Auftragsverarbeitung gemäß Art. 28 DS-GVO

1. Datenverarbeitung in der EU

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen 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. DS-GVO erfüllt sind.

2. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der nach DS-GVO erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren. Diese Maßnahmen sind Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Es handelt es sich bei den zu treffenden Vorkehrungen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Der Auftragnehmer verpflichtet sich zur Umsetzung und weiteren Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1]. Die Prüfung der getroffenen technischen und organisatorischen Maßnahmen durch den Auftraggeber erfolgt im Rahmen seiner Kontrollbefugnisse nach Ziffer 6 dieses Vertrages.

3. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich oder bezüglich anderer Betroffenenrechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit die Parteien dies in einem Vertrag separat vereinbart haben, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

4. Weitere Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags seine gesetzlichen Pflichten aus Art. 28 bis 33 DS-GVO zu erfüllen; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Sofern gesetzlich erforderlich, erfolgt die schriftliche Bestellung eines Datenschutz-beauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Die Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers sind Punkt 10 dieser Vereinbarung zu entnehmen. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO zu wahren. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich durch EU Recht oder nationales Recht des Auftragsverarbeiters zur Verarbeitung verpflichtet sind.

c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

d) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

e) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

f) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

5. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikations-leistungen, Post-/Transportdienstleistungen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Unterauftragnehmer in Anspruch zu nehmen, wenn

- mit dem Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird,
- der Auftragnehmer den Auftraggeber in Textform informiert – zum Beispiel per E-Mail/Newsletter bzw. über einen Link -, wenn er die Hinzuziehung weiterer oder die Ersetzung von Unterauftragnehmern beabsichtigt.

Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben, wobei dies nicht ohne wichtigen datenschutz-rechtlichen Grund erfolgen darf. Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 14 Tagen nach Bereitstellung der Information über die Änderung gegenüber dem Auftragnehmer in Textform an die unten unter Punkt 10 genannten Kontaktdaten des Datenschutzbeauftragten zu erheben. Im Falle des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist - die Leistung

gegenüber dem Auftraggeber innerhalb von 4 Wochen nach Zugang des Einspruchs einstellen und die Leistungsvereinbarung fristlos und mit sofortiger Wirkung kündigen.
(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Auftragnehmers (mind. Textform) oder einer allgemeinen Genehmigung des Auftragnehmers analog Absatz 2. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

6. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig (grundsätzlich mindestens zwei Wochen Vorlauf) anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Betriebs- und Geschäftsgeheimnisse des Auftragnehmers, die dem Auftraggeber bei einer Überprüfung bekannt werden, sind vom Auftraggeber streng vertraulich zu behandeln. Es dürfen keine Aufzeichnungen über solche Geheimnisse gemacht werden, es sei denn, dies ist absolut notwendig, um das Kontrollrecht seitens des Auftraggebers auszuüben.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Datenschutzbeauftragter, Wirtschaftsprüfer, Revision, IT-Sicherheits-abteilung, Datenschutzauditoren, Qualitätsauditoren).
(4) Der Zutritt zu den Betriebsstätten des Auftragnehmers erfolgt ausschließlich in ständiger Anwesenheit eines Vertreters des Auftragnehmers. Dieser Vertreter ist befugt zu entscheiden, wie die Überprüfung in dem erforderlichen Umfang ablaufen soll, um Störungen des Geschäftsbetriebs des Auftragnehmers zu vermeiden und die Geheimhaltungspflichten des Auftragnehmers gegenüber Dritten zu wahren.
(5) Regelmäßige Kontrollen durch den Kunden vor Ort sind maximal einmal pro Kalenderjahr zulässig. Zusätzliche Kontrollen durch den Kunden können nur aus einem wichtigen vom Kunden nachzuweisenden Grund durchgeführt werden.

