Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO

Zwischen

nachfolgend „**Auftraggeber**“ genannt

und

Kohlschein Dental GmbH & Co. KG
Boschstrasse 8
48341 Altenberge

nachfolgend „**Auftragnehmer**“ genannt

Präambel

Der Auftragnehmer verarbeitet im Rahmen abgeschlossener oder abzuschließender Verträge personenbezogene Daten aus dem datenschutzrechtlichen Verantwortungsbereich des Auftraggebers im Sinne des Art. 28 Datenschutzgrundverordnung (DSGVO). Die dem Auftragnehmer vom Auftraggeber überlassenen personenbezogenen Daten unterliegen den Bestimmungen der DSGVO und den sonstigen datenschutzrechtlichen Vorschriften (z. B. BDSG). Diese Vereinbarung legt die Rahmenbedingungen zur Gewährleistung der Einhaltung der datenschutzrechtlichen Regelungen fest.

1. Inhalt der Auftragsverarbeitung

Umfang, Art und Zweck der Auftragsverarbeitung sind ebenso wie die Art der Daten und der Kreis der Betroffenen in Anlage 1 beschrieben. Insbesondere ist der Auftragnehmer zur Erfüllung von zwischen den Parteien geschlossenen Verträgen unter Einhaltung der Bestimmungen dieses Vertrages zur Durchführung aller erforderlichen Verarbeitungsschritte und Nutzungen der vom Auftraggeber überlassenen sowie der ggf. für ihn erhobenen Daten (z. B. Duplizieren von Beständen für die Verlustsicherung, Anlegen von Log-Files, Zwischendateien und Arbeitsbereichen etc.) berechtigt, soweit dies nicht zu einer inhaltlichen Umgestaltung führt.

2. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme zu gewährleisten. 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 DSGVO zu berücksichtigen. Soweit die Verarbeitung außerhalb der Betriebsräumlichkeiten des Auftragnehmers zulässig ist, wird das gleiche Schutzniveau sichergestellt.

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.

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. DSGVO erfüllt sind.

3. Berichtigung, Einschränkung und Löschung von Daten

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 unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4. Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt, soweit eine gesetzliche Verpflichtung zur Benennung besteht. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt. Soweit der Auftragnehmer nicht zur Benennung eines Datenschutzbeauftragten verpflichtet ist, wird ein Ansprechpartner für Datenschutzangelegenheiten benannt. Die Kontaktdaten des Datenschutzbeauftragten oder des Ansprechpartners für Datenschutzangelegenheiten sind in Anlage 1 hinterlegt.
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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 einschließlich der in diesem Vertrag eingeräumten Befugnisse verarbeiten, es sei denn, dass der Auftragnehmer nach dem Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO. Einzelheiten zu den technischen und organisatorischen Maßnahmen sind in Anlage 2 aufgeführt.
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers 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.
f) 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.
g) Angemessene Unterstützung des Auftraggebers in seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von geltend gemachten Rechten durch betroffene Personen.
h) 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

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 Telekommunikationsleistungen, Post-/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 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.

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der in Anlage 3 aufgeführten Unterauftragnehmer zu – unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO.

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU / des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen – insbesondere durch Abschluss von Verträgen nach den aktuellen Standardvertragsklauseln der EU-Kommission – sicher. Sämtliche vertraglichen Regelungen zur Auftragsverarbeitung sind auch weiteren Unterauftragnehmern aufzuerlegen.

6. Kontrollrechte des Auftraggebers

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 rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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.

7. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO 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 und

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8. Weisungsbefugnis des Auftraggebers

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform. 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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9. Löschung von Daten und Rückgabe von Datenträgern

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.

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. Gleiches gilt für Test- und Ausschussmaterial.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

10. Laufzeit und Kündigung

Der Vertrag tritt mit seiner Unterzeichnung durch beide Parteien in Kraft und behält Gültigkeit, bis die vereinbarte Datenverarbeitung abgeschlossen ist. Das Recht zur außerordentlichen Kündigung bleibt unberührt. Jede Kündigung bedarf der Schriftform.

Datum/Unterschrift Auftraggeber	Datum/Unterschrift Auftragnehmer

Anlagen:

1. Einzelheiten zur Auftragsverarbeitung
2. Technische und organisatorische Maßnahmen des Auftragnehmers
3. Unterauftragsverhältnisse

Anlage 1 – Einzelheiten zur Auftragsverarbeitung

1. Kontaktdaten des Datenschutzbeauftragten oder Ansprechpartners für Datenschutzangelegenheiten des Auftragnehmers:

Name/Position: Martina Brinkmann / ext. Datenschutzbeauftragte
E-Mail-Adresse: dsb.kdm@cortina-consult.de

2. Gegenstand und Dauer der Verarbeitung

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- besteht in erster Linie nicht in der Verarbeitung personenbezogener Daten; durch die im Folgenden beschriebenen Leistungen kann jedoch ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden.
- Umfasst Service-, Wartungs-, Reparaturmaßnahmen technischer Gerätschaften.
- Umfasst Fernwartungen mithilfe sogenannter Remote-Desktop-Anwendungen.

