**Vertrag zur Prüfung und Wartung von**

**informationstechnischen Systemen**

**A C H T U N G !**

**ALLGEMEINER HINWEIS**

 **für die**

**VERWENDUNG DES NACHFOLGENDEN MUSTER-VERTRAGES**

**Bei dem nachfolgenden Vertrag handelt es sich um einen unverbindlichen MUSTER-Vertrag, der der Darstellung und Erläuterung vielfach anzutreffender Regelungen in Verträgen zur IT-Wartung dient.**

**Der MUSTER-Vertrag erhebt keinen Anspruch auf Vollständigkeit, sondern gibt lediglich unver­bindliche Anhaltspunkte für eine mögliche Vertragsgestaltung. Der MUSTER-Vertrag muss deshalb individuell überprüft und den Praxisverhältnissen im Einzelfall angepasst werden. Er ersetzt keinesfalls eine Beratung durch einen Rechtsanwalt. Für die Verwendung oder Nutzung des MUSTER-Vertrages haftet die jeweilige Anwenderin bzw. der jeweilige Anwender.**

**Vertrag zur Prüfung und Wartung von informationstechnischen Systemen**

zwischen

der Firma

Name Firma

Straße Firma

PLZ Ort Firma

vertreten durch Ansprechpartner Firma - im Folgenden „Auftragnehmer“ genannt -

und

der Zahnarztpraxis

Name Praxis

Straße Praxis

PLZ Ort Praxis - im Folgenden „Auftraggeber“ genannt -

gemeinsam „die Vertragsparteien“ genannt.

**§ 1**

**Gegenstand und Dauer des Auftrags**

1. Der Auftraggeber hat den Auftragnehmer mit der Wartung der beim Auftraggeber vorhandenen informationstechnischen Systeme beauftragt. Im Zuge dessen erfolgt auch eine Fernwartung beim Auftraggeber durch Aufbau externer Kommunikationsverbindungen („Remote-Zugriff“).
2. Da nicht ausgeschlossen werden kann, dass der Auftragnehmer in Erfüllung seiner Aufgaben, einen Zugriff auf personenbezogene Daten erhält, erfolgt die Dienstleistung als Auftragsdatenverarbeitung nach den für den Auftraggeber einschlägigen deutschen und europäischen Datenschutzgesetzen.
3. Dieser Vertrag beginnt mit Unterzeichnung beider Vertragsparteien. Er endet jedoch nicht vor Erfüllung der Lösch- und Rückgabepflichten nach § 10 dieses Vertrages.
4. Eine Verarbeitung erfolgt nur, soweit dies im zugrundeliegenden Leistungsvertrag vereinbart oder geregelt ist. Hierunter fallen ebenfalls Tätigkeiten bei denen Daten von einem System in ein anderes migrieren.
5. Die beim Auftraggeber durch Remotezugriff oder Datenmigration betroffenen personenbezogenen Daten sind nach ihrem Umfang, der Art und dem Zweck der vorgesehenen Erhebung, der Verarbeitung oder Nutzung von Daten, der Art der Daten und dem Kreis der Betroffenen vom Auftraggeber vor der Auftragserteilung schriftlich zu fixieren.

**§ 2**

**Technische und organisatorische Maßnahmen**

1. Der Auftragnehmer verpflichtet sich, für die zu verarbeitenden Daten angemessene und dem Stand der Technik entsprechende technische und organisatorische Sicherheitsmaßnahmen nach den für den Auftraggeber einschlägigen deutschen und europäischen Datenschutzgesetzen zu treffen. Der Auftragnehmer berücksichtigt dabei insbesondere die Vorgaben des Art. 32 EU-Datenschutz-Grundverordnung (EU-DSGVO), wie

a) Zutrittskontrolle

b) Zugangskontrolle

c) Zugriffskontrolle

d) Weitergabekontrolle

e) Eingabekontrolle

f) Auftragskontrolle

g) Verfügbarkeitskontrolle

h) Trennungskontrolle

1. Die Datensicherheitsmaßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind vom Auftragnehmer mit dem Auftraggeber schriftlich abzustimmen. Diese sind für die Dauer des Auftragsverhältnisses aufzubewahren.
2. Der Auftragnehmer ist verpflichtet, ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 EU-DSGVO) über die durch ihn im Auftrag verarbeiteten Daten zu erstellen und dieses dem Auftraggebers zur Verfügung zu stellen. Das Verzeichnis ist regelmäßig vom Auftragnehmer auf Aktualität zu prüfen und dem Auftraggeber ohne besondere Aufforderung die jeweils aktuelle Fassung des Verzeichnisses vom Auftragnehmer zur Verfügung zu stellen.
3. Der Auftragnehmer stellt dem Auftraggeber auf Anforderung ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsdatenverarbeitung sowie die zugriffsberechtigten Personen zur Verfügung.

