Dokumenteninformationen

Dokument	Auftragsverarbeitungsvertrag (AVV)
Version	1.3
Stand	15. November 2026
Gültig ab	15.11.2026
Herausgeber	DentaTool GmbH & Co. KG

Änderungshistorie

1.0 – Juli 2026	Erstfassung
1.1 – Oktober 2026	KI-gestützte Funktionen und Geheimhaltung nach § 203 StGB (§ 6a), Unterauftragsverarbeiter Amazon Web Services EMEA SARL und Lettermint B.V. (Anlage 2, Nr. 4 und 5), TOM für KI-Assistenten (Anlage 1, Ziffer 5 und 19), Löschfristen und KI-Verarbeitung (Anlage 3 und 4)
1.2 - 31. Oktober 2026	Zusätzliche Aufnahme von Lettermint für den Versand transaktionaler E-Mails einschließlich Zustelltracking; Präzisierung der Aufbewahrung und Versandverarbeitung (Anlagen 2 bis 4)
1.3 - 15. November 2026	Speicherung hochgeladener Dateien im Objektspeicher von Amazon Web Services EMEA SARL (Region Frankfurt) statt bei Hetzner (Anlage 2, Nr. 1 und 6); TOM zu Dateispeicher, Verschlüsselung und Versionierung (Anlage 1); Aufbewahrung gelöschter Dateien bis zu 30 Tage (Anlage 3)

Ansprechpartner Datenschutz

DentaTool GmbH & Co. KG

E-Mail: datenschutz@dentatool.de

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

dem jeweiligen Kunden (Dentallabor)

– nachfolgend **„Auftraggeber"** –

und

DentaTool GmbH & Co. KG
Berlin
Deutschland

– nachfolgend **„Auftragnehmer"** –

gemeinsam auch **„Parteien"** genannt.

Präambel

Der Auftraggeber nutzt die cloudbasierte Softwarelösung **DentaTool** zur Organisation und Verwaltung zahntechnischer Arbeitsabläufe innerhalb seines Dentallabors.

DentaTool ist eine Software-as-a-Service-(SaaS)-Plattform zur digitalen Verwaltung von Laboraufträgen, Kundenbeziehungen, Patientenfällen, Abrechnungen, Material- und Chargendokumentation, Kommunikation mit Zahnarztpraxen sowie weiterer betrieblicher Prozesse eines Dentallabors.

Im Rahmen der Nutzung verarbeitet der Auftragnehmer personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers.

Hierzu schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO.

Der Auftraggeber bleibt hinsichtlich sämtlicher personenbezogener Daten Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Leistungen und verfolgt keinerlei eigene Zwecke hinsichtlich der vom Auftraggeber überlassenen personenbezogenen Daten.

---

§1 Gegenstand der Auftragsverarbeitung

(1) Vertragsgegenstand

Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Rahmen der Bereitstellung und des Betriebs der Softwareplattform **DentaTool**.

Die Verarbeitung erfolgt ausschließlich zur Durchführung der zwischen den Parteien bestehenden Leistungsvereinbarung.

Hierzu gehören insbesondere folgende Funktionen der Plattform:

- Verwaltung zahntechnischer Aufträge
- Verwaltung von Zahnärzten, Praxen und Ansprechpartnern
- digitale Auftragszettel
- Kundenportal für Zahnarztpraxen
- Kommunikation zwischen Labor und Praxis
- Verwaltung von Patientenfällen
- Dokumentation gemäß EU-Medizinprodukteverordnung (EU-MDR)
- Material- und Chargendokumentation
- Erstellung und Verwaltung von Kostenvoranschlägen
- Erstellung von Laborrechnungen
- Dokumentenmanagement
- Upload und Speicherung digitaler Dateien
- Kalender- und Terminverwaltung
- Benachrichtigungsfunktionen
- Benutzer- und Rechteverwaltung
- Arbeitszeit- und Personalverwaltung (soweit vom Auftraggeber genutzt)
- Archivierung von Vorgängen
- Sicherung und Wiederherstellung der Daten
- technischer Support

---

(2) Art der Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten insbesondere durch

- Erheben
- Erfassen
- Speichern
- Ordnen
- Strukturieren
- Anpassen
- Auslesen

- Verwenden
- Übermitteln
- Bereitstellen
- Archivieren
- Löschen

soweit dies zur vertragsgemäßen Bereitstellung der Software erforderlich ist.

Eine Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung des Auftraggebers.

---

(3) Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung von DentaTool.

Nach Beendigung des Hauptvertrages gelten die Regelungen dieses Vertrages hinsichtlich Rückgabe, Löschung und Aufbewahrung personenbezogener Daten fort.

---

§2 Art der personenbezogenen Daten

Je nach Nutzung der Software können insbesondere folgende Kategorien personenbezogener Daten verarbeitet werden:

Stammdaten

- Vorname
- Nachname
- Titel
- Kundennummer
- Patienten-ID
- Geburtsdatum
- Anschrift
- Telefonnummer
- E-Mail-Adresse

Patientenbezogene Daten

Hierzu gehören insbesondere

- Patientenname
- Patientenkennung
- behandelnder Zahnarzt
- Zahnschema
- Zahnpositionen
- Behandlungsinformationen
- Auftragsinformationen
- zahntechnische Arbeitsdaten
- Termininformationen

Soweit diese Daten Rückschlüsse auf den Gesundheitszustand zulassen, handelt es sich um besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO.

Gesundheitsdaten

Je nach Nutzung können insbesondere verarbeitet werden:

- zahnmedizinische Befunde
- Zahnschemata
- Präparationsinformationen
- Implantatinformationen
- Kieferinformationen
- Okklusionsdaten
- Abformungsinformationen
- Scandaten
- medizinische Notizen
- Fotos
- Röntgenbilder
- intraorale Scans

Digitale Dateien

Der Auftraggeber kann insbesondere folgende Dateiformate speichern:

- STL
- PLY
- OBJ
- DCM
- PDF
- JPG
- PNG

- TIFF
- ZIP
- XML
- sonstige Dokumente und CAD-Dateien

Abrechnungsdaten

- Rechnungen
- Gutschriften
- Kostenvoranschläge
- Zahlungsinformationen
- BEL-/BEB-Positionen
- Laborpreise
- XML-Abrechnungsnummern
- Rechnungsnummern

Kommunikationsdaten

- Kommentare
- Rückfragen
- Nachrichten
- Benachrichtigungen
- E-Mail-Inhalte
- Supportanfragen

Mitarbeiterdaten

Soweit genutzt:

- Benutzerkonten
- Rollen
- Berechtigungen
- Arbeitszeiten
- Urlaubsdaten
- Krankmeldungen
- Zeitbuchungen

