Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO

Zwischen der

Betriebsmedizinisches Zentrum Kassel GmbH, Wilhelmshöher Allee 122, 34119 Kassel, Deutschland

- nachstehend **Auftraggeber** genannt -

und der

Firma **eTermin GmbH,** Mättivor 3, 6430 Schwyz, Schweiz

- nachstehend **Auftragnehmer** genannt -

Präambel

Der Auftragnehmer betreibt die SaaS-Anwendung eTermin, über welche dem Auftraggeber ermöglicht wird, die Terminvereinbarung mit ihren Kunden, Patienten und Klienten zu automatisieren. Im Rahmen dieser vertraglich vereinbarten Leistungserbringung (nachfolgend „**Hauptvertrag**“ genannt, welcher durch die elektronische Bestellung und Akzeptierung der AGB zustande kommt) ist es erforderlich, dass der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert.

Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Vertragsparteien im Zusammenhang mit dem Umgang des Auftragnehmers mit den Daten des Auftraggebers zur Durchführung des Hauptvertrags.

1. Anwendungsbereich, Gegenstand und Dauer der Verarbeitung

(1) Diese Datenschutzvereinbarung findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Soweit in dieser Vereinbarung keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus dieser Vereinbarung mit Rechtswirkung ausschließlich für diese Vereinbarung vor.

(2) Der Gegenstand und die Dauer des Auftrages sowie Umfang, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem Hauptvertrag. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

(3) Die Laufzeit und Kündigung dieser Vereinbarung richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieser Vereinbarung. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

(4) Gegenstand der Erhebung und Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten (z.B. Name, Vorname, Anschrift, Geburtsdatum)

- Kontaktdaten (z.B. Telefonnummern, E-Mail-Adressen)
- Termine (über eTermin vereinbarte Zeitpunkte)
- Kommunikationsdaten (z.B. über eTermin abgewickelte Kommunikation, E-Mail-Nachrichten)
- Von den Nutzern im Wege der Kommunikation erzeugte Inhalte („user-generated content“)

(5) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden/Vertragspartner, künftige Vertragspartner oder Interessenten des Auftraggebers
- Beschäftigte des Auftraggebers

(6) Die Verarbeitung der Daten findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2. Definitionen

(1) Personenbezogene Daten
Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO).
(2) Datenverarbeitung im Auftrag
Datenverarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Sinne des Art. 28 DSGVO.
(3) Weisung
Eine Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Berichtigung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag und diese Vereinbarung festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

3. Verantwortlichkeit für die Datenverarbeitung

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung, verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO). Sollten Dritte gegen den Auftragnehmer aufgrund der Erhebung, Verarbeitung oder Nutzung von Daten des Auftraggebers Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

(2) Dem Auftraggeber obliegt es, dem Auftragnehmer die Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Daten.

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4. Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer sichert die Umsetzung und Einhaltung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO vor Beginn der Verarbeitung zu. Diese sind durch den Auftragnehmer in der beigefügten Anlage „Übersicht über die technisch-organisatorischen Maßnahmen“ dokumentiert.

(2) Die in der vorgenannten Anlage dokumentierten Maßnahmen sind Grundlage dieser Vereinbarung. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, sofern das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers und sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(4) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers über die Anwendung eTermin in erster Linie in einem Rechenzentrum mit Sitz in Frankfurt in Deutschland. Die bei dieser Datenverarbeitung ergriffenen technischen und organisatorischen Maßnahmen des Rechenzentrumsbetreibers sind gleichfalls in der beigefügten Anlage „Übersicht über die technisch-organisatorischen Maßnahmen“ dokumentiert.

5. Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat Daten nur nach Weisung des Auftraggebers unter Beachtung von Ziff. 7 dieser Vereinbarung zu verarbeiten. Der Auftragnehmer hat ausschließlich nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten oder Auskunft über die gespeicherten Daten des Auftraggebers wenden sollte, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer stellt sicher und kontrolliert regelmäßig, dass die Datenverarbeitung und -nutzung im Rahmen der Leistungserbringung nach dem Hauptvertrag in seinem Verantwortungsbereich, der Unterauftragnehmer nach Ziff. 10 dieser Vereinbarung einschließt, in Übereinstimmung mit den Bestimmungen dieser Vereinbarung erfolgt.