Die Dauer des Auftrags ist unbefristet.

3. Umfang, Art und Zweck der Verarbeitung:

Nähere Beschreibung des Auftragsgegenstands im Hinblick auf Umfang, Art und Zweck der Aufgaben des Auftragnehmers:

- besteht in erster Linie nicht in der Verarbeitung personenbezogener Daten; durch die im Folgenden beschriebenen Leistungen kann jedoch ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden.
- Service,- Wartungs- und Reparaturmaßnahmen werden sowohl remote (per Fastsupport, Teamviewer oder mithilfe eines vergleichbaren Remote-Desktop-Programms) als auch vor Ort erbracht.

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.

4. Art der personenbezogenen Daten:

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Patientenakte (beinhaltet u.a.: Personalstammdaten, Kommunikationsdaten, Krankheits- und Behandlungsverlauf, Röntgenbilder)

5. Kategorien betroffener Personen:

- Patienten
- Beschäftigte der Praxis

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der Zutrittskontrolle:

- Alarmanlage - Einsatz einer Alarmanlage (evtl. mit Meldung an Sicherheitsdienst)
- Bewegungsmelder - Bewegungsmelder
- Chipkarten - Chipkarten-/Transponder-Schließsystem
- Empfang - Besucherkontrolle am Empfang
- Schließanlage - Einsatz einer Schließanlage
- Schlüsselverwaltung - Schlüsselregelung mit Dokumentation der Schlüssel (z. B. Schlüsselbuch)

M.1.2 Beschreibung der Zugangskontrolle:

- Authentifikation mit Benutzer + Passwort - Authentifikation mit Benutzer + Passwort
- Benutzerberechtigungen - Benutzerberechtigungen verwalten (z. B. bei Eintritt, Änderung, Austritt)
- Firewall - Einsatz von Firewalls zum Schutz des Netzwerkes
- MDM - Einsatz von Mobile Device Management
- Sorgfältige Personalauswahl - Sorgfältige Auswahl von Personal (insbesondere in Bereichen mit sensibler Datenverarbeitung und in der IT-Administration sowie bei Reinigungs- und Sicherheitspersonal)
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren

M.1.3 Beschreibung der Zugriffskontrolle:

- Berechtigungskonzept - Erstellen und Einsatz eines Berechtigungskonzepts
- Datenlöschung - Sichere Löschung von Datenträgern vor deren Wiederverwendung (z. B. durch mehrfaches Überschreiben)
- Einsatz von Aktenvernichtern - Einsatz von Aktenvernichtern (min. Sicherheitsstufe 3 und Schutzklasse 2)
- Einsatz von Aktenvernichtungs-Dienstleistern - Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit DIN 66399 Zertifikat)
- Passwortlichtlinien - Passwortrichtlinie inkl. Länge und Komplexität
- Sichere Aufbewahrung - Sichere Aufbewahrung von Datenträgern
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren

- Verschlüsselung von Smartphones - Verschlüsselung von Smartphones mit dem Stand der Technik entsprechenden Verfahren

M.1.4 Beschreibung der Weitergabekontrolle:

- E-Mail-Verschlüsselung - E-Mail-Verschlüsselung mit S/MIME oder PGP Verfahren (oder anderen, dem Stand der Technik entsprechenden Verfahren)
- SSL / TLS Verschlüsselung - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet
- VPN-Tunnel - Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung - Logische Mandantentrennung (softwareseitig)

M.1.6 Beschreibung der Verschlüsselung:

- Speicherung - Verschlüsselte Datenspeicherung (z. B. Dateiverschlüsselung nach AES256 Standard)
- Übertragung - Verschlüsselte Datenübertragung (z. B. E-Mailverschlüsselung nach PGP oder S/Mime, VPN, verschlüsselte Internetverbindungen mittels TLS/SSL, Einsatz FTAPI - Datentransfertool)

M.1.7 Beschreibung der Datenträgerkontrolle:

- Sichere Aufbewahrung - Sichere Aufbewahrung von Datenträgern
- Sichere Aufbewahrung - Sichere Aufbewahrung von Datenträgern
- Vernichtung - Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Verschlüsselung - Verschlüsselung von (mobilen) Datenträgern

M.1.10 Beschreibung der Benutzerkontrolle:

- Passwortvergabe - Schutz der Benutzeraccounts durch Passwörter
- Sperrung von Ex-Mitarbeiter - Sperren von Benutzeraccounts ausgeschiedener Mitarbeiter

M.1.11 Beschreibung der Übertragungskontrolle:

- Empfängerdokumentation - Dokumentation der Empfänger von Daten sowie deren Bereitstellungsdauer
- Protokollierung - Protokollierung aller Abruf- und Übermittlungsvorgänge

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Personalisierte Benutzernamen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung - Protokollierung der Eingabe, Änderung und Löschung von Daten
- Zugriffsrechte - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.

