Vereinbarung zur Auftragsdatenverarbeitung gem. § 11 BDSG

Zwischen der

……..
(Ihr Unternehmensname und Adresse)

- nachstehend **Auftraggeber** genannt -

und der

Firma **eTermin GmbH**, Im Wiesengrund 8, 8304 Wallisellen, Schweiz

- nachstehend **Auftragnehmer** genannt -

Präambel

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

Durch diese Vereinbarung werden die datenschutzrechtlichen Verpflichtungen der Parteien im Hinblick auf die Erfordernisse des § 11 BDSG (Auftragsdatenverarbeitung) konkretisiert.

1. Anwendungsbereich, Gegenstand und Dauer des Auftrags, Art und Zweck 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.

(3) Die Laufzeit und Kündigung dieser Vereinbarung richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieser Vereinbarung. Eine isolierte Kündigung dieser Vereinbarung ist ausgeschlossen.

(4) Die Verarbeitung der Daten findet ausschließlich im Gebiet der Schweiz und/oder in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland (außer der Schweiz) bedarf der

vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

2. Art der Daten und Kreis der Betroffenen

(1) Gegenstand der Erhebung und Verarbeitung personenbezogener Daten sind folgende Datenkategorien:

- 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)

(2) Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrages Betroffenen umfasst:

- Kunden/Vertragspartner, künftige Vertragspartner oder Interessenten des Auftraggebers
- Beschäftigte (i. S. d. § 3 Abs. 11 BDSG) des Auftraggebers

3. Verantwortlichkeit für die Datenverarbeitung

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der Daten des Auftraggebers sowie für die Wahrung der Rechte der Betroffenen verantwortlich. 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.

(3) Die Inhalte dieser Vereinbarung gelten im Sinne des § 11 Abs. 5 BDSG entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

4. Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer sichert die Umsetzung und Einhaltung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen gem. § 9 BDSG und der Anlage zu § 9 BDSG 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. 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 Straßburg. 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. Berichtigung, Sperrung und Löschung von Daten; Anfragen von Betroffenen

(1) Der Auftragnehmer hat nur nach Weisung des Auftraggebers unter Beachtung von Ziff. 10 dieser Vereinbarung die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener 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) Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen. Im Fall der Geltendmachung der Betroffenenrechte auf Berichtigung, Löschung, Sperrung oder auf Auskunft bezüglich Daten des Auftraggebers hat der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Ansprüche in angemessenem und für den Auftraggeber erforderlichen Umfang zu unterstützen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung des Auftragnehmers erfüllen kann. Der Auftragnehmer erhält vom Auftraggeber eine Entschädigung für seinen im Rahmen der Mitwirkung anfallenden Aufwand in Höhe von 150 Euro pro Stunde.

6. Pflichten des Auftragnehmers

(1) 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. 7 dieser Vereinbarung einschließt, in Übereinstimmung mit den Bestimmungen dieser Vereinbarung erfolgt.

(2) 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.

(3) 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.

(4) Der Auftragnehmer ist verpflichtet, einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten nach § 4f BDSG zu bestellen, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind.

(5) Der Auftragnehmer hat die bei der Verarbeitung von Daten des Auftraggebers beschäftigten Personen gemäß § 5 BDSG schriftlich auf das Datengeheimnis zu verpflichten.

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der zuständigen Datenschutzaufsichtsbehörde informieren, sofern hiervon Daten des Auftraggebers betroffen sind.

7. Unterauftragsverhältnisse

(1) Der Auftragnehmer darf Unterauftragsverhältnisse hinsichtlich der Verarbeitung oder Nutzung von Daten des Auftraggebers nur nach vorheriger schriftlicher Zustimmung des Auftraggebers begründen. Eine solche vorherige Zustimmung darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund verweigert werden. Derzeit setzt der Auftragnehmer als Unterauftragnehmer den Betreiber des Rechenzentrums (Host Europe) – in diesem Fall erteilt der Auftraggeber hiermit ausdrücklich seine Zustimmung. Der Auftragnehmer wird dem Auftraggeber auf Anforderung eine aktuelle Übersicht über die eingeschalteten Unterauftragnehmer übergeben.

(2) Keiner Zustimmung bedarf die Einschaltung von Subunternehmern, bei denen der Subunternehmer 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 Transportleistungen von Post- oder Kurierdiensten sowie Geldtransportdienstleistungen, Telekommunikationsdienste, Bewachungsdienste und Reinigungsdienste, nicht aber Prüfungs- und Wartungsleistungen i.S.v. § 11 Abs. 5 BDSG. Der Auftragnehmer wird mit solchen Subunternehmern branchenübliche Geheimhaltungsvereinbarungen treffen.