(3) Der Auftragnehmer darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsdatenverarbeitung keine Kopien oder Duplikate der Daten des Auftraggebers 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.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde im Rahmen des Zumutbaren und Erforderlichen, soweit diese Kontrollen die Datenverarbeitung durch den Auftragnehmer betreffen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden, nachzuweisenden Aufwände und Kosten in Höhe von 150 Euro pro Stunde.

(5) Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit (sofern ein solcher vom Auftragnehmer nach den gesetzlichen Bestimmungen zu bestellen ist) und den Ansprechpartner für im Rahmen des Vertrags anfallende Datenschutzfragen.

(6) Der Auftragnehmer hat die bei der Verarbeitung von Daten des Auftraggebers beschäftigten Personen gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO zur Vertraulichkeit zu verpflichten.

(7) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er feststellt, dass er oder ein Mitarbeiter bei der Verarbeitung von Daten des Auftraggebers gegen datenschutzrechtliche Vorschriften oder gegen Festlegungen aus dieser Vereinbarung verstoßen haben und die Voraussetzungen der Art. 33, 34 DSGVO vorliegen. Soweit den Auftraggeber gesetzliche Informationspflichten wegen einer unrechtmäßigen Kenntniserlangung von Daten des Auftraggebers (insbesondere nach Art. 33, 34 DSGVO) treffen, hat der Auftragnehmer den Auftraggeber bei der Erfüllung der Informationspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden, nachzuweisenden Aufwände und Kosten zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen

6. Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von betroffenen Personen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Dem Auftraggeber obliegen die aus Art. 33, 34 DSGVO resultierenden Meldepflichten.

7. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Daten des Auftraggebers ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie abschließend in den Bestimmungen dieser Vereinbarung und den Festlegungen des Hauptvertrags Ausdruck finden. Weisungen des Auftraggebers dürfen die vertraglich vereinbarten Leistungspflichten aus dem Hauptvertrag nicht unmöglich machen. Einzelweisungen, die von den Festlegungen dieser Vereinbarung abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers.

Ziehen Einzelweisungen Mehrkosten nach sich, insbesondere wenn diese über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind diese dem Auftragnehmer zu vergüten.

(2) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder in Textform (z.B. per E-Mail) bestätigen.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 S. 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

8. Unterstützungspflichten

(1) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Informationen oder Auskünfte zur Verarbeitung von Daten dieser Person zu geben oder die Rechte von betroffenen Personen nach Kapitel III (Artt. 12 bis 23) der DSGVO zu gewährleisten, wird der Auftragnehmer den Auftraggeber soweit vereinbart bei der Erfüllung dieser Pflichten mit geeigneten technischen und organisatorischen Maßnahmen entsprechend Art. 28 Abs. 3 lit. e DSGVO unterstützen.
(2) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten entsprechend Art. 28 Abs. 3 lit. f DSGVO bei der Einhaltung der in den Artt. 32 bis 36 DSGVO genannten Pflichten.
(3) Bei der Erbringung der Unterstützungsleistungen nach Abs. 1 und 2 dem Auftragnehmer entstehenden und nachzuweisenden Aufwände und Kosten sind vom Auftraggeber zu ersetzen.
(4) Im Falle einer Inanspruchnahme einer Vertragspartei durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO verpflichtet sich die in Anspruch genommene Vertragspartei, die andere Vertragspartei unverzüglich zu informieren. Die Vertragsparteien werden sich bei der Abwehr des Anspruchs gegenseitig unterstützen.

9. Kontrollrechte des Auftraggebers

(1) Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach Art. 28 Abs. 3 lit. h DSGVO stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen gemäß der Anlage zu dieser Vereinbarung überzeugen kann.

(2) Der Auftragnehmer gewährt dem Auftraggeber die zur Durchführung dieser Kontrollen erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.

(3) Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und

Vertragsmanagementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Kontrollzwecke sind, zu erhalten.

(4) Der Auftraggeber ist berechtigt, im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers, in denen die Daten des Auftraggebers verarbeitet werden, zu betreten, um sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß der Anlage zu dieser Vereinbarung zu überzeugen. Sofern ein Unterauftragnehmer eine Vor-Ort-Kontrolle nicht zulassen sollte (z.B. Microsoft beim Betrieb von Rechenzentren), werden dem Auftraggeber auf Anfrage alternative geeignete Nachweise vorgelegt (z.B. Auditberichte unabhängiger Auditoren).

(5) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen gemäß der Anlage zu dieser Vereinbarung anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit, einer Bestätigung der Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO oder der Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DSGVO erbracht werden, wenn diese Prüfungsberichte es dem Auftraggeber in angemessener Weise ermöglichen, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß der Anlage zu dieser Vereinbarung zu überzeugen.