M.2.2 Beschreibung der Datenintegrität:

- Datensicherungskonzept - Erstellen eines Backup- und Wiederherstellungskonzeptes
- Dokumentensignatur - Signatur von Dokumenten, um deren Integrität sicherzustellen
- E-Mail-Signatur - Signatur von E-Mails, um deren Integrität sicherzustellen

M.2.3 Beschreibung der Speicherkontrolle:

- Berechtigungskonzept - Festlegung von Berechtigungen in einem Berechtigungskonzept
- Protokollierung - Speicherung der Zugriffshistorie in entsprechenden Logfiles

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Antivirensoftware - Einsatz von Antivirensoftware zum Schutz vor Malware
- Auslagerung Datensicherung - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Backup- und Recoverykonzept - Erstellen eines Backup- und Recoverykonzepts
- Brandmeldeanlagen - Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte - Feuerlöschgeräte in Serverräumen
- Klimaanlage - Klimaanlage in Serverräumen
- Redundante Datenhaltung - Redundante Datenhaltung (z.B. gespiegelte Festplatten, RAID 1 oder höher, gespiegelter Serverraum)
- Schutzsteckdosenleisten - Schutzsteckdosenleisten in Serverräumen
- Temperaturüberwachung - Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Unterbrechungsfreie Stromversorgung - (USV) Unterbrechungsfreie Stromversorgung

M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- Datenwiederherstellungen - Regelmäßige und dokumentierte Datenwiederherstellungen

M.4 Weitere Maßnahmen zum Datenschutz

M.4.1 Beschreibung der Auftragskontrolle:

- Audits - Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten
- Auswahl - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- AV-Vertrag - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO
- DSB - Benennung eines Datenschutzbeauftragten
- Laufende Überprüfung - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Schulung - Wiederkehrende Schulungen aller zugriffsberechtigten Mitarbeiter
- Verpflichtung - Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO

M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- DSB - Benennung eines Datenschutzbeauftragten
- Managementsystem Datenschutz - Managementsystem zum Datenschutz (z. B. in Anlehnung an VdS 10010)
- Schulung - Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen.
- Schwachstellenanalysen - Durchführung regelmäßiger IT-Schwachstellenanalysen (z. B. Penetrationstest)
- Software Voreinstellungen - Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DSGVO)
- Softwaregestützte Tools - Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (audatis MANAGER)

M.4.3 Beschreibung der Organisationskontrolle:

- Datenschutzbeauftragter - Ein Datenschutzbeauftragter ist benannt, gemeldet und seine Kontaktdaten sind veröffentlicht
- Dokumentation der Verarbeitung - Alle Verarbeitungstätigkeiten sind dokumentiert und werden regelmäßig überprüft
- Richtlinien - Es existieren verbindliche Richtlinien für den Umgang mit personenbezogenen Daten
- Sensibilisierung - Mitarbeiter werden regelmäßig zum Datenschutz sensibilisiert und geschult

Anlage 3 – Unterauftragsverhältnisse[AB1]

Firma Unterauftragnehmer	Anschrift/Land	Leistung
KaVo Dental GmbH	Bismarckring 39 88400 Biberach	Unterstützung bei Installationen und Reklamationen
DÜRR DENTAL SE	Höpfigheimer-Str. 17 74321 Bietigheim	Unterstützung bei Installationen und Reklamationen
Morita Europe GmbH	Justus-von-Liebig-Str. 27A 63128 Dietzenbach	Unterstützung bei Installationen und Reklamationen
xRAY Germany GmbH & Co. KG	Franz-Kirsten-Straße 1 55411 Bingen	Unterstützung bei Installationen und Reklamationen
Melag Medizintechnik oHG	Geneststr. 9-10 10829 Berlin	Unterstützung bei Installationen und Reklamationen
EIZO Europe GmbH	Helmut-Grashoff-Str. 18 41179 Mönchengladbach	Unterstützung bei Installationen und Reklamationen
Planmeca Vertriebs GmbH	Nordsternstr. 65 45329 Essen	Unterstützung bei Installationen und Reklamationen
EH Germany GmbH (Dexis)	Konrad-Zuse-Straße 6 52134 Herzogenrath	Unterstützung bei Installationen und Reklamationen
CoSi dental GmbH	In den Käppeleswiesen 7 72488 Sigmaringen	Unterstützung bei Installationen und Reklamationen
Frenz IT 4 You	Furth 9 41334 Nettetal	Unterstützung bei Installationen und Reklamationen
orangedental GmbH & Co. KG	Aspachstraße 11 88400 Biberach	Unterstützung bei Installationen und Reklamationen
Barco GmbH	Greschbachstraße 5a 76229 Karlsruhe	Unterstützung bei Installationen und Reklamationen