7. Mitteilung bei Verstößen des Auftragnehmers

Wenn nötig, insbesondere weil die relevanten Informationen dem Auftraggeber nicht anderweitig zur Verfügung stehen, und unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragnehmer den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken

berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten, es sei denn, die Rechtsvorschriften der EU oder des nationalen Rechts erfordern die Speicherung personenbezogener Daten.
(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

10. Konkretisierung des Auftragsinhalts, Unterauftragnehmer und Datenschutzbeauftragter

Gegenstand des Auftrags	Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: • Anfertigung von zahnästhetischen Schien- und Drahtsystemen (insbesondere sog. Aligner und Retainersysteme) nach Vorgaben des Auftraggebers sowie die Herstellung sonstiger Medizinprodukte. Die einzelnen Medizinprodukte sind insbesondere der Website des Auftragnehmers zu entnehmen.

Dauer des Auftrags	Die Laufzeit dieses Auftrags ist begrenzt auf die Dauer der Geschäftsverbindung.
Art und Zweck der vorgesehenen Verarbeitung von Daten	• Der Auftraggeber übermittelt dem Auftragnehmer Patientendaten, auf deren Grundlage das konkrete Medizinprodukt durch den Auftragnehmer gefertigt wird. Zu diesem Zweck hält der Auftragnehmer ein Internetportal zum Hochladen der notwendigen Patienteninformationen bereit. Alternativ erfolgt die Übersendung der Patientendaten postalisch (insbesondere die Übersendung des Zahnabdrucks)
Kategorien betroffener Personen	• Patienten des Auftraggebers
Art der Daten	Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien: • allgemeine Personendaten des Patienten (zum Beispiel: Name, Geburtsdatum, Geschlecht, ID) • Gesundheitsdaten (zum Beispiel: Diagnosedaten, insbesondere Scan/Modell des Kiefers, Patientenhistorie, gewünschtes Medizinprodukt) • Vertragsdurchführungsdaten • körperliche Merkmale (zum Beispiel: Geschlecht, Größe, Gewicht).
Eingesetzte Unterauftragnehmer	1. SCHEU-DENTAL GmbH, Am Burgberg 20, 58642 Iserlohn, Buchhaltung, 2. Timme Hosting GmbH & Co. KG, Ovelgönner Weg 43,21335 Lüneburg, Hosting Services.
Datenschutzbeauftragter des Auftragnehmers	Herr Rechtsanwalt Dietrich Felgner, mip Consult GmbH, Wilhelm-Kabus-Str. 9, 10829 Berlin, 030-2088999-0, d.felgner@mip-consult.de

Anhang 1

Technische und organisatorische Maßnahmen (TOM)

von SCHEU-DENTAL custom-made GmbH

i.S.v.

Art. 25, 32 Datenschutz-Grundverordnung (DSGVO)

Auftragsverarbeiter	
Firma	SCHEU-DENTAL custom-made GmbH
Anschrift des Auftragsverarbeiter	
Straße	Walder Straße 53
Postleitzahl	40724
Ort	Hilden
Telefon	02104 80041-00
Fax	02104 80041-99