**§ 3**

**Berichtigung, Löschung und Sperrung von Daten**

Der Auftragnehmer darf die Daten, die er im Auftrag des Auftraggebers verarbeitet, nur berichtigen, löschen und sperren, wenn der Auftraggeber dies anweist. Der Auftragnehmer fertigt ohne Wissen des Auftraggebers keine Kopien oder Duplikate der Daten.

**§ 4**

**Pflichten des Auftragnehmers**

1. Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes unter Berücksichtigung des Berufsgeheimnisschutzes des Auftraggebers gerecht wird.
2. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis und die Vertraulichkeit verpflichtet worden sind. Dabei berücksichtigt der Auftragnehmer auch, dass ihm vom Auftraggeber Daten zur Verfügung gestellt werden, die dem besonderen Berufsgeheimnisschutz unterfallen. Die Verpflichtung ist so zu fassen, dass sie auch nach Beendigung eines Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleibt. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Form nachzuweisen.
3. Der Auftraggeber wird dem Auftragnehmer nur die für die Durchführung der vereinbarten Tätigkeit benötigten Zugriffsrechte bereitstellen, deren Aktualisierung regelmäßig überprüfen und ggf. Korrekturen vornehmen. Der Auftragnehmer darf von den ihm eingeräumten Zugriffsrechten nur in dem für die Durchführung der Tätigkeit unerlässlich notwendigen Umfang Gebrauch machen.
4. Der Auftraggeber hat das Recht, den Zugriff des Auftragnehmers auf die informationstechnischen Systeme des Auftraggebers zu unterbrechen. Dies insbesondere, wenn der Verdacht besteht, dass unbefugt auf Informationen und Ressourcen zugegriffen wird.
5. Notwendige Datenübertragungen zu Zwecken des Zugriffs müssen in hinreichend verschlüsselter Form erfolgen; Ausnahmen sind besonders zu begründen.
6. Soweit gesetzlich vorgeschrieben, bestellt der Auftragnehmer schriftlich einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Über einen Wechsel der Person des Beauftragten für Datenschutz beim Auftragnehmer ist der Auftraggeber unverzüglich zu unterrichten.
7. Der Auftraggeber ist dazu berechtigt, sämtliche Aktionen des Auftragnehmers innerhalb seiner Infrastruktur zu protokollieren und auszuwerten.
8. Der Auftragnehmer darf die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich im Geltungsbereich der EU-DSGVO erheben, verarbeiten oder nutzen. Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen den für den Auftraggeber einschlägigen Datenschutzgesetzen erfüllt sind.
9. Soweit Daten durch den Auftragnehmer verarbeitet werden, sichert dieser zu, dass diese von sonstigen Datenbeständen strikt getrennt werden.
10. Der Auftragnehmer unterstützt den Auftraggeber bei allen gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsdatenverarbeitung stehen. Auskünfte an Betroffene oder Dritte darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers erteilen. Soweit ein Betroffener seine Rechte nach den einschlägigen Datenschutzgesetzen unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
11. Dem Auftragnehmer ist bekannt, dass der Auftraggeber Berufsgeheimnisträger ist und Verstöße dagegen nach § 203 StGB strafbewährt sind.

**§ 5**

**Berechtigung zur Begründung von Unterauftragsverhältnissen**

1. Der Auftragnehmer darf Unterauftragnehmer zur Verarbeitung von Daten des Auftraggebers nur mit schriftlicher Zustimmung des Auftraggebers beauftragen. Der Auftragnehmer sichert für diesen Fall zu, dass die vertraglichen Vereinbarungen mit dem Unterauftragnehmer, den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen. In dem Vertrag mit dem Unterauftragnehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragnehmers deutlich voneinander abgegrenzt werden. Der Auftragnehmer prüft die Einhaltung der Vertragspflichten durch den Unterauftragnehmer regelmäßig und dokumentiert dies.
2. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählt z. B. der Einsatz von Reinigungskräften. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

**§ 6**

**Kontrollrechte des Auftraggebers**

 Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber oder eine von ihm beauftragte Person, berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften, die Einsichtnahme in die Datenverarbeitungsprogramme oder durch Zugang zu den Arbeitsräumen des Auftragnehmers. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

