Auftragnehmerin mit der Kontrolle beauftragen.

(7) Im Einvernehmen der Parteien kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anhang I anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen erbracht werden, wenn der Prüfungsbericht es dem Kunden in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anhang I zu diesem Vertrag zu überzeugen.

10. Unterauftragsverhältnisse

(1) Bei Erteilung des Auftrags gelten die in Anlage II zu dieser Vereinbarung aufgeführten Unternehmen als genehmigte Unterauftragsverarbeiter. Eine gesonderte Genehmigung durch den Kunden ist insoweit nicht erforderlich.

(2) Die Auftragnehmerin ist berechtigt, zur Erbringung der vertraglich vereinbarten Leistungen weitere Unterauftragsverarbeiter einzusetzen, sofern sie den Kunden hierüber rechtzeitig vorab in Textform informiert. Der Kunde kann der beabsichtigten Änderung binnen vier Wochen nach Zugang der Information widersprechen. Erfolgt kein Widerspruch innerhalb dieser Frist, gilt die Zustimmung als erteilt. Widerspricht der Kunde der weiteren Unterauftragsvergabe, und scheitert eine einvernehmliche Lösungsfindung zwischen den Parteien, ist die Auftragnehmerin berechtigt, das mit dem Kunden bestehende Vertragsverhältnis insgesamt zum Zeitpunkt des geplanten Einsatzes

des Unterauftragnehmers zu kündigen, wenn der Einsatz des vorgesehenen Unterauftragsverarbeiters für die Leistungserbringung wesentlich ist.

(3) Die Auftragnehmerin verpflichtet sich, mit sämtlichen Unterauftragsverarbeitern eine Vereinbarung zu treffen, die den Anforderungen nach Art. 28 Abs. 3 DSGVO entspricht. Dies umfasst insbesondere die Verpflichtung des Unterauftragsverarbeiters zur Einhaltung angemessener technischer und organisatorischer Maßnahmen sowie zur Wahrung der Vertraulichkeit.

(4) Unterauftragsverarbeiter, die in einem Drittland in Bezug auf die Datenverarbeitung gemäß dieser Vereinbarung tätig werden, unterliegen den erweiterten Anforderungen gemäß Art. 44 ff. DSGVO. Falls kein Angemessenheitsbeschluss nach Art. 45 Absatz 3 DSGVO vorliegt, darf eine Übermittlung an entsprechende Unterauftragsverarbeiter nur erfolgen, sofern geeignete Garantien vorgesehen sind und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Die Auftragnehmerin stellt in diesen Fällen sicher, dass entweder verbindliche interne Datenschutzvorschriften oder gültige Standardvertragsklauseln bzw. Standarddatenschutzklauseln vorliegen, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung den Anforderungen der DSGVO entspricht. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet die Auftragnehmerin gemäß Art. 28 Abs. 4 S. 2 DSGVO gegenüber dem Kunden für die Einhaltung der Pflichten jenes Unterauftragsverarbeiters.

(5) Nicht als Unterauftragsverhältnisse sind dagegen solche Dienstleistungen anzusehen, die die Auftragnehmerin bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die die Auftragnehmerin für den Kunden erbringt, Post- und Kurierdienste, Transportleistungen oder Bewachungsdienste. Gleichwohl ist die Auftragnehmerin verpflichtet, auch bei von Dritten erbrachten Nebenleistungen Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten.

(6) Für den Fall, dass der Unterauftragsverarbeiter Verarbeitungsdaten außerhalb der EU / des EWR verarbeitet oder nutzt, bevollmächtigt der Kunde die Auftragnehmerin hiermit, in Vertretung des Kunden mit einem Unterauftragsverarbeiter einen Vertrag unter Einbeziehung der jeweils gültigen EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern zu schließen. Der Kunde erklärt sich bereit, an der Erfüllung der Voraussetzungen im erforderlichen Maße mitzuwirken.

11. Betroffenenrechte und Mitwirkungspflichten

(1) Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Kunden geltend zu machen.

(2) Soweit ein Betroffener sich unmittelbar an die Auftragnehmerin zwecks Auskunft, Berichtigung, Löschung oder Sperrung der ihn betreffenden Daten wenden sollte, wird die Auftragnehmerin dieses Ersuchen zeitnah an den Kunden weiterleiten.