(6) Zur Durchführung der Kontrolle muss der Auftragnehmer nur eine solche Person zulassen, die besonders zur Geheimhaltung, insbesondere in Bezug auf Informationen über den Betrieb des Auftragnehmers, dessen Ausstattung, Geschäftsgeheimnisse des Auftragnehmers und Sicherheitsmaßnahmen, verpflichtet ist. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen. Eine die Kontrolle im Namen des Auftraggebers durchführende Person muss mindestens eine Woche vor Durchführung der Kontrolle ihre Legitimation durch den Auftraggeber schriftlich oder per Telefax nachweisen.

(7) Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von schwerwiegenden Vorkommnissen durchzuführen.

(8) Die Kosten für die Durchführung der Kontrolle trägt der Auftraggeber. Das Ergebnis der Prüfung wird dem Auftragnehmer auf Verlangen in geeigneter Form (Gutachten, Testat, Berichte, Berichtsauszüge, etc.) zur Verfügung gestellt. Der Auftragnehmer erhält vom Auftraggeber eine pauschale Aufwandsentschädigung für seinen im Rahmen dieser Kontrollen anfallenden Aufwand in Höhe von 150 Euro pro Stunde.

10. Unterauftragnehmer (weiterer Auftragsverarbeiter nach Art. 28 Abs. 2 und 4 DSGVO)

(1) Die Weitergabe von Aufträgen im Rahmen der im Hauptvertrag konkretisierten Tätigkeiten an Subunternehmer oder Unterauftragnehmer (im Folgenden einheitlich: Unterauftragnehmer) durch den

Auftragnehmer bedarf der vorherigen gesonderten oder allgemeinen schriftlichen Genehmigung durch den Auftraggeber. Gleiches gilt für die Ersetzung eines bestehenden Unterauftragnehmers.

(2) Der Auftraggeber erteilt hiermit die allgemeine Genehmigung, weitere Unterauftragnehmer hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen Unterauftragnehmer ergeben sich aus Anlage 2, für welche die Genehmigung mit Unterzeichnung dieser Vereinbarung als erteilt gilt. Der Auftragnehmer informiert den Aufraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen diese Änderung Einspruch zu erheben (Art. 28 Abs. 2 DSGVO). Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Erfolgt kein Einspruch innerhalb von 14 Tage ab Bekanntgabe, gilt die Genehmigung zur Änderung als gegeben. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

(3) Erteilt der Auftragnehmer unter Beachtung von Abs. 1 Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen nach Artt. 44 ff. DSGVO sicher.

(5) Keiner Zustimmung bedarf die Einschaltung von Unterauftragnehmern, bei denen der Unterauftragnehmer lediglich eine Nebenleistung zur Unterstützung bei der Leistungserbringung nach dem Hauptvertrag in Anspruch nimmt, auch wenn dabei ein Zugriff auf die Daten des Auftraggebers nicht ausgeschlossen werden kann; dazu zählen insbesondere Telekommunikationsleistungen, Post- oder Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragnehmer wird mit solchen Unterauftragnehmern branchenübliche Geheimhaltungsvereinbarungen treffen.

11. Löschung von Daten und Rückgabe von Datenträgern

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrags – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Daten des Auftraggebers, die Gegenstand dieser Vereinbarung sind, zu löschen und von dem Auftraggeber erhaltene Datenträger, die zu diesem Zeitpunkt noch Daten des Auftraggebers enthalten, an den Auftraggeber auszuhändigen. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) Führt eine vom Auftraggeber verlangte Löschung der Daten des Auftraggebers dazu, dass der Auftragnehmer seine Leistungspflichten nach dem Hauptvertrag nicht mehr ordnungsgemäß erbringen kann, wird der Auftragnehmer von der Verpflichtung zur Leistung frei.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

12. Haftung

(1) Der Auftragnehmer haftet dem Auftraggeber für Vorsatz oder grobe Fahrlässigkeit und im Falle von Arglist, für Personenschäden, bei der Haftung nach dem Produkthaftungsgesetz und der bei Fehlen einer Beschaffenheit, für die der Auftragnehmer eine Garantie übernommen hat nach Maßgabe der gesetzlichen Bestimmungen.