**§ 7**

**Mitzuteilende Verstöße des Auftragnehmers**

1. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Auftraggebers mit sich bringen sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten des Auftraggebers. Gleiches gilt, wenn der Auftragnehmer feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.
2. Meldungen über eine Verletzung des Schutzes personenbezogener Daten an den Auftraggeber erfolgen schriftlich und enthalten
* eine Beschreibung der Art der Verletzung und soweit möglich Angaben über Kategorie und Zahl der betroffenen Datensätze
* eine Erläuterung der vom Auftragnehmer ergriffenen Maßnahmen zur Behebung der Verletzung und Verringerung möglicher nachteiliger Auswirkungen

**§ 8**

**Weisungen des Auftraggebers**

1. Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Datenverarbeitung sowie für die Wahrung der Betroffenenrechte, allein verantwortlich.

1. Der Auftraggeber hat das Recht, dem Auftragnehmer Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Grundsätzlich können Weisungen mündlich erteilt werden. Mündlich erteilte Weisungen sind zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn der Auftragnehmer dies verlangt.
2. Der Auftragnehmer verarbeitet die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen des Auftraggebers und im Rahmen der getroffenen Vereinbarungen.
3. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.
4. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

**§ 9**

**Beendigung**

1. Nach Beendigung des Vertragsverhältnisses hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Datenträger und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Vertragsverhältnis stehen, an den Auftraggeber zurückzugeben. Nicht mehr benötigte Daten sind durch den Auftragnehmer unverzüglich zu löschen, sofern der Löschung keine gesetzlichen Speicherfristen entgegenstehen. Hierüber ist der Auftragnehmer durch den Auftraggeber schriftlich in Kenntnis zu setzen.
2. Der Auftraggeber kann das Vertragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragnehmer einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen gesetzliche Bestimmungen der für den Auftraggeber einschlägigen deutschen und europäischen Datenschutzgesetzen begeht und dem Auftraggeber aufgrund dessen die Fortsetzung des Vertrages bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.
3. Nach Abschluss der Auftragsdatenverarbeitung hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Datenträger und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, an den Auftraggeber zurückzugeben. Nicht mehr benötigte Daten sind durch den Auftragnehmer unverzüglich zu löschen, sofern der Löschung keine gesetzlichen Speicherfristen entgegenstehen. Hierüber ist der Auftragnehmer durch den Auftraggeber schriftlich in Kenntnis zu setzen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.
4. Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über Personen, Geschäftsgeheimnisse und Datensicherheitsmaßnahmen auch nach Beendigung des Vertrages vertraulich zu behandeln.

**§ 10**

**Haftung**

Auf Art. 82 EU-DSGVO wird hingewiesen.

**§ 11**

**Schlussbestimmungen**

1. Die Vertragsparteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Vertragspartei vertraulich zu behandeln. Geschäftsgeheimnisse sind alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Geheimnisträger ein berechtigtes Interesse hat. Datensicherheitsmaßnahmen sind alle technischen und organisatorischen Sicherheitsmaßnahmen, die eine Partei nach den für den Auftraggeber einschlägigen deutschen und europäischen Datenschutzgesetzen getroffen hat. Diese Geheimhaltungspflicht besteht nach Beendigung dieses Vertrags fort.
2. Sofern eine Vertragspartei weiteren Geheimnisschutzregeln unterliegt und sie dies der anderen Vertragspartei zu Vertragsbeginn schriftlich mitteilt, ist auch diese Vertragspartei verpflichtet, die Geheimnisschutzregeln zu beachten.
3. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Auftraggebers ausgeschlossen.
4. Für Vertragsänderungen und Nebenabreden ist die Schriftform erforderlich.
5. Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

…………………………………………… ……………………………………………

Ort, Datum Ort, Datum

…………………………………………… ……………………………………………

Auftraggeber Auftragnehmer

**Anhang: Umfang der Datenverarbeitung**

**(Art der Verarbeitung, Art der Daten, Zweck der Erhebung, Nutzung der Daten, Kreis der Betroffenen)**

**Mögliches Beispiel IT-Dienstleister**

Art der Verarbeitung: Erfassen, Organisation, Speicherung, Auslesen, Abfragen, und Verwendung personenbezogener Daten

Art der personenbezogenen Daten: Name, Adresse, Geburtsdatum, Versichertenstatus, Geschlecht und ggf. Gesundheitsdaten, je nach Erfordernis

Nutzung der Daten: Erbringung des Wartungsvertrages für die IT-Systeme der Praxis

Kategorie betroffener Personen: Patienten und ggf. Daten von Mitarbeitern der Praxis