A. Vertraulichkeit und Integrität, Art. 32 Abs. 1 lit. b DSGVO

I. Zutritts- und Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (räumlich und technisch).

Technisch-organisatorische Maßnahmen

• Zugangssicherung der Räumlichkeiten über Schließanlage
  ○ Sicherheitsschlüssel mit dokumentierter Schlüsselverwaltung
• Maßnahmen zur Prophylaxe vor und Detektierung von unbefugten Zutritten und Zutrittsversuchen durch regelmäßige Überprüfung der Einbruchssicherheit der Türen, Tore und Fenster
• Separate Zugangskontrolle für folgende Räumlichkeiten (Schlüsselvergabe nur an berechtigte Personen auf „need-to-know"-Basis) / Dokumentierter Zugang / Begleitung:
  ○ Server
  ○ Separates Backup in 2.tem Brandabschnitt
• Zugangsberechtigungen zu DV-Systemen und nicht öffentlichen Netzwerken sind auf das erforderliche Mindestmaß beschränkt (need-to-know Prinzip)
• Schriftliche Regelung für Mitarbeiter für die korrekte und sichere Verwendung von Passwörtern (angemessene Passwortsicherheit)
• Empfangsbuch: Protokollierung der Besucher inkl. Verpflichtung auf Vertraulichkeit, Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO (bisher § 5 BDSG-ALT)
• Dokumentierte und nachvollziehbare Prozesse zur Erlangung, Veränderung und Rücknahme von Zugriffsberechtigungen
• Zugangsberechtigungen werden regelmäßig auf ihre Aktualität geprüft und die Prüfung wird dokumentiert
• Sicherung der Netzwerk-Infrastruktur durch Netzwerk-Port-Security nach IEEE 802.1X, Intrusion Detection Systeme, Trennung von Netzen (WLAN-Netz getrennt von LAN-Infrastruktur, per WLAN Zugriff auf interne Ressourcen nicht möglich), Content-Filter, verschlüsselte Netzwerkprotokolle.
• Unverzügliche Installation von kritischen/ oder wichtigen Sicherheits-Updates/Patches
  ○ in Client-Betriebssysteme,
  ○ in Server-Betriebssysteme, die über öffentliche Netze erreichbar sind (bspw. Webserver),
  ○ in Anwendungsprogramme (inkl. Browser, Plugins, PDF-Reader usw.) und
  ○ in Sicherheits-Infrastruktur (Virenscanner, Firewalls, IDS-Systeme, Content-Filter, Router usw.) binnen 48h nach Veröffentlichung durch den Hersteller sowie in Server-Betriebssysteme interner Server binnen 1 Woche nach Veröffentlichung durch den Hersteller.

II. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern

Technisch-organisatorische Maßnahmen
• Protokollierung der autorisierten Weitergabe von Datenträgern (Externe Festplatten, USB-Sticks, Speicherkarten, usw.) • Die Entsorgung nicht mehr benötigter Datenträger erfolgt datenschutzgerecht • Schriftliche Regelungen für Mitarbeiter für den Umgang und die Sicherheit bei mobilen Geräten und Datenträgern

III. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten

Technisch-organisatorische Maßnahmen
• Berechtigungskonzept mit bedarfsgerechten Zugriffsrechten auf Dateisystemebene (gesteuert durch LDAP) • Berechtigungskonzept mit bedarfsgerechten Zugriffsrechten für die eingesetzte Software • Protokollierung von Zugriffen innerhalb der eingesetzten Anwendungen • Physische Löschung von Datenträgern vor Wiederverwendung • Regelmäßige Prüfung und Verwaltung der Rechte durch Systemadministrator • Einsatz von Aktenvernichtern • Keine Verwendung von geteilten Nutzer-Accounts bzw. Nutzerzugängen

IV. Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte

Technisch-organisatorische Maßnahmen
• Individuelle Benutzerkennung und Passwort sind für die Benutzung der Systeme erforderlich • Schriftliche Regelung für Mitarbeiter für die korrekte Verwendung von Passwörtern (angemessene Passwortsicherheit), bei Verwendung von Passwörtern zur Authentisierung ist eine durchgängige Passwörterqualität von mindestens 8 Zeichen, 3 Komplexitätsgraden und einem Wechselturnus von maximal 180 Tagen gewährleistet. • Einsatz automatischer Sperrmechanismen

• Verpflichtung der Mitarbeiter sich bei Entfernen vom Arbeitsplatz vom System abzumelden bzw. das System zu sperren • Mehrfacheingabe falscher Zugangsdaten untersagt • Zugangsvergabe gemäß Anweisung Geschäftsführung bzw. gemäß Einzelentscheidung Geschäftsführung • Zugangsberechtigungen werden regelmäßig auf ihre Aktualität geprüft und die Prüfung wird dokumentiert • Erzwingung sicherer Kennwörter in allen Applikationen über Anwendung bzw. LDAP

V. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben

Technisch-organisatorische Maßnahmen
• Zugangsberechtigungen werden regelmäßig auf ihre Aktualität geprüft und die Prüfung wird dokumentiert • Wirksame Kontrolle der Zugriffsberechtigungen durch ein adäquates Rechte- und Rollenkonzept • Beschränkung der Zugriffsberechtigungen zu Auftragsdaten auf das absolut benötigte Mindestmaß (need-to-know-Prinzip, least privilege principle) • Dokumentierte und nachvollziehbare Prozesse zur Erlangung, Veränderung und Rücknahme von Zugriffsberechtigungen • Protokollierung von Zugriffen auf Anwendungen inkl. Administratoren • Maßnahmen zum Schutz von Endgeräten, Servern und anderen Infrastruktur-Elementen vor unbefugtem Zugriff: Virenschutz-Konzept, Content-Filter, Application Firewall, Intrusion Detection System

VI. Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können

Technisch-organisatorische Maßnahmen
• Ausgehende Verbindungen geschützt • Ein-/Ausstiegspunkte für Netzwerk dokumentiert • Zugriff auf Systeme auf denen personenbezogene Daten verarbeitet werden, nur über verschlüsselte Verbindungen. • AES Verschlüsselung über AES-256 bei Zugriff auf Kunden / Patientendaten • Festlegung auf ausschließlich sichere Übermittlungswege HTTPS Protokoll) • HSTS Headers via Helmet (Prod/Test/Test2) • Übertragung von Daten per FTPS

- Administration der Systeme über SSH
- Passwörter gemäß Passwort Policy (8 Zeichen, Buchstaben, Zahlen, Sonderzeichen)
- IPSEC / L2TP (PSK) bei VPN Verbindungen

VII. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind

Technisch-organisatorische Maßnahmen
• Protokollierung der Eingabe, Änderung und Löschung von personenbezogenen Daten sowie Nachvollziehbarkeit durch individuelle Benutzernamen • Nur spezifisch definierte Mitarbeiter haben Zugriff auf Systeme mit personenbezogenen Daten (Eingrenzung der Eingebenden) • Keine Nutzung von Gruppen-Accounts (auch Administratoren oder root) bzw. eines Accounts durch mehrere Mitarbeiter • Vergabe von Rechten an individuelle Benutzer zur Eingabe, Änderung und Löschung von Daten

VIII. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden

Technisch-organisatorische Maßnahmen
• Einrichtung von VPN-Tunneln • TLS Protokoll bei Email-Versand • Sicherung der Netzwerk-Infrastruktur durch Netzwerk-Port-Security nach IEEE 802.1X, Intrusion Detection System, Trennung von Netzen, Content-Filter, verschlüsselte Netzwerkprotokolle • Verwendung verschlüsselter Übertragungsprotokolle (bspw. SSL-basierte Protokolle)

IX. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

Technisch-organisatorische Maßnahmen
• Backupmechanismen (periodisch regelmäßig) und Dokumentation des Wiederherstellungsmechanismus • Disaster Recovery Plan und entsprechende Tests (insbesondere das Backups wieder eingespielt werden können)

X. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können

Technisch-organisatorische Maßnahmen
• Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern (je nach Zweck) bzw. in verschiedenen Zugriffsbereichen bzw. Ordnern mit entsprechenden Zugriffsrechten • Logische und/oder physische Trennung von Test-, Entwicklungs- und Produktionssystemen

XI. Maßnahmen zur Pseudonymisierung und Verschlüsselung, Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO

Pseudonymisierung: Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Details sind ggf. im Rahmen des Verzeichnisses der Verarbeitungstätigkeiten auszuführen.