(3) Für den Fall, dass eine betroffene Person ihre Rechte aus Kapitel III der DSGVO, insbesondere auf Berichtigung oder Löschung von Verarbeitungsdaten oder auf Auskunft über die gespeicherten Verarbeitungsdaten und den Zweck der Speicherung, wahrnimmt, unterstützt die Auftragnehmerin den Kunden dabei nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen.
(4) Die Auftragnehmerin unterstützt den Kunden unter Berücksichtigung der ihm zur Verfügung stehenden Informationen, die Pflichten des Kunden aus den Artikeln 30 bis 36 DSGVO, zu erfüllen.
(5) Die Auftragnehmerin wird dem Kunden ermöglichen, Verarbeitungsdaten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Kunden die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem Kunden selbst unmöglich ist.

12. Datenrückgabe und Löschung

(1) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher auf Anweisung des Kunden hat die Auftragnehmerin sämtliche Verarbeitungsdaten nach Wahl des Kunden entweder zurückzugeben oder – vorbehaltlich gesetzlicher Aufbewahrungspflichten – datenschutzgerecht zu löschen.
(2) Über die Löschung bzw. Vernichtung von Verarbeitungsdaten hat die Auftragnehmerin ein Protokoll zu erstellen, das dem Kunden auf Anforderung vorzulegen ist.
(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch die Auftragnehmerin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.
(4) Daten, die die Auftragnehmerin rechtmäßig anonymisiert hat, sind von der Pflicht zur Rückgabe oder Löschung ausgenommen.

13. Schlussbestimmungen

(1) Dieser Vertrag gilt auch, wenn und soweit Behörden oder Gerichte abweichend eine gemeinsame Verantwortlichkeit der Vertragsparteien nach Art. 26 DSGVO annehmen.
(2) Sollten sich einzelne Bestimmungen des Vertrags ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, so bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrags 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. Sollte sich der Vertrag als lückenhaft erweisen, so gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrags entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.
(3) Der Vertrag unterliegt ausschließlich dem Recht der Bundesrepublik Deutschland unter Ausschluss seiner internationalen Verweisungsnormen.
(4) Ausschließlicher Gerichtsstand bei allen Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist der Sitz der Auftragnehmerin.

Anhang zur Vereinbarung zur Auftragsverarbeitung

Anhang I: Technische und organisatorische Maßnahmen

Anhang II: Unterauftragsverarbeiter

Stand: 01.09.2025

Anhang I – Technische und organisatorische Maßnahmen der Privatärztliche Verrechnungsstelle Westfalen Nord GmbH

Die Auftragnehmerin trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

a) Zutrittskontrolle

Ziel: Verhinderung des unbefugten physischen Zugangs zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
- Chipkarten-/Transpondersystem für Zutritt zu Gebäudeteilen - Zutritt zum Foyer während Öffnungszeiten ohne Transponder möglich, alle weiteren Türen nur mit autorisiertem Chip/Transponder - Verschlossene Türen außerhalb der Öffnungszeiten, Haupteingang zusätzlich verriegelt - Alarmanlage mit elektronischer Steuerung und Protokollierung - Grundstück durch Zaun gesichert; Zufahrten mit abschließbaren Schiebetoren	- Empfang im Foyer; bei Abwesenheit Klingelhinweis - Besucher müssen sich am Empfang anmelden und werden immer von einem Mitarbeiter begleitet - Alarmanlage kann nur von berechtigten Mitarbeitern (de-)aktiviert werden - Überwachung der Alarmanlage durch externes Sicherheitsunternehmen - Meldung bei Nichtaktivierung an zuständige Führungskraft und externes Sicherheitsunternehmen mit Vor-Ort-Prüfung (entweder durch zust. Führungskraft oder Sicherheitsunternehmen)

Die unternehmenseigenen Server befinden sich innerhalb der gesicherten Büroräume am Firmensitz und unterliegen den vorstehend beschriebenen Zutrittskontrollen.

b) Zugangskontrolle

Ziel: Sicherstellung, dass nur berechtigte Nutzer auf IT-Systeme zugreifen können, in denen personenbezogene Daten verarbeitet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
- Anmeldung mit Benutzername und Passwort - Intrusion-Detection-Systeme - Anti-Viren-Software auf Servern - Anti-Viren-Software auf Clients	- Verwaltung von Benutzerberechtigungen - Erstellung von Benutzerprofilen - Zentrale Passwortvergabe - Richtlinie „Sicheres Passwort“

- Firewall - Einsatz von VPN bei Remote-Zugriffen - Verschlüsselung von Notebooks/Tablets - Sperre externer Schnittstellen (z. B. USB) - Automatische Desktopsperre - Passwortrichtlinie	- Richtlinie „Löschen/Vernichten“ - Richtlinie „Clean Desk“ - Allgemeine Richtlinie Datenschutz/Sicherheit

c) Zugriffskontrolle

Ziel: Gewährleistung, dass berechtigte Nutzer nur auf diejenigen Daten und Funktionen zugreifen können, für die ihre Zugriffsrechte bestehen, und dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
- Aktenschredder (mind. Stufe P3) - Externer Aktenvernichter (DIN 32757) - Physische Löschung von Datenträgern - Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	- Einsatz Berechtigungskonzepte - Minimale Anzahl an Administratoren - Verwaltung Benutzerrechte durch Administratoren

d) Trennungskontrolle

Ziel: Sicherstellung, dass personenbezogene Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden und nicht unbefugt vermischt werden.