(2) Im Falle leichter Fahrlässigkeit haftet der Auftragnehmer nur für Schäden, die auf einer wesentlichen Pflichtverletzung beruhen, die die Erreichung des Vertragszwecks gefährdet, oder auf der Verletzung von Pflichten, deren Erfüllung die ordnungsgemäße Durchführung dieser Auftragsdatenverarbeitung überhaupt erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf. Die Haftung des Auftragnehmers ist in diesen Fällen der Höhe nach beschränkt auf die Höhe des vorhersehbaren Schadens, mit dessen Entstehung typischerweise gerechnet werden muss.

(3) Die Haftungsbeschränkungen gemäß den vorstehenden Regelungen gelten auch für etwaige Schadensersatzansprüche gegen die Organe, leitenden Angestellte, Mitarbeiter oder Beauftragte des Auftragnehmers.

(4) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung beim Auftragnehmer im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

13. Schlussvorschriften

(1) Soweit in dieser Vereinbarung keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen dieser Vereinbarung und Regelungen aus sonstigen vertraglichen Abreden, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus dieser Vereinbarung vor.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers oder Änderungen der Anlage - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Hinsichtlich der Datenverarbeitung gemäß dieser Vereinbarung ist das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG) anwendbar.

Von dieser Vereinbarung haben beide Vertragsschließenden je ein Exemplar erhalten.

Schwyz, 08.04.2026

Kassel, 08.04.2026

Peter Zierl

eTermin GmbH

Matthias Knappe

Betriebsmedizinisches Zentrum Kassel GmbH,
Wilhelmshöher Allee 122, 34119 Kassel,
Deutschland

Anlage 1

Übersicht über die technisch-organisatorischen Maßnahmen

I. Vertraulichkeit

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

1. Zutrittskontrolle (Rechenzentrum)

Die Verarbeitung personenbezogener Daten erfolgt im Microsoft Azure Rechenzentrum in Frankfurt am Main (Deutschland).

Microsoft gewährleistet u. a.:

- Mehrstufige physische Zutrittskontrollen
- Sicherheitsbereiche mit Zugangsbeschränkung
- Videoüberwachung
- ISO 27001- und ISO 27018-Zertifizierung

2. Zugangskontrolle (Systemzugang)

Es wird verhindert, dass Unbefugte Datenverarbeitungssysteme nutzen können.

Ergriffene Maßnahmen:

- Authentifizierung mittels Benutzername und Passwort
- Zwei-Faktor-Authentifizierung für administrative Zugänge
- Kein allgemeiner Root- oder Global-Administrator-Zugriff für Mitarbeiter auf die Cloud-Infrastruktur
- Administrationsrechte werden restriktiv und rollenbasiert vergeben
- IP-Adress-Filterung für Administrations- und Wartungszugänge
- Firewall- und Virenschutzsysteme
- Automatische Sperrung von Endgeräten
- Deaktivierung von Benutzerkonten bei Ausscheiden von Mitarbeitern

3. Zugriffskontrolle (Berechtigungssystem)

Es wird sichergestellt, dass berechtigte Personen nur auf die ihrer Rolle entsprechenden Daten zugreifen können.

Ergriffene Maßnahmen:

- Rollenbasiertes Berechtigungskonzept
- Differenzierte Benutzer- und Administratorrechte
- Zentrale Vergabe von Benutzerrechten
- Trennung von Test- und Produktivumgebungen
- Zugriff auf Kundendaten ausschließlich im Supportfall
- Protokollierung administrativer Zugriffe

4. Trennungskontrolle

Es wird sichergestellt, dass Daten verschiedener Auftraggeber logisch getrennt verarbeitet werden.

Ergriffene Maßnahmen:

- Logische Mandantentrennung mittels eindeutiger Tenant-ID
- Keine mandantenübergreifenden Datenabfragen
- Funktionale Trennung innerhalb der Anwendung

II. Integrität

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

1. Weitergabekontrolle

Es wird verhindert, dass personenbezogene Daten bei der elektronischen Übertragung unbefugt gelesen oder verändert werden können.

Ergriffene Maßnahmen:

- Verschlüsselte Datenübertragung mittels HTTPS unter Verwendung aktueller TLS-Protokolle.
- Zugriff auf Administrationsschnittstellen nur über definierte IP-Adressen
- Protokollierung sicherheitsrelevanter Systemereignisse

2. Eingabekontrolle

Es wird nachvollziehbar dokumentiert, wer personenbezogene Daten eingegeben, verändert oder gelöscht hat.

Ergriffene Maßnahmen:

- Protokollierung von Änderungen und Löschungen von Termindaten
- Nachvollziehbarkeit von Benutzeraktionen innerhalb der Anwendung

III. Verfügbarkeit und Belastbarkeit

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

Es wird sichergestellt, dass personenbezogene Daten gegen Verlust oder Zerstörung geschützt sind.

Ergriffene Maßnahmen:

- Nutzung der hochverfügbaren Infrastruktur von Microsoft Azure
- Redundante Stromversorgung und Brandschutz gemäß Azure-Standard
- Regelmäßige Datensicherungen
- Schutz vor Schadsoftware
- Monitoring der Systemverfügbarkeit
- Löschung oder Rückgabe personenbezogener Daten nach Vertragsende gemäß den vertraglichen Vereinbarungen
- Keine dauerhafte lokale Speicherung von Kundendaten außerhalb der Produktivsysteme
- Konfigurierbare Aufbewahrungsdauer von Terminen nach Terminende
- Konfigurierbare Aufbewahrungsdauer nach Löschung

- Möglichkeit zur Anonymisierung von Termindaten anstelle einer Löschung
- Konfigurierbare Aufbewahrungsdauer von Kontaktdaten nach dem zuletzt gebuchten Termin

IV. Auftragskontrolle

(Art. 28 DSGVO)

Es wird sichergestellt, dass personenbezogene Daten ausschließlich gemäß den Weisungen des Auftraggebers verarbeitet werden.

Ergriffene Maßnahmen:

- Abschluss eines Auftragsverarbeitungsvertrages gemäß Art. 28 DSGVO
- Klare vertragliche Regelung von Rechten und Pflichten
- Der Einsatz von Unterauftragsverarbeitern erfolgt ausschließlich auf Grundlage eines Vertrags gemäß Art. 28 DSGVO.
- Der Auftraggeber wird über beabsichtigte Änderungen in Bezug auf Unterauftragsverarbeiter informiert, sofern dies vertraglich vereinbart ist.
- Der Unterauftragsverarbeiter Microsoft (Azure, Rechenzentrum Frankfurt am Main) ist vertraglich zur Einhaltung geeigneter technisch-organisatorischer Maßnahmen verpflichtet.
- Zugriff auf Kundendaten ausschließlich im Rahmen von Support- oder Wartungsfällen
- Dokumentation von Supportzugriffen
- Keine Weitergabe personenbezogener Daten an Dritte ohne vertragliche Grundlage
- Verpflichtung aller Mitarbeiter auf Vertraulichkeit

V. Verfahren zur regelmäßigen Überprüfung und Bewertung

(Art. 32 Abs. 1 lit. d DSGVO)

Es wird eine regelmäßige Überprüfung der getroffenen Maßnahmen durchgeführt.

Ergriffene Maßnahmen:

- Regelmäßige Überprüfung von Benutzerberechtigungen
- Installation von Sicherheitsupdates für eingesetzte Systeme
- Dokumentation sicherheitsrelevanter Vorfälle
- Interne Sensibilisierung der Mitarbeiter im Bereich Datenschutz

VI. Endgerätesicherheit (Organisatorische Maßnahmen)

Ergriffene Maßnahmen:

- Vollverschlüsselung aller Unternehmensendgeräte mittels Festplattenverschlüsselung
- Passwort-/PIN-/biometrischer Geräteschutz
- Automatische Gerätesperre bei Inaktivität
- Kein lokales Speichern von Kundendaten

VII. Verfahren bei Sicherheitsvorfällen

(Art. 33 DSGVO – Meldepflicht)

Es bestehen interne Prozesse zur Behandlung sicherheitsrelevanter Vorfälle.

Ergriffene Maßnahmen:

- Dokumentation sicherheitsrelevanter Ereignisse
- Interne Bewertung möglicher Datenschutzverletzungen
- Unverzügliche Information des Auftraggebers bei Vorliegen einer meldepflichtigen Datenschutzverletzung
- Unterstützung des Auftraggebers bei der Erfüllung gesetzlicher Meldepflichten

Anlage 2

Übersicht über die Die vom Auftragnehmer eingesetzten Unterauftragnehmer gem. Ziff 10 Abs. 2

Firma Unterauftragnehmer	Anschrift/Land	Beschreibung der übernommenen Teilleistung
Microsoft Ireland Operations Limited	Carmanhall Road Sandyford Business Estate Dublin 18	Hosting der eTermin Server, Microsoft Azure Cloud, Rechenzentrum Standort Frankfurt in Deutschland