Auftragsverarbeitung

Gemäß Art. 28 DSGVO wird eine Vereinbarung über die Auftragsverarbeitung geschlossen.

Die Vereinbarung zur Datenverarbeitung wird zwischen den zwei folgenden Parteien geschlossen:

Zwischen _____
_____
(„Auftraggeber“)

Und Görlitz Dental GmbH
Böken 6, 24582 Brügge
(„Auftragnehmer“)

_____
Datum / Unterschrift Auftraggeber

_____
Datum / Unterschrift Auftragnehmer

Auftragsverarbeitung

1. GEGENSTAND UND DAUER DES AUFTRAGS

(1) Gegenstand

* Der Gegenstand des Auftrags ergibt sich aus der jeweiligen Beauftragung im Einzelnen und umfasst alle folgenden Aufträge für die ein Vertrag zur Auftragsdatenverarbeitung gem. DS-GVO erforderlich ist (im Folgenden Leistungsvereinbarung).

(2) Dauer

* Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 1 Monat zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt. Eine Kündigung dieses Vertrages betrifft keine sonstigen Verträge zwischen Auftraggeber und Auftragnehmer, sondern schränkt diese ggfs. nur in der Möglichkeit der Erbringung von Dienstleistungen für den Auftraggeber durch den Auftragnehmer ein.

2. KONKRETISIERUNG DES AUFTRAGSINHALTS

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

* Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber werden in jedem Einzelauftrag beschrieben. Grundsätzlich gehören dazu folgende Leistungsarten:

* Datenbankreparaturen, Datenbankanpassungen, Datenbankkonvertierung, Datenübernahme und ähnliche Dienstleistungen, bei denen der Auftragnehmer Zugriff auf personenbezogene Daten erhält oder die Möglichkeit des Zugriffs besteht

* Beratungs-, Consulting- und Schulungsdienstleistungen sowohl vor Ort oder Fernwartung, bei denen der Auftragnehmer Zugriff auf personenbezogene Daten erhält oder die Möglichkeit des Zugriffs besteht

* Abwicklung von Bestellungen über das Partnerportal, Bestellungen direkt aus den Programmen (White-Label), Bestellungen per E-Mail oder direkte Bestellungen durch Endkunden

* Nicht aufgeführte Tätigkeiten sind in der Auftragserteilung im Einzelfall gesondert zu bezeichnen und durch diese Vereinbarung ebenfalls abgedeckt.

_____
Datum / Unterschrift Auftraggeber

_____
Datum / Unterschrift Auftragnehmer

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) Art der Daten

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

* Personenstammdaten (Kunden, Lieferanten, Mitarbeiter)
* Lohn-, Fehlzeiten- und Reisekostendaten Mitarbeiter
* Kommunikationsdaten (z.B. Telefon, E-Mail)
* Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
* Kundenhistorie
* Vertragsabrechnungs- und Zahlungsdaten
* Planungs- und Steuerungsdaten
* Bewegungsdaten aus Fakturierung und Buchhaltung, sofern diese personenbezogene Daten enthalten

(3) Kategorien betroffener Personen

* Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

* Kunden
* Interessenten
* Abonnenten
* Beschäftigte/Mitarbeiter
* Lieferanten
* Handelsvertreter
* Ansprechpartner
* Patienten

3. VERGÜTUNG

(1) Die Vergütung der Dienstleistung wird jeweils durch den Hauptvertrag geregelt. Findet sich dort keine Vergütungsregelung, gelten die kommunizierten Standardstundensätze als vereinbart.

4. TECHNISCH-ORGANISATORISCHE MAßNAHMEN

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen 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 [Einzelheiten in Anlage 1].

(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.

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

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

6. QUALITÄTSSICHERUNG UND SONSTIGE PFLICHTEN DES AUFTRAGNEHMERS

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

* Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet.
* Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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 zur Verarbeitung verpflichtet sind.
* Die Umsetzung und 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].
* Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
* 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.
* 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. Dies erfolgt kostenpflichtig.
* 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.
* Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

7. 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 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.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) beauftragen. Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit dies aus technischen bzw. organisatorischen Gründen erforderlich ist und mit dem jeweiligen Unterauftragnehmer eine entsprechende Vereinbarung zur Auftragsdatenverarbeitung besteht, die mindestens die gleichen Anforderungen wie diese Vereinbarung aufweist.

(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 Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

8. 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 anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(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

* die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
* die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
* aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
* eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

9. MITTEILUNG BEI VERSTÖßEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer unterstützt 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.

* 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

* die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
* 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
* die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
* die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

10. WEISUNGSBEFUGNIS DES AUFTRAGGEBERS

(1) Weisungsbefugnisse ergeben sich aus dem jeweiligen Hauptvertrag. Dort ist auch eine verantwortliche Person auf Seiten des Auftraggebers zu benennen.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(3) 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.

11. 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. Gleiches gilt für Test- und Ausschussmaterial.

Das Protokoll der Löschung ist auf Anforderung vorzulegen. Der Auftragnehmer ist berechtigt, die Daten bis zum vollständigen Ausgleich der Forderungen aus dem jeweiligen Auftrag zum Zwecke des Nachweises der Leistungserbringung aufzubewahren. Eine vorzeitige Löschung ist nur möglich, wenn eine Bestätigung über die korrekte und vollständige Leistungserbringung durch den Auftraggeber erfolgt ist.

(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.

Anlagen: Anlage 1 - Technisch-organisatorische Maßnahmen (TOMS)

ANLAGE 1 – TECHNISCH-ORGANISATORISCHE MAßNAHMEN

1. VERTRAULICHKEIT (ART. 32 ABS. 1 LIT. B DS-GVO)

* Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, Sicherung durch Sicherheitsschlüssel mit Schutz durch Schlüsselkarte, Alarmanlagen, Videoüberwachung;
* Zugangskontrolle
Keine unbefugte Systembenutzung, Sicherung durch (sichere) Kennwörter, automatische Sperrmechanismen, Verschlüsselung von Datenträgern (bei hochkritischen Daten);
* Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Sicherung durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
* Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, Sicherung durch Verarbeitung in einzelnen abgeschotteten virtuellen Maschinen;

2. INTEGRITÄT (ART. 32 ABS. 1 LIT. B DS-GVO)

* Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, Sicherung durch SSL-Verschlüsselung, Unternehmensintern durch VPN, elektronische Signatur;
* Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, Sicherung durch Protokollierung, Dokumentenmanagement;

3. VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B DS-GVO)

* Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV) für alle Serversysteme, Virenschutz, Firewall, Meldewege und Notfallpläne; IDS-Systeme auf allen exponierten Servern
* Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO); Live-Restore aller kritischen Server-Systeme

4. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (ART. 32 ABS. 1 LIT. D DS-GVO; ART. 25 ABS. 1 DS-GVO)

* Datenschutz-Management;
* Incident-Response-Management;
* Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
* Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.