Protokolldaten

Zum sicheren Betrieb der Plattform werden außerdem verarbeitet:

- Login-Zeitpunkte
- IP-Adressen
- Browserinformationen
- Betriebssystem
- Zeitstempel
- Audit-Logs
- Fehlerprotokolle
- Sicherheitsereignisse

---

§3 Kategorien betroffener Personen

Von der Verarbeitung können insbesondere folgende Personengruppen betroffen sein:

- Patienten
- Zahnärzte
- Mitarbeiter von Zahnarztpraxen
- Mitarbeiter des Auftraggebers
- Ansprechpartner des Auftraggebers
- Lieferanten und Geschäftspartner
- sonstige vom Auftraggeber verwaltete Personen

---

§4 Anwendungsbereich und Verantwortlichkeit

(1) Verantwortlichkeit des Auftraggebers

Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

Er entscheidet allein über die Zwecke und Mittel der Verarbeitung personenbezogener Daten innerhalb der DentaTool-Plattform.

Der Auftraggeber ist insbesondere verantwortlich für

- die Rechtmäßigkeit der Erhebung personenbezogener Daten,
- das Vorliegen einer geeigneten Rechtsgrundlage gemäß Art. 6 bzw. Art. 9 DSGVO,
- die Erfüllung sämtlicher Informationspflichten gegenüber betroffenen Personen,
- die Wahrnehmung der Betroffenenrechte,

- die Rechtmäßigkeit der Übermittlung personenbezogener Daten an den Auftragnehmer.

Der Auftragnehmer übernimmt keine Verantwortlichkeit hinsichtlich der datenschutzrechtlichen Zulässigkeit der durch den Auftraggeber veranlassten Verarbeitung.

---

(2) Stellung des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach dokumentierter Weisung des Auftraggebers.

Der Auftragnehmer verarbeitet die Daten nicht zu eigenen Zwecken.

Insbesondere erfolgt keine Nutzung der Daten

- zu Marketingzwecken,
- zur Profilbildung,
- zur Erstellung statistischer Nutzerprofile,
- zum Verkauf an Dritte,
- zur Weitergabe an unberechtigte Dritte,
- zum Training von KI-Modellen oder vergleichbaren Systemen.

Eine Auswertung personenbezogener Daten erfolgt ausschließlich, soweit dies zur Bereitstellung der vertragsgegenständlichen Leistungen technisch erforderlich ist.

---

(3) Mandantentrennung

Die Daten sämtlicher Auftraggeber werden innerhalb der Plattform logisch voneinander getrennt verarbeitet.

Der Auftragnehmer stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass ausschließlich berechtigte Benutzer auf die ihrem Benutzerkonto zugeordneten Daten zugreifen können.

Ein Zugriff anderer Auftraggeber auf Daten eines fremden Mandanten ist technisch ausgeschlossen.

---

(4) Weisungsrecht

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf Grundlage

- dieses Vertrages,
- des Hauptvertrages sowie
- dokumentierter Weisungen des Auftraggebers.

Weisungen können insbesondere in Textform per E-Mail oder über hierfür vorgesehene Funktionen innerhalb der DentaTool-Plattform erfolgen.

Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

---

(5) Unzulässige Weisungen

Hält der Auftragnehmer eine Weisung des Auftraggebers für datenschutzrechtlich unzulässig oder offensichtlich rechtswidrig, informiert er den Auftraggeber unverzüglich.

Der Auftragnehmer ist berechtigt, die Durchführung einer Weisung auszusetzen, bis der Auftraggeber diese bestätigt oder anpasst.

Eine Verpflichtung zur rechtlichen Prüfung sämtlicher Weisungen besteht nicht.

---

§5 Rechte und Pflichten des Auftraggebers

Der Auftraggeber verpflichtet sich,

- ausschließlich rechtmäßig erhobene personenbezogene Daten zu verarbeiten,
- nur berechtigten Personen Zugang zur Plattform zu gewähren,
- Benutzerkonten aktuell zu halten,
- Zugangsberechtigungen unverzüglich zu entziehen, sobald Mitarbeiter ausscheiden oder keine Berechtigung mehr besitzen,
- starke Passwörter zu verwenden und diese vertraulich zu behandeln.

Der Auftraggeber trägt die Verantwortung für sämtliche Inhalte, die innerhalb seines Mandanten gespeichert werden.

Betroffenenrechte

Der Auftraggeber ist für die Bearbeitung von Anträgen betroffener Personen verantwortlich.

Hierzu gehören insbesondere

- Auskunft
- Berichtigung
- Löschung
- Einschränkung der Verarbeitung
- Datenübertragbarkeit
- Widerspruch

Soweit der Auftragnehmer hierzu Unterstützung leisten kann, erfolgt diese im Rahmen der technischen Möglichkeiten.

Datenschutzbeauftragter

Soweit gesetzlich erforderlich, benennt der Auftraggeber einen Datenschutzbeauftragten und teilt dessen Kontaktdaten dem Auftragnehmer auf Anfrage mit.

---

§6 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich insbesondere,

- personenbezogene Daten ausschließlich nach Weisung des Auftraggebers zu verarbeiten,
- sämtliche Mitarbeiter auf Vertraulichkeit zu verpflichten,
- geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO zu treffen,
- den Auftraggeber bei der Erfüllung seiner datenschutzrechtlichen Pflichten angemessen zu unterstützen,
- Datenschutzverletzungen unverzüglich mitzuteilen,
- eingesetzte Unterauftragsverarbeiter sorgfältig auszuwählen,
- regelmäßige Datensicherungen durchzuführen,
- ein angemessenes Sicherheitsniveau entsprechend dem Stand der Technik aufrechtzuerhalten.

Vertraulichkeit

Der Auftragnehmer stellt sicher, dass sämtliche mit der Verarbeitung personenbezogener Daten befassten Personen

- zur Vertraulichkeit verpflichtet sind,
- regelmäßig im Datenschutz geschult werden,
- ausschließlich im Rahmen ihrer Aufgaben Zugriff auf personenbezogene Daten erhalten.

Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

Unterstützungspflichten

Der Auftragnehmer unterstützt den Auftraggeber im angemessenen Umfang bei

- Datenschutz-Folgenabschätzungen,
- Sicherheitsvorfällen,
- Anfragen von Aufsichtsbehörden,
- Erfüllung von Betroffenenrechten,
- Nachweisen gegenüber Datenschutzbehörden.

Soweit hierfür erheblicher zusätzlicher Aufwand entsteht, kann der Auftragnehmer eine angemessene Vergütung verlangen, sofern dies vertraglich vereinbart wurde oder gesetzlich zulässig ist.