(3) Der Auftragnehmer hat sicherzustellen, dass die in dieser Vereinbarung vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber den betreffenden Subunternehmern gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

8. Kontrollrechte des Auftraggebers

(1) Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags 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.

(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 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.

9. Mitzuteilende Verstöße des Auftragnehmers

(1) Der Auftragnehmer informiert den Auftraggeber zeitnah, 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, sofern deshalb die Gefahr besteht, dass Daten des Auftraggebers unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.

(2) Soweit den Auftraggeber aufgrund eines Vorkommnisses nach Ziff 9 Abs. 1 dieser Vereinbarung gesetzliche Informationspflichten wegen einer unrechtmäßigen Kenntniserlangung von Daten des Auftraggebers (insbesondere nach § 42a BDSG) 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.

10. 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, 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 entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

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.

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.

.....	.....
Ort und Datum	Ort und Datum
.....	.....
Unterschrift eTermin GmbH	Unterschrift Auftraggeber

Anlage

Übersicht über die technisch-organisatorischen Maßnahmen

Die Anwendung eTermin wird primär über ein Rechenzentrum betrieben, wo auch die relevanten personenbezogenen Daten verarbeitet werden.
Das hierfür eingesetzte Rechenzentrum in Straßburg/Frankreich ist beim DCSA (Data Center Star Audit, Version 3.0) mit der Höchstwertung von fünf Sternen ausgezeichnet.

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

Ergriffene Maßnahmen in den Büroräumlichkeiten:

- Festlegung der zugangsberechtigten Personen
- Closed Shop-Betrieb, kein Besucherverkehr
- Schlüsselregelung und aktuelle Schlüsselliste
- Verschlossene Bürotüren und Fenster bei Abwesenheit

Ergriffene Maßnahmen im Rechenzentrum:

- Sicherheitsbereich mit Eingangskontrolle
- eingezäuntes Gelände inkl. Videoüberwachung
- Regelmäßige Kontrollgänge durch das Sicherheitspersonal
- Zutrittskontrollsystem mit Chipkarten.

2. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Ergriffene Maßnahmen:

- Festlegung der nutzungsberechtigten Personen
- Identifikation und Authentifizierung der Benutzer durch Login
- Firewall, Virenschutz
- Automatische Sperrung der Endgeräte mit Passwortschutz bei Pausen
- Zugang auf Datenverarbeitungssysteme zu Wartungszwecken nur über wenige, zuvor explizit erlaubte IP Adresse

3. Zugriffskontrolle

Es ist Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Ergriffene Maßnahmen:

- Berechtigungskonzept mit differenzierten Berechtigungen (sowohl für Anwender, als auch für Administratoren)
- Identifikation und Authentifizierung der Benutzer
- Zentrale Vergabestelle von Benutzerrechten

4. Weitergabekontrolle

Es ist Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Ergriffene Maßnahmen:

- Physikalische Löschung aller Datenträger vor einer neuen Beschreibung und nach jeder Verarbeitung
- Überprüfung aller Daten und Datenträger hinsichtlich Virenbefall
- Protokollierung der Datenübermittlung
- Fernwartungskonzept
- Verschlüsselte Datenübertragungen zwischen Endgeräten und Rechenzentrum

5. Eingabekontrolle

Es ist Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Ergriffene Maßnahmen:

- Festlegung von Eingabebefugnissen
- Protokollierung der Eingaben , Veränderungen und Löschungen von Terminen

6. Auftragskontrolle

Es ist eine auftrags- und weisungsgemäße Auftragsdatenverarbeitung zu gewährleisten.

Ergriffene Maßnahmen:

- Klare Vertragsgestaltung und -ausführung
- Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber
- Sorgfältige Auswahl des Auftragnehmers
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrages

7. Verfügbarkeitskontrolle

Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Ergriffene Maßnahmen in den Büroräumlichkeiten:

- Backup-Systeme zur Wiederherstellung verlorener Daten
- Räumlich getrennte Aufbewahrung der erstellten Datensicherungen
- Virenschutzkonzept
- Zentrale Datensicherung

Ergriffene Maßnahmen im Rechenzentrum:

- unterbrechungsfreie Stromversorgung (USV) und Netzersatzanlage
- redundante Stromversorgung der Server
- Überspannungsschutz
- Branderkennungs- und Frühwarnsystem, Löschanlage
- Backup-Systeme zur Wiederherstellung verlorener Daten

8. Trennungskontrolle

Es ist Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Ergriffene Maßnahmen:

- Datenspeicherung wird mit dem Zweck der Datenerhebung versehen (z.B. durch Dateibezeichnung)
- Mandantentrennung - Logische Trennung der Daten (basierend auf UID)
- Funktionstrennung