Technisch-organisatorische Maßnahmen
• Regelmäßige Prüfung, welche Daten anonymisiert bzw. gelöscht werden können

B. Verfügbarkeit und Belastbarkeit, Art. 32 Abs. 1 lit. b DSGVO

I. Schnelle Wiederherstellbarkeit, Art. 32 Abs. 1 lit. c DSGVO

Gewährleistung, dass eingesetzte Systeme im Störungsfall schnell wiederhergestellt werden können

Technisch-organisatorische Maßnahmen
• Backup- & Recovery Konzept, insbesondere automatisierte Erstellung von Backups

• Aufbewahrung von Datensicherung in einem zweiten Brandabschnitt • Testen von Datenwiederherstellung

II. Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden

Technisch-organisatorische Maßnahmen
• System monitoring (automatisiert und manuell) • Error log handling • Speicherplatzüberwachung Server

III. Verfügbarkeitskontrolle

Es muss sichergestellt werden, dass personenbezogene Daten gegen mutwillige oder zufällige Zerstörung sowie Verlust geschützt sind.

Technisch-organisatorische Maßnahmen
• Unterbrechungsfreie Stromversorgung (USV) • Betrieb und regelmäßige Wartung von Serverräumen durch IT • Lagerung des Backups in separaten und geschützten Räumlichkeiten • Erstellung täglicher Backups • Regelmäßige Überprüfung der Backups auf die Wiederherstellung der Daten • Prozesse und Dokumentationen zur Wiederherstellung von Systemen und Daten

C. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung; Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DSGVO

I. Datenschutz-Management

- Ein Datenschutzbeauftragter ist schriftlich bestellt:
  - Rechtsanwalt Dietrich Felgner, mip Consult GmbH, Wilhelm-Kabus-Straße 9, 10829 Berlin, d.felgner@mip-consult.de, Tel. +49-30-20 88 999 0
  - Fachkundenachweis des Datenschutzbeauftragten liegen vor.
- Die Mitarbeiter werden in regelmäßig angebotenen Schulungen für das Thema Datenschutz sensibilisiert.
  - Es existieren Nachweise über Verpflichtungen auf das Datengeheimnis für jeden Mitarbeiter.
  - Es erfolgen regelmäßig Hinweise und Sensibilisierungsmaßnahmen, um das datenschutz-rechtliche Problembewusstsein zu fördern.

- Ein Verzeichnis von Verarbeitungstätigkeiten ist vorhanden und wird fortlaufend aktualisiert.
- Die folgenden Dokumentationen liegen vor.
    - Technisch-organisatorische Maßnahmen, siehe dieses Dokument
    - Schriftliche Arbeitsanweisungen/Richtlinien/Merkblätter
- Es ist ein Konzept zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung implementiert. Insbesondere wird 1 x jährlich mit den zuständigen IT-Mitarbeitern ein Review der technischen und organisatorischen Maßnahmen durchgeführt, entsprechende Schritte formuliert und nachgehalten sowie im Jahresbericht dokumentiert.
- Die Aufbewahrung der Protokolle zu Datenschutzthemen ist geregelt.
- Es werden Vorabkontrollen gem. § 4d BDSG bzw. Datenschutz-Folgeabschätzungen gem. Art. 35 DSGVO durchgeführt und protokolliert.
- Adresse für Auskunftsansprüche gemäß Art. 15 DGSVO und die weiteren Rechte nach DSGVO: datenschutz@scheu-dental.com
- Es finden gelegentliche, unangekündigte Kontrollen der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen statt.

Albert Sterkenburg

Certified by yousign

Rüdiger Schmidt

Certified by yousign

SCHEU-DENTAL
custom-made GmbH
Walder Straße 53
40724 Hilden

Geschäftsführer/
Managing Director:
CEO Albert Sterkenburg
CFO Rüdiger Schmidt

phone: +49 2104 80041 00
fax: +49 2104 80041 99
info@scheu-dental.com
www.scheu-dental.com

Düsseldorf HRB 102015
USt-IdNr.: DE815391438

Apobank Düsseldorf
IBAN DE79 3006 0601 0001 1606 99
BIC DAAEDEDDXXX

Stadtsparkasse Düsseldorf
IBAN DE06 3005 0110 1006 4574 59
BIC DUSSDEDDXXX