Supportzugriffe

Soweit dies zur Fehleranalyse oder technischen Unterstützung erforderlich ist, können autorisierte Mitarbeiter des Auftragnehmers auf Daten innerhalb des Mandanten des Auftraggebers zugreifen.

Solche Zugriffe erfolgen ausschließlich

- auf Veranlassung des Auftraggebers,
- zur Fehlerbehebung,
- zur Erfüllung vertraglicher Supportleistungen oder
- zur Gewährleistung der Betriebssicherheit.

Supportzugriffe werden auf das erforderliche Maß beschränkt und nach Möglichkeit protokolliert.

§6a KI-gestützte Funktionen (Amazon Bedrock)

Dieser Paragraph ergänzt §1 und gilt, soweit der Auftraggeber KI-Funktionen der Plattform nutzt.

(1) Leistungsgegenstand

Soweit vom Auftraggeber beauftragt, umfasst die Auftragsverarbeitung auch KI-gestützte administrative Assistenzfunktionen im Kundenportal und im Laborbereich sowie die KI-gestützte Erfassung von Auftragszetteln. Hierzu gehören die Auswertung der Eingaben und Gesprächsverläufe, das Abrufen auftragsbezogener Daten, das Erzeugen von Antworten und Erfassungsvorschlägen sowie die Ausführung der in der Leistungsbeschreibung festgelegten Aktionen. Die Verarbeitung erfolgt ausschließlich zur Erfüllung der beauftragten Leistungen auf dokumentierte Weisung des Auftraggebers.

Verarbeitet werden je nach Funktion Nachrichten, Gesprächsverläufe, Namen, Auftrags- und Abrechnungsdaten, Zahn- und Behandlungsangaben, Bilder von Auftragszetteln sowie KI-Ausgaben und Aktionsprotokolle. Diese Daten können Gesundheitsdaten gemäß Art. 9 DSGVO enthalten.

(2) Modellverarbeitung und Zweckbindung

Für die KI-Funktionen setzt der Auftragnehmer ausschließlich Amazon Bedrock mit dem in Anlage 2 genannten EU-Inferenzprofil ein. Der Auftragnehmer verwendet nur Sprachmodelle, für die der Anbieter nach seiner Dokumentation keine Speicherung der Ein- und Ausgaben und keine menschliche Prüfung verlangt, und hat im eigenen Konto die Aufbewahrung der Ein- und Ausgaben ausgeschlossen sowie die Protokollierung der Modellaufrufe ausgeschaltet. Ein Wechsel des Modells oder Anbieters erfolgt nur nach Prüfung dieser Eigenschaften und nach Information des Auftraggebers gemäß Anlage 2.

Eine Nutzung von Kundendaten zum Training oder zur allgemeinen Verbesserung eigener oder fremder KI-Modelle ist nicht Bestandteil des Auftrags und wird nicht gestattet. Der Auftragnehmer stellt in den Unterauftragsverhältnissen sicher, dass Kundendaten nur zur Erbringung der beauftragten Leistungen verwendet werden.

(3) Weisung und Funktionsaktivierung

Der Auftraggeber bestimmt, welche Assistenzfunktionen er beauftragt und welche Benutzer bzw. Kunden diese nutzen dürfen. Die KI-Funktionen werden erst nutzbar, nachdem der Auftraggeber diesem Vertrag zugestimmt hat. Die Zustimmung wird mit Version, Zeitpunkt und zustimmendem Benutzer dokumentiert. Dies gilt auch bei kostenloser oder zeitlich begrenzter Nutzung.

Das Ende einer Testphase bestimmt der Auftragnehmer; sie dauert pauschal 30 Tage ab Einrichtung des Zugangs und kann im Einzelfall verlängert werden. Kommt nach einer Testphase kein kostenpflichtiger Vertrag zustande, löscht der Auftragnehmer die im Test verarbeiteten Daten rund 30 Tage nach dem Ende der Testphase.

(4) Unterauftragsverarbeiter

Die bei Vertragsschluss vorgesehenen Unterauftragsverarbeiter ergeben sich aus Anlage 2, einschließlich der Anbieterin der KI-Modellverarbeitung. Für spätere Hinzunahmen oder wesentliche Änderungen gilt das in §12 vereinbarte Informations- und Widerspruchsverfahren mit der Frist von 30 Kalendertagen.

(5) Betroffenenrechte

Die Pflichten zur Unterstützung bei Auskunft, Berichtigung, Löschung und Einschränkung (§10 und §11) erstrecken sich auf KI-Unterhaltungen, zugehörige Dateien und Aktionsprotokolle, soweit sie dem Auftrag zuzuordnen sind.

(6) Geheimhaltung

Soweit Patientengeheimnisse im Anwendungsbereich des § 203 StGB verarbeitet werden, stellt der Auftragnehmer die erforderliche Verpflichtung der mitwirkenden Personen zur Verschwiegenheit sicher. Dies gilt für die eigenen Mitarbeiter und für Unterauftragsverarbeiter, soweit diese auf Inhalte zugreifen können. Mit dem Unterauftragsverarbeiter für den Versand von E-Mails (Anlage 2, Nr. 5) besteht hierzu eine Vertraulichkeitsvereinbarung.

§7 Technische und organisatorische Maßnahmen

(1) Sicherheitsniveau

Der Auftragnehmer trifft gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen (TOM), um ein dem Risiko angemessenes Schutzniveau für die verarbeiteten personenbezogenen Daten sicherzustellen.

Bei der Auswahl der Maßnahmen berücksichtigt der Auftragnehmer insbesondere

- den Stand der Technik,
- die Implementierungskosten,
- Art, Umfang, Umstände und Zwecke der Verarbeitung,
- die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere möglicher Risiken für die Rechte und Freiheiten natürlicher Personen.

---

(2) Beschreibung der Maßnahmen

Die beim Auftragnehmer implementierten technischen und organisatorischen Maßnahmen ergeben sich aus **Anlage 1** dieses Vertrages.

Diese umfasst insbesondere Maßnahmen zur

- Zutrittskontrolle,
- Zugangskontrolle,
- Zugriffskontrolle,
- Weitergabekontrolle,
- Eingabekontrolle,
- Auftragskontrolle,
- Verfügbarkeitskontrolle,
- Trennungskontrolle,
- Verschlüsselung,
- Datensicherung,
- Wiederherstellung,
- Protokollierung,
- Incident Response,
- Mandantentrennung.

---

(3) Weiterentwicklung der Sicherheitsmaßnahmen

Der Auftragnehmer ist berechtigt, technische und organisatorische Maßnahmen fortlaufend an den Stand der Technik anzupassen oder zu verbessern, sofern dadurch das vertraglich vereinbarte Datenschutzniveau nicht unterschritten wird.

---

§8 Vertraulichkeit

Der Auftragnehmer gewährleistet, dass sämtliche mit der Verarbeitung personenbezogener Daten befassten Personen

- auf Vertraulichkeit verpflichtet wurden,
- über datenschutzrechtliche Anforderungen informiert wurden,
- ausschließlich im Rahmen ihrer jeweiligen Aufgaben Zugriff auf personenbezogene Daten erhalten.

Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung der jeweiligen Tätigkeit fort.

---

§9 Datenschutzverletzungen

(1) Meldung

Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, soweit diese den Verantwortungsbereich des Auftraggebers betrifft.

Die Mitteilung erfolgt ohne schuldhaftes Zögern und enthält, soweit möglich,

- Art der Datenschutzverletzung,
- betroffene Datenkategorien,
- Anzahl der betroffenen Datensätze,
- bereits ergriffene Maßnahmen,
- empfohlene Gegenmaßnahmen,
- Kontaktdaten einer Ansprechperson.

---

(2) Zusammenarbeit

Die Parteien arbeiten bei der Untersuchung und Beseitigung von Datenschutzverletzungen eng zusammen.

Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung gesetzlicher Meldepflichten gegenüber Aufsichtsbehörden sowie gegebenenfalls gegenüber betroffenen Personen.

---

§10 Betroffenenrechte

Der Auftraggeber bleibt für die Wahrnehmung der Rechte betroffener Personen verantwortlich.

Hierzu gehören insbesondere

- Auskunft
- Berichtigung
- Löschung
- Einschränkung der Verarbeitung
- Datenübertragbarkeit
- Widerspruch
- Widerruf einer Einwilligung

Soweit der Auftragnehmer Anfragen betroffener Personen unmittelbar erhält, wird er diese unverzüglich an den Auftraggeber weiterleiten, sofern keine gesetzliche Verpflichtung zur eigenständigen Bearbeitung besteht.

Der Auftragnehmer wird ohne Weisung des Auftraggebers keine Auskünfte gegenüber betroffenen Personen erteilen.

---

§11 Unterstützungspflichten

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen in angemessenem Umfang bei der Erfüllung seiner datenschutzrechtlichen Pflichten.

Dies umfasst insbesondere Unterstützung bei

- Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO,
- Konsultationen mit Aufsichtsbehörden gemäß Art. 36 DSGVO,
- Nachweisen gegenüber Datenschutzaufsichtsbehörden,

- Erfüllung von Betroffenenrechten,
- Sicherheitsvorfällen.

Soweit hierfür erheblicher zusätzlicher Aufwand entsteht, kann der Auftragnehmer eine angemessene Vergütung verlangen, sofern dies gesetzlich zulässig oder vertraglich vereinbart ist.

---

§12 Unterauftragsverarbeiter

(1)

Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern gemäß Art. 28 Abs. 2 DSGVO.

Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter ergeben sich aus **Anlage 2** dieses Vertrages.

---

(2)

Der Auftragnehmer verpflichtet sämtliche Unterauftragsverarbeiter vertraglich mindestens auf diejenigen Datenschutzpflichten, die sich aus diesem Vertrag ergeben.

---

(3)

Beabsichtigt der Auftragnehmer den Einsatz neuer Unterauftragsverarbeiter oder wesentliche Änderungen bestehender Unterauftragsverhältnisse, informiert er den Auftraggeber mindestens **30 Kalendertage** vor deren Einsatz in Textform.

Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen.

Erfolgt innerhalb der Frist kein Widerspruch, gilt die Zustimmung als erteilt.

---

(4)

Widerspricht der Auftraggeber berechtigt und kann der Auftragnehmer keine zumutbare Alternative anbieten, sind beide Parteien berechtigt, den Hauptvertrag hinsichtlich der betroffenen Leistung außerordentlich zu kündigen.

---

§13 Audits und Nachweise

(1)

Der Auftraggeber ist berechtigt, die Einhaltung der Verpflichtungen aus diesem Vertrag in angemessenem Umfang zu überprüfen.

---

(2)

Der Auftragnehmer kann geeignete Nachweise über die Einhaltung datenschutzrechtlicher Anforderungen zur Verfügung stellen.

Hierzu zählen insbesondere

- aktuelle Zertifizierungen,
- Prüfberichte,
- Selbstauskünfte,
- Dokumentationen der technischen und organisatorischen Maßnahmen,
- sonstige geeignete Nachweise.

---

(3)

Vor-Ort-Kontrollen sind nur zulässig,

- wenn sie erforderlich sind,
- nach vorheriger schriftlicher Ankündigung mit einer Frist von mindestens vier Wochen,
- während der üblichen Geschäftszeiten,
- unter Berücksichtigung berechtigter Betriebs- und Geschäftsgeheimnisse des Auftragnehmers,
- soweit hierdurch weder die Sicherheit noch der Betrieb der Plattform beeinträchtigt werden.

---

(4)

Der Auftraggeber trägt die Kosten eines von ihm veranlassten Audits, soweit gesetzlich nichts anderes vorgeschrieben ist.

---

(5)

Der Auftraggeber darf im Rahmen eines Audits keine Informationen, Systeme oder personenbezogenen Daten anderer Auftraggeber einsehen oder Zugriff auf diese verlangen. Der Auftragnehmer ist berechtigt, Nachweise zu anonymisieren oder zu schwärzen, soweit dies zum Schutz anderer Kunden, zur Wahrung von Geschäftsgeheimnissen oder zur Gewährleistung der IT-Sicherheit erforderlich ist.

§14 Rückgabe und Löschung personenbezogener Daten

(1) Vertragsende

Nach Beendigung des Hauptvertrages verarbeitet der Auftragnehmer personenbezogene Daten des Auftraggebers grundsätzlich nicht mehr, sofern keine gesetzliche Verpflichtung zur weiteren Speicherung besteht.

Der Auftraggeber kann bis zum Ende des Vertragsverhältnisses seine Daten über die hierfür vorgesehenen Exportfunktionen der DentaTool-Plattform exportieren oder den Auftragnehmer mit der Bereitstellung eines Datenexports beauftragen.

---

(2) Datenexport

Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch die im Rahmen der vertragsgegenständlichen Verarbeitung gespeicherten Daten in einem gängigen, maschinenlesbaren Format zur Verfügung, soweit dies technisch möglich und wirtschaftlich zumutbar ist.

Der Datenexport umfasst die im Mandanten des Auftraggebers gespeicherten Daten einschließlich der zugehörigen Dokumente, soweit diese Bestandteil der Plattform sind.

Ein Anspruch auf Herausgabe von Software, Quellcode, Datenbankstrukturen, internen Systemdateien oder Geschäftsgeheimnissen des Auftragnehmers besteht nicht.

---

(3) Löschung

Nach Ablauf gesetzlicher Aufbewahrungsfristen sowie angemessener technischer Vorhaltezeiten löscht oder anonymisiert der Auftragnehmer sämtliche personenbezogenen Daten des Auftraggebers, soweit keine gesetzliche Verpflichtung zur weiteren Speicherung besteht.

Dies gilt ebenfalls für sämtliche Sicherungskopien, sobald diese im Rahmen der regulären Backup-Rotation überschrieben werden.

---

(4) Gesetzliche Aufbewahrungspflichten

Soweit gesetzliche Aufbewahrungspflichten einer sofortigen Löschung entgegenstehen, werden die betreffenden Daten für die Dauer der gesetzlichen Aufbewahrungsfrist gesperrt und ausschließlich zu diesem Zweck aufbewahrt.

Nach Ablauf der jeweiligen Fristen werden die Daten unverzüglich gelöscht.

---

(5) Nachweis der Löschung

Der Auftragnehmer bestätigt dem Auftraggeber auf Wunsch die Löschung der personenbezogenen Daten in geeigneter Form.

Ein Anspruch auf Löschung einzelner Datensätze aus Sicherungskopien besteht nicht, sofern diese ausschließlich zu Zwecken der Datensicherung vorgehalten werden und einer regulären Backup-Rotation unterliegen.

---

§15 Vertraulichkeit und Geschäftsgeheimnisse

Die Parteien verpflichten sich, sämtliche im Zusammenhang mit diesem Vertrag bekannt werdenden vertraulichen Informationen sowie Geschäfts- und Betriebsgeheimnisse der jeweils anderen Partei vertraulich zu behandeln.

Diese Verpflichtung gilt auch nach Beendigung des Vertragsverhältnisses fort.

Als vertrauliche Informationen gelten insbesondere

- technische Dokumentationen,
- Softwarearchitektur,
- Quellcode,
- Sicherheitsmaßnahmen,
- Systemkonfigurationen,
- Kundenlisten,
- wirtschaftliche Informationen,
- interne Prozesse.

Hiervon ausgenommen sind Informationen,

- die öffentlich bekannt sind oder werden,
- deren Offenlegung gesetzlich vorgeschrieben ist oder
- die einer Partei bereits rechtmäßig bekannt waren.

---

§16 Haftung

Die Haftung der Parteien richtet sich nach den gesetzlichen Vorschriften der Datenschutz-Grundverordnung sowie den Bestimmungen des zwischen den Parteien geschlossenen Hauptvertrages.

Die Vorschriften der Art. 82 ff. DSGVO bleiben unberührt.

Soweit mehrere Parteien für einen Schaden verantwortlich sind, haften diese entsprechend den gesetzlichen Vorschriften.

---

§17 Änderungen dieses Vertrages

Der Auftragnehmer ist berechtigt, diesen Vertrag zu ändern, soweit

- gesetzliche Änderungen,
- Entscheidungen von Datenschutzaufsichtsbehörden,
- Änderungen der Rechtsprechung,
- technische Weiterentwicklungen oder
- Anpassungen der angebotenen Leistungen

dies erforderlich machen.

Über wesentliche Änderungen wird der Auftraggeber mindestens 30 Kalendertage vor Inkrafttreten in Textform informiert.

Widerspricht der Auftraggeber den Änderungen nicht innerhalb dieser Frist, gelten diese als genehmigt.

Widerspricht der Auftraggeber fristgerecht und ist dem Auftragnehmer die Fortführung des Vertrags zu den bisherigen Bedingungen nicht zumutbar, sind beide Parteien berechtigt, den Hauptvertrag mit angemessener Frist zu kündigen.

---

§18 Schlussbestimmungen

(1)

Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Die Parteien verpflichten sich, die unwirksame Regelung durch eine solche zu ersetzen, die dem wirtschaftlichen Zweck der ursprünglichen Regelung möglichst nahekommt.

---

(2)

Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform, sofern nicht gesetzlich eine strengere Form vorgeschrieben ist.

---

(3)

Dieser Vertrag ergänzt den zwischen den Parteien bestehenden Hauptvertrag.

Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen hinsichtlich der Verarbeitung personenbezogener Daten die Regelungen dieses Vertrages vor.

---

(4)

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

Zwingende datenschutzrechtliche Vorschriften bleiben unberührt.

---

(5)

Gerichtsstand für sämtliche Streitigkeiten aus diesem Vertrag ist – soweit gesetzlich zulässig – der Sitz des Auftragnehmers.

---

(6)

Dieser Auftragsverarbeitungsvertrag ist Bestandteil des zwischen den Parteien geschlossenen Nutzungsvertrages über die DentaTool-Plattform.

Der Auftragsverarbeitungsvertrag kommt mit Abschluss des Nutzungsvertrages zustande. Soweit der Vertrag elektronisch über die DentaTool-Plattform abgeschlossen wird, erfolgt der Vertragsschluss durch die elektronische Zustimmung des Auftraggebers.

Anlagen

Die nachfolgenden Anlagen sind Bestandteil dieses Auftragsverarbeitungsvertrages:

- Anlage 1 – Technische und organisatorische Maßnahmen (TOM)
- Anlage 2 – Unterauftragsverarbeiter
- Anlage 3 – Lösch- und Aufbewahrungskonzept
- Anlage 4 – Beschreibung der Datenverarbeitung

Anlage 1

Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 DSGVO

Stand: Version 1.2 (November 2026)

Diese technischen und organisatorischen Maßnahmen beschreiben das Sicherheitskonzept der DentaTool-Plattform und dienen der Gewährleistung eines dem Risiko angemessenen Schutzniveaus gemäß Art. 32 DSGVO.

Die Maßnahmen werden regelmäßig überprüft und entsprechend dem Stand der Technik fortentwickelt.

1. Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, unbefugten Personen den physischen Zugang zu Systemen und Datenträgern zu verwehren.

Die DentaTool-Plattform wird ausschließlich in professionellen Rechenzentren innerhalb Deutschlands betrieben. Anwendungsserver, Datenbank und Datenbanksicherungen liegen beim Hostinganbieter, hochgeladene Dateien im Objektspeicher von Amazon Web Services in der Region Frankfurt (Anlage 2, Nr. 1 und 6).

Die eingesetzten Hosting- und Speicheranbieter stellen insbesondere folgende Maßnahmen sicher:

- mehrstufige Zutrittskontrollen
- elektronische Zugangssysteme
- Videoüberwachung sicherheitsrelevanter Bereiche
- Einbruchmeldeanlagen
- Alarmierungssysteme
- Brandschutzmaßnahmen
- unterbrechungsfreie Stromversorgung
- Notstromversorgung
- Klimatisierung der Serverräume
- Zugang ausschließlich für autorisierte Personen

Der Auftragnehmer selbst betreibt keine eigenen Serverräume.

2. Zugangskontrolle

Ziel der Zugangskontrolle ist die Verhinderung der Nutzung von IT-Systemen durch unbefugte Personen.

Hierzu werden insbesondere folgende Maßnahmen eingesetzt:

- persönliche Benutzerkonten
- individuelle Benutzerkennungen
- Passwortschutz

sichere Passwortspeicherung mittels moderner Hashverfahren
- verschlüsselte Authentifizierung
- Sitzungsverwaltung
- automatische Sitzungsbeendigung nach Inaktivität
- rollenbasierte Benutzerverwaltung
- Sperrung deaktivierter Benutzerkonten
- verschlüsselte Kommunikation mittels TLS

Soweit verfügbar, unterstützt DentaTool die Verwendung einer Zwei-Faktor-Authentifizierung.

3. Zugriffskontrolle

Ziel der Zugriffskontrolle ist sicherzustellen, dass berechtigte Benutzer ausschließlich auf diejenigen Daten zugreifen können, für die sie autorisiert sind.

Hierzu werden insbesondere eingesetzt:

- Rollen- und Berechtigungskonzept
- Mandantenverwaltung
- Zugriff ausschließlich entsprechend der zugewiesenen Benutzerrolle
- Einschränkung administrativer Rechte
- regelmäßige Überprüfung administrativer Berechtigungen
- Protokollierung administrativer Tätigkeiten
- Least-Privilege-Prinzip
- Dateispeicher ohne öffentlichen Zugriff (Block Public Access); Zugriff nur über die Anwendung mit einem eigenen Dienstkonto, das auf Lesen, Schreiben, Löschen und Auflisten des jeweiligen Speichers beschränkt ist

Administratoren des Auftragnehmers erhalten ausschließlich Zugriff, soweit dies zur Fehleranalyse, Wartung oder Erfüllung vertraglicher Supportleistungen erforderlich ist.

4. Trennungskontrolle

DentaTool ist als mandantenfähige Cloud-Plattform entwickelt.

Die Daten verschiedener Auftraggeber werden logisch voneinander getrennt verarbeitet.

Es ist technisch ausgeschlossen, dass Benutzer eines Auftraggebers auf Daten eines anderen Auftraggebers zugreifen können.

Mandantenbezogene Datenzugriffe werden ausschließlich innerhalb des jeweiligen Mandanten ausgeführt.

Auch interne Verwaltungsfunktionen berücksichtigen die Mandantentrennung.

5. Weitergabekontrolle

Personenbezogene Daten werden ausschließlich auf Weisung des Auftraggebers oder auf gesetzlicher Grundlage an Dritte übermittelt.

Zur Sicherstellung der Vertraulichkeit werden insbesondere eingesetzt:

- TLS-Verschlüsselung bei der Datenübertragung
- verschlüsselte E-Mail-Kommunikation soweit technisch möglich

Zugriff ausschließlich über authentifizierte Benutzerkonten
- Berechtigungskonzepte
- vertragliche Verpflichtung sämtlicher Unterauftragsverarbeiter nach Art. 28 DSGVO

Die KI-Modellverarbeitung erfolgt ausschließlich in den EU-Regionen von Amazon Web Services (Frankfurt, Stockholm, Paris, Mailand, Spanien und Irland). Der Auftragnehmer nutzt dafür ausschließlich EU-Inference-Profile; eine Verarbeitung in Regionen außerhalb der Europäischen Union ist technisch ausgeschlossen. Soweit der Unterauftragsverarbeiter zu einer Unternehmensgruppe mit Sitz außerhalb der Europäischen Union gehört, stellt der Auftragnehmer die Voraussetzungen der Art. 44 ff. DSGVO für etwaige Zugriffe aus Drittländern sicher (siehe Anlage 2). Im Übrigen erfolgt eine Übermittlung personenbezogener Daten in Drittstaaten grundsätzlich nicht.

6. Eingabekontrolle

Zur Nachvollziehbarkeit der Datenverarbeitung werden geeignete Protokollierungsmechanismen eingesetzt.

Soweit technisch vorgesehen, werden insbesondere protokolliert:

- Benutzeranmeldungen
- Änderungen wichtiger Stammdaten
- Erstellung und Änderung von Aufträgen
- Änderungen an Benutzerrechten
- administrative Tätigkeiten
- sicherheitsrelevante Ereignisse

Die Protokollierung dient ausschließlich der Systemsicherheit, Fehleranalyse und Nachvollziehbarkeit.

7. Auftragskontrolle

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich auf dokumentierte Weisung des Auftraggebers.

Mitarbeiter des Auftragnehmers erhalten ausschließlich Zugriff auf personenbezogene Daten, soweit dies

- zur Fehlerbehebung,
- zur Wartung,
- zur Weiterentwicklung der Plattform oder
- zur Erfüllung vertraglicher Supportleistungen

erforderlich ist.

Alle Mitarbeiter sind auf Vertraulichkeit verpflichtet.

Unterauftragsverarbeiter werden ausschließlich nach Abschluss eines Vertrages gemäß Art. 28 DSGVO eingesetzt.

8. Verfügbarkeitskontrolle

Zum Schutz vor Verlust personenbezogener Daten werden unter anderem folgende Maßnahmen eingesetzt:

- regelmäßige Datensicherungen
- redundante Speichersysteme der Hosting- und Speicheranbieter
- Versionierung des Dateispeichers (gelöschte oder überschriebene Dateien sind bis zu 30 Tage wiederherstellbar)
- Monitoring zentraler Systemkomponenten
- automatische Fehlerüberwachung
- Wiederherstellungsverfahren
- Schutz vor Stromausfällen
- Brandschutzmaßnahmen im Rechenzentrum
- redundante Internetanbindungen der Hosting- und Speicheranbieter

Datensicherungen werden regelmäßig überprüft.

9. Verschlüsselung

Zum Schutz personenbezogener Daten werden geeignete Verschlüsselungsverfahren eingesetzt.

Hierzu gehören insbesondere:

- TLS für sämtliche Datenübertragungen
- serverseitige Verschlüsselung der im Objektspeicher abgelegten Dateien (AES-256)
- verschlüsselte Speicherung von Passwörtern mittels moderner Hashverfahren
- verschlüsselte Speicherung sicherheitsrelevanter Zugangsdaten
- verschlüsselte Sicherungskopien, soweit technisch vorgesehen

Kryptographische Verfahren werden regelmäßig entsprechend dem Stand der Technik überprüft.

Schutz besonders sensibler personenbezogener Daten

Zum zusätzlichen Schutz personenbezogener Daten werden ausgewählte Datenfelder mit besonderem Schutzbedarf bereits auf Anwendungsebene verschlüsselt gespeichert.

Hierzu zählen insbesondere personenbezogene Daten, deren Offenlegung ein erhöhtes Risiko für die Rechte und Freiheiten betroffener Personen begründen würde, wie beispielsweise Patientennamen.

Die hierfür eingesetzten kryptographischen Verfahren und Schlüssel werden durch den Auftragnehmer nach dem Stand der Technik verwaltet und regelmäßig überprüft.

Die Verschlüsselung ergänzt die weiteren technischen und organisatorischen Maßnahmen und dient der Verringerung des Risikos eines unbefugten Zugriffs auf personenbezogene Daten.

Die Verschlüsselung erfolgt zusätzlich zu den Maßnahmen der Transportverschlüsselung sowie der Zugriffskontrolle und stellt einen weiteren Baustein des Sicherheitskonzepts der DentaTool-Plattform dar.

10. Wiederherstellbarkeit

Zur Sicherstellung der Wiederherstellbarkeit personenbezogener Daten bestehen Verfahren zur regelmäßigen Datensicherung.

Im Rahmen des Backupkonzeptes werden Datensicherungen erstellt und für einen begrenzten Zeitraum vorgehalten.

Die Wiederherstellung einzelner Systeme kann im Bedarfsfall durchgeführt werden.

11. Belastbarkeit der Systeme

Die Plattform wird kontinuierlich überwacht.

Hierzu gehören insbesondere:

- Servermonitoring
- Fehlerüberwachung
- Ressourcenüberwachung
- Log-Auswertung
- automatische Benachrichtigung bei kritischen Systemzuständen

Sicherheitsupdates werden zeitnah eingespielt.

12. Datenschutz durch Technikgestaltung

Bereits bei Entwicklung neuer Funktionen werden Datenschutzanforderungen berücksichtigt.

Hierzu gehören insbesondere:

- Datenminimierung
- rollenbasierte Berechtigungen
- Mandantentrennung
- sichere Standardkonfigurationen
- datenschutzfreundliche Voreinstellungen
- regelmäßige Sicherheitsüberprüfung neuer Funktionen

Neue Funktionen werden vor ihrer Bereitstellung getestet.

13. Datenschutzfreundliche Voreinstellungen

Standardmäßig werden ausschließlich diejenigen personenbezogenen Daten verarbeitet, die zur Erbringung der jeweiligen Funktion erforderlich sind.

Neue Funktionen werden unter Berücksichtigung des Grundsatzes der Datenminimierung entwickelt.

14. Mitarbeiterschulung

Mitarbeiter des Auftragnehmers werden regelmäßig hinsichtlich

- Datenschutz,
- Informationssicherheit,
- Vertraulichkeit sowie
- sicherem Umgang mit personenbezogenen Daten

sensibilisiert.

Zugriffsberechtigungen werden regelmäßig überprüft und bei Ausscheiden eines Mitarbeiters unverzüglich entzogen.

15. Sichere Softwareentwicklung

Der Auftragnehmer berücksichtigt Anforderungen der Informationssicherheit und des Datenschutzes bereits während der Entwicklung neuer Funktionen der DentaTool-Plattform.

Hierzu gehören insbesondere:

- Entwicklung nach etablierten Grundsätzen sicherer Softwareentwicklung (Secure Development Lifecycle)
- Verwendung einer Versionsverwaltung zur Nachvollziehbarkeit sämtlicher Quellcodeänderungen
- Dokumentation von Änderungen im Rahmen des Entwicklungsprozesses
- Prüfung neuer Funktionen vor deren Bereitstellung in der Produktivumgebung
- Zeitnahe Installation sicherheitsrelevanter Updates für eingesetzte Softwarekomponenten
- Regelmäßige Aktualisierung von Abhängigkeiten und Bibliotheken im Rahmen der technischen Wartung
- Beschränkung des Zugriffs auf Entwicklungs- und Produktivsysteme auf autorisierte Personen
- Verwendung getrennter Entwicklungs-, Test- und Produktivumgebungen, soweit technisch vorgesehen

Neue Funktionen werden vor ihrer Bereitstellung auf ihre technische Funktionsfähigkeit sowie auf erkennbare Sicherheitsrisiken überprüft.

Der Auftragnehmer verfolgt bekannte Sicherheitslücken in den eingesetzten Softwarekomponenten und behebt diese im Rahmen eines risikoorientierten Patchmanagements.

16. Administrativer Zugriff und Support

Der Auftragnehmer beschränkt den Zugriff auf personenbezogene Daten auf diejenigen Mitarbeiter, deren Zugriff zur Erfüllung ihrer jeweiligen Aufgaben erforderlich ist.

Administrativer Zugriff auf Kundendaten erfolgt ausschließlich

- zur Fehleranalyse,
- zur Fehlerbehebung,
- zur Durchführung von Wartungsarbeiten,
- zur Erfüllung vertraglich vereinbarter Supportleistungen oder
- zur Gewährleistung eines sicheren Betriebs der Plattform.

Supportzugriffe erfolgen ausschließlich durch hierzu autorisierte Mitarbeiter.

Der Zugriff wird auf das zur Erfüllung des jeweiligen Zwecks erforderliche Maß beschränkt.

Mitarbeiter des Auftragnehmers sind auf die Vertraulichkeit personenbezogener Daten verpflichtet und werden regelmäßig hinsichtlich Datenschutz und Informationssicherheit sensibilisiert.

Soweit technisch vorgesehen, werden administrative Tätigkeiten protokolliert.

Der Auftragnehmer ist bestrebt, die Möglichkeiten zur Nachvollziehbarkeit administrativer Zugriffe sowie deren technische Einschränkung fortlaufend weiterzuentwickeln.

17. Mandantenfähigkeit und logische Datentrennung

Die DentaTool-Plattform ist als mandantenfähige (Multi-Tenant-)Cloud-Anwendung konzipiert.

Ziel der Mandantenarchitektur ist es, sicherzustellen, dass personenbezogene Daten verschiedener Auftraggeber jederzeit logisch voneinander getrennt verarbeitet werden und ausschließlich berechtigten Benutzern innerhalb des jeweiligen Mandanten zugänglich sind.

Hierzu werden insbesondere folgende Maßnahmen umgesetzt:

- Jeder Auftraggeber erhält einen eigenen logisch getrennten Mandanten innerhalb der Plattform.
- Benutzerkonten sind eindeutig einem Mandanten zugeordnet.
- Datenzugriffe erfolgen ausschließlich innerhalb des jeweils zugeordneten Mandanten.
- Berechtigungen werden serverseitig geprüft und durchgesetzt.
- Benutzer können ausschließlich auf Daten zugreifen, für die ihnen innerhalb ihres Mandanten entsprechende Berechtigungen erteilt wurden.
- Ein Zugriff auf Daten anderer Mandanten ist technisch ausgeschlossen.
- Die Mandantenzuordnung erfolgt zentral innerhalb der Anwendung und wird bei sämtlichen datenverarbeitenden Vorgängen berücksichtigt.
- Administrative Funktionen berücksichtigen die Mandantentrennung und beschränken Zugriffe auf das jeweils erforderliche Maß.

Die Mandantentrennung stellt einen wesentlichen Bestandteil des Sicherheitskonzeptes der DentaTool-Plattform dar und dient dem Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten personenbezogenen Daten.

18. Regelmäßige Überprüfung und Weiterentwicklung

Der Auftragnehmer überprüft die in dieser Anlage beschriebenen technischen und organisatorischen Maßnahmen regelmäßig auf ihre Wirksamkeit und Angemessenheit.

Soweit erforderlich, werden die Maßnahmen unter Berücksichtigung des Stands der Technik, technischer Weiterentwicklungen, neuer Bedrohungslagen sowie geänderter gesetzlicher oder regulatorischer Anforderungen angepasst.

Dabei wird sichergestellt, dass das Schutzniveau der Verarbeitung personenbezogener Daten nicht abgesenkt wird.

19. KI-Assistenten (Amazon Bedrock)

Diese Maßnahmen gelten für die KI-Funktionen (Web-Assistent und KI-Auftragszettelerfassung), soweit der Auftraggeber sie nutzt. Abweichend von Ziffer 1 erfolgt die Modellverarbeitung nicht in Rechenzentren in Deutschland, sondern in den EU-Regionen des Unterauftragsverarbeiters Amazon Web Services EMEA SARL (Anlage 2, Nr. 4). Die Plattform selbst wird weiterhin bei dem in Anlage 2 genannten Hostinganbieter betrieben.

Es bestehen insbesondere folgende Maßnahmen:

- Begrenzung auf Mandant und Berechtigte: Der Assistent sieht nur Daten des eigenen Labors; Praxisnutzer sehen nur Daten ihrer eigenen Praxis. Aktionen werden serverseitig gegen die Berechtigungen des handelnden Benutzers geprüft.
- Nutzung nur nach Zustimmung zum AVV: Die KI-Funktionen sind erst nach Zustimmung (Testphase) oder Vertragsschluss verfügbar.

Feste Modellfreigabe: Nur freigegebene Modelle von Amazon Bedrock im EU-Inferenzprofil sind konfigurierbar; eine andere Konfiguration verhindert den Start der Anwendung.

- Keine Aufbewahrung beim Modellanbieter: Aufbewahrung der Ein- und Ausgaben ist in allen Regionen des Profils ausgeschlossen, die Protokollierung der Modellaufrufe ist ausgeschaltet.
- Datenminimierung: Das Modell erhält nur die für die Anfrage nötigen Abfrageergebnisse und den Gesprächsverlauf der jeweiligen Unterhaltung.
- Schutz vor Missbrauch: Mengenbegrenzung der Anfragen je Benutzer und Labor; Inhalte aus Nachrichten werden als Daten behandelt und können die Regeln des Assistenten nicht ändern; bei Fehlern oder Zweifeln erfolgt die Übergabe an das Labor.
- Nachvollziehbarkeit: Ausgeführte Aktionen des Assistenten werden protokolliert; Inhalte von KI-Antworten werden nicht in Betriebsprotokolle geschrieben.
- Löschung: Unterhaltungen werden nach der vom Auftraggeber gewählten Frist (7 Tage, 30 Tage oder 12 Monate seit der letzten Nachricht) automatisch gelöscht.
- Transportverschlüsselung (TLS) zum Modellservice.
- Eigener, beschränkter Zugang zum Modellservice: Der Zugang erfolgt über einen eigens dafür angelegten technischen Zugang, dessen Rechte auf den Modellaufruf in den EU-Regionen beschränkt sind. Er hat keine Rechte für andere Dienste, für die Konfiguration oder für Abonnements.
- Mehrfaktor-Authentifizierung für die Konsole: Die Konsolenzugänge zur Cloud-Umgebung (Administrator und Hauptkonto) sind durch Mehrfaktor-Authentifizierung geschützt.
- Protokollierung von Konfigurationsänderungen: Änderungen und Anmeldungen in der Cloud-Umgebung werden über AWS CloudTrail in allen Regionen protokolliert; die Protokolle liegen in einem nicht öffentlichen Speicher in der EU (Frankfurt), sind durch eine Integritätsprüfung gegen Manipulation geschützt und werden nach 12 Monaten automatisch gelöscht. Die Modellaufrufe selbst und ihre Inhalte werden nicht protokolliert.

Anlage 2

Genehmigte Unterauftragsverarbeiter

gemäß Art. 28 Abs. 2 DSGVO

Stand: Version 1.3 (15. November 2026)

Der Auftragnehmer ist berechtigt, zur Erfüllung seiner vertraglichen Leistungen die nachfolgend aufgeführten Unterauftragsverarbeiter einzusetzen.

Alle Unterauftragsverarbeiter werden vor ihrer Beauftragung sorgfältig ausgewählt und vertraglich gemäß Art. 28 DSGVO zur Einhaltung eines angemessenen Datenschutzniveaus verpflichtet.

Die Verarbeitung erfolgt ausschließlich im zur Leistungserbringung erforderlichen Umfang.

---

1. Hosting

Unternehmen	**Hetzner Online GmbH**
Anschrift	Industriestraße 25, 91710 Gunzenhausen, Deutschland
Leistung	Hosting und Betrieb der DentaTool-Plattform (Anwendungsserver, Datenbank und Datenbanksicherungen)
Zweck	Bereitstellung der Serverinfrastruktur sowie Speicherung und Verarbeitung der Kundendaten in der Datenbank
Datenkategorien	Die im Rahmen der Nutzung von DentaTool in der Datenbank verarbeiteten personenbezