Vereinbarung für den Remote-Zugriff auf die Software OpTra®Dent

Diese Vereinbarung inkl. der Anlage dient der Gewährleistung von Informations- und Datensicherheit für Auftraggeber und Auftragnehmer gemäß des Datenschutzgesetzes 2018.

Bitte lesen Sie die Vereinbarung sorgsam durch und senden Sie diese unterschrieben an uns zurück.
Durch Ihre Unterschrift bestätigen Sie, dass Sie die genannten Informationen zur Kenntnis genommen und inhaltlich verstanden haben.

Sie erklären sich damit einverstanden, dass die Dental Innovation GmbH Daten von Ihrem System einsehen und ggf. für einen Fehler-Analyseprozess kopieren darf.

Die Dental Innovation GmbH garantiert Ihnen, dass die Daten nach der Bearbeitung von deren Systemen gelöscht werden. Eine zusätzliche Bestätigung über die Löschung der Daten erfolgt nicht.

Vielen Dank.

Vereinbarung zwischen der

Dental Innovation GmbH (Auftragnehmer)
Otto Hahn Straße 15
D-**44227 Dortmund**
Telefon: + 49 231 725469-300 Zentrale

und

dem Auftraggeber

vollständige Anschrift oder Stempel

1. Gegenstand der Vereinbarung

1.1 Die Mitarbeiter des Auftragnehmers sollen, falls im Supportfall erforderlich, mit einer Software (zurzeit TeamViewer) einen Fernzugriff auf die bei Ihnen installierte Software OpTra®Dent vornehmen können.
Bei diesem Zugriff können dem Auftragnehmer zwangsläufig personenbezogene Daten zugänglich werden, zum Beispiel von Mitarbeitern und Patienten des Auftraggebers (insbesondere die Patientenakte).
Die Einzelheiten dieses Zugriffs werden durch diese Vereinbarung geregelt.

1.2 Für die Beurteilung der Zulässigkeit des Zugriffs auf personenbezogene Daten sowie für die Wahrung der Rechte der Betroffenen ist der Auftraggeber verantwortlich, er ist "Herr der Daten" und trägt Sorge, dass die Voraussetzungen für eine ggf. erforderliche Zugänglichmachung und Verarbeitung von Patientendaten durch den Auftragnehmer erfüllt sind (Offenbarungsbefugnis).

2. Laufzeit der Vereinbarung

Die Vereinbarung ist mit einer Frist von einem Monat zum Quartalsende kündbar. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Eine Kündigung bedarf zu ihrer Wirksamkeit der Schriftform (Telefax oder eMail mit Bestätigungs-eMail durch die Dental Innovation GmbH).

3. Weisungen des Auftraggebers

Der Auftragnehmer darf den Zugriff nur im Rahmen der Weisungen des Auftraggebers durchführen. Der Auftragnehmer wird den Auftraggeber informieren, wenn eine vom Auftraggeber erteilte Weisung nach Auffassung des Auftragnehmers gegen gesetzliche Vorschriften verstößt.
Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.
Der Auftraggeber kann durch Einzelweisungen die Berichtigung, Löschung und Sperrung von Daten verlangen, die der Auftragnehmer bei dem Zugriff erhalten hat.

4. Mitwirkung des Auftraggebers

4.1 Der Auftraggeber hat dafür zu sorgen, dass eine tagesaktuelle Datensicherung vorhanden ist.

4.2 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er im Rahmen der Beauftragung Fehler oder Unregelmäßigkeiten feststellt.

5. Kontrollrechte des Auftraggebers

Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren. Der Auftragnehmer wirkt hierbei mit.

6. Durchführung des Zugriffs

6.1 Der Zugriff wird ausschließlich von den Geschäftsräumen des Auftragnehmers aus vorgenommen und nur mit vorheriger Zustimmung des Auftraggebers. Hierzu wird ein Verfahren zur Einleitung des Zugriffs (Benachrichtigung, Freischaltung) vereinbart.
Der Auftraggeber kann jeden Zugriff ununterbrochen begleiten und überwachen.

6.2 Der Zugriff ist unter einer separaten, über Identifikations- und Authentisierungsmechanismen (Benutzerkennung, Passwort, Token etc.) geschützten Zugangskennung durchzuführen.
Solange ein Zugriff nicht erforderlich ist, sollte die Zugangskennung deaktiviert sein. Die Zugriffsmöglichkeiten sind auf das erforderliche Maß zu beschränken. Für Arbeiten, die besondere Berechtigungen erfordern, sind gesonderte Zugangskennungen einzurichten.

6.3 Der Auftragnehmer dokumentiert Zeitpunkt, sowie Art und Umfang eines Zugriffs, so dass dieser hinreichend nachvollzogen werden kann.
Dabei muss insbesondere erkennbar sein, von wem, zu welchem Zeitpunkt, auf welche Daten, Zugriff genommen wurde bzw. welche Arbeiten durchgeführt wurden. Die Protokolle sind für die Dauer von zwölf Monaten aufzubewahren und dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

6.4 Daten dürfen aus dem IT-System des Auftraggebers nur mit dessen Zustimmung übernommen werden. Der Auftragnehmer darf erhaltene Daten ausschließlich für die Durchführung der Hotline-Leistungen verarbeiten oder nutzen.

6.5 Datenträger mit personenbezogenen Daten, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden (z.B. Sicherungsdatenträger), sind eindeutig zu kennzeichnen. Eingang und Ausgang bzw. der Verbleib sind zu dokumentieren.

6.6 Im Rahmen des Zugriffs erhaltene Daten und Datenträger sind dem Auftraggeber bei Vertragsende zu übergeben oder auf sein Verlangen hin zu löschen bzw. ordnungsgemäß zu vernichten.
Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen.

7. Unterauftragnehmer

Die Beauftragung von Unterauftragnehmern im Rahmen des Zugriffs ist dem Auftragnehmer nur mit schriftlicher Zustimmung des Auftraggebers erlaubt.

8. Technische und organisatorische Maßnahmen

8.1 Der Auftragnehmer trifft die gemäß § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen und gestaltet die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Schutzes personenbezogener Daten gerecht wird. Die Maßnahmen sind in Anlage 1 beschrieben. Sie können im Laufe des Auftragsverhältnisses der Weiterentwicklung angepasst werden.

8.2 Der Auftraggeber ist berechtigt, sich von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen.

8.3 Sollte sich beim Supporteinsatz herausstellen, dass das Betriebssystem des Anwenderrechners nicht aktuell ist und aus diesem Grund eine Beeinträchtigung der Funktionen der Software OpTra®Dent stattfindet, müsste das System eventuell aktualisiert (z.B. Windows-Update) oder konfiguriert werden.

8.4 Sollte der Mitarbeiter der Dental Innovation GmbH direkt mit der Durchführung beauftragt werden, haftet er nicht für Schäden die durch Drittsoftware entstehen könnten.

9. Datenschutzbeauftragter, Datengeheimnis, Auskünfte, Verstöße

9.1 Die Kontaktdaten des/der Datenschutzbeauftragten des Auftragnehmers werden dem Auftraggeber vom Auftragnehmer bekannt gegeben.

9.2 Die mit der Verarbeitung von personenbezogenen Daten des Auftraggebers befassten Mitarbeiter des Auftragnehmers sind dem Datengeheimnis gemäß § 5 BDSG verpflichtet.

9.3 Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

9.4 Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße durch den Auftragnehmer oder der beim Auftragnehmer beschäftigten Personen gegen datenschutzrechtliche Bestimmungen und Unregelmäßigkeiten bei der Durchführung des Zugriffs mit. Dies gilt auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers nach § 42 a BDSG. Der Auftragnehmer wird den Auftraggeber hierbei unterstützen.

10. Widerruf der Datenschutzerklärung

Sie können diese Datenschutzvereinbarung jederzeit widerrufen, indem Sie dies der Dental Innovation GmbH schriftlich mitteilen. Schicken Sie als Auftraggeber Ihren Widerruf mit dem Vermerk „Widerruf zum Onlinesupport“ an den Datenschutzbeauftragten der Dental Innovation GmbH, Otto-Hahn Str. 15, D-44227 Dortmund. Bitte geben Sie in Ihrem Schreiben an, ob Sie eine Bestätigung des Widerrufs benötigen. Andernfalls erfolgt keine weitere Nachricht seitens der Dental Innovation GmbH.

11. Gefährdung durch Maßnahmen Dritter

Werden die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet, informiert der Auftragnehmer den Auftraggeber unverzüglich. Der Auftragnehmer wird ferner alle ihm in diesem Zusammenhang bekannten relevanten Dritte unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

12. Schriftform

Ergänzungen und sonstige Änderungen dieser Vereinbarung bedürfen der Schriftform (§ 11 Abs.2 BDSG).

13. Salvatorische Klausel

Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam oder nichtig sein oder werden, so wird dadurch die Gültigkeit des übrigen Vertragsinhalts nicht berührt. Die Vertragsparteien verpflichten sich erforderlichenfalls in einem solchen Fall, die unwirksame Bestimmung durch eine Regelung zu ersetzen, die dem Zweck der weggefallenen Bestimmung am nächsten kommt und rechtlich zulässig ist.

Auftragnehmer

Dental Innovation GmbH
Dr. Dr. Stephan Weihe
Geschäftsführung Datenschutzbeauftragter

Dortmund

_____

Ort, Datum

Auftraggeber

_____

Ort, Datum

_____

_____

_____

_____

_____

Name /Unterschrift Datum

Anlage Notwendige Vorkehrungen zur Sicherung personenbezogener Daten

Beschreibung der technischen und organisatorischen Maßnahmen der Datensicherung.

1. **Zutrittskontrolle**

   Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

   Verschlossene Türen mit elektrischen Türöffnern. Chipkartenregelung.

2. **Zugangskontrolle**

   Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:
   Bildschirmschoner mit Passwortschutz beim Verlassen des Arbeitsplatzes aktivieren.

3. **Zugriffskontrolle**

   Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

   Freigabe durch den Auftraggeber.

4. **Weitergabekontrolle**

   Maßnahmen, die gewährleisten, 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:

   Authentifizierung durch Zugangscode.

5. **Eingabekontrolle**

   Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind:

   Ständige Überwachung durch den Auftraggeber für die Dauer des Remotezugriffs.
   Ein Eingriff in die vorhandenen Patientendaten findet nicht statt.

6. **Auftragskontrolle**

   Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

   Verarbeitung gemäß Vertrag des Auftraggebers und den Inhalten dieses Dokumentes.

7. **Verfügbarkeitskontrolle**

   Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

   Datensicherung vor der Verbindung beim Auftraggeber.

8. **Trennungskontrolle**

   Es werden keine Daten nach der Trennung mehr übertragen.
   Mit Beendigung des Remotezugriffs erfolgt die absolute Trennung.