Technische Maßnahmen	Organisatorische Maßnahmen
- Trennung von Produktiv- und Testumgebung	- Steuerung über Berechtigungskonzept - Festlegung von Datenbankrechten

e) Pseudonymisierung

Ziel: Verarbeitung personenbezogener Daten in einer Form, bei der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
- Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System	- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

2. Integrität

a) Weitergabekontrolle

Ziel: Sicherstellung, dass personenbezogene Daten bei der elektronischen Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass Empfänger von Daten identifiziert werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
- Email-Verschlüsselung - Einsatz von VPN - Protokollierung der Zugriffe und Abrufe - Bereitstellung über verschlüsselte Verbindungen	

b) Eingabekontrolle

Ziel: Nachvollziehbarkeit, ob und von wem personenbezogene Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten - Manuelle oder automatisierte Kontrolle der Protokolle	- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen) - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts - Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit

Ziel: Gewährleistung der Verfügbarkeit personenbezogener Daten und der Belastbarkeit der Systeme, einschließlich der Fähigkeit, bei physischen oder technischen Zwischenfällen die Verfügbarkeit und den Zugang zu Daten rasch wiederherzustellen.

Technische Maßnahmen	Organisatorische Maßnahmen
- Feuer- und Rauchmeldeanlagen - Feuerlöscher Serverraum - Serverraumüberwachung Temperatur und Feuchtigkeit - Serverraum klimatisiert - USV (unterbrechungsfreie Stromversorgung)	- Backup & Recovery-Konzept - Kontrolle des Sicherungsvorgangs - Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse

- Schutzsteckdosenleisten Serverraum - Datenschutztresor - RAID System / Festplattenspiegelung	- Getrennte Partitionen für Betriebssysteme und Daten - Keine sanitären Anschlüsse im oder oberhalb des Serverraums - Existenz eines Notfallplans

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Ziel: Sicherstellung einer kontinuierlichen Überprüfung und Verbesserung der Wirksamkeit der technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten.

Technische Maßnahme	**Organisatorische Maßnahmen**
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (Wiki) - Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	- Datenschutzbeauftragter - Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet - Regelmäßige Sensibilisierung der Mitarbeiter - mindestens jährlich - Datenschutz-Folgenabschätzung (DSFA) vorhanden

Stand: 01.09.2025

Anhang II – Liste der Unterauftragsverarbeiter der Privatärztliche Verrechnungsstelle Westfalen Nord GmbH für den Dienst praxisToni

Unterauftragsverarbeiter	Anschrift	Verarbeitungstätigkeit	Standort der Datenverarbeitung
seven communications GmbH & Co. KG	Willestr. 4-6 24103 Kiel	Versand von SMS	Deutschland
Quadcore GmbH	Brandsende 12 20095 Hamburg	Hosting	Deutschland
Twilio Ireland Limited	70 Sir John Rogerson's Quay D02 R296 Dublin 2, Irland	Telefonie	EU
Parloa GmbH	Schönhauser Allee 9 10119 Berlin	Sprachverarbeitung (Speach to Text, Verarbeitung mittels Sprachmodell und Text to Speach)	Deutschland
Atlassian	Atlassian. Pty Ltd Level 6, 341 George Street Sydney NSW 2000 Australien	Sevicemanagement	Deutschland
Hotjar	Hotjar Ltd Dragonara Business Center 5th Floor, Dragonara Road, Paceville St Julian's STJ 3141 Malta, Europa	Nutzerfeedback	EU
eTracker GbmH	eTracker GmbH Erste Brunnenstraße 1 20459 Hamburg Germany	Verhaltensanalysen für Nutzung von Websites	Deutschland
Brevo	Sendinblue GmbH Köpenicker Straße 126 10179 Berlin	E-Mail-Service	Deutschland
Microsoft	Microsoft Ireland Operations, Ltd. Attn: Data Privacy One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland	Cloud Computing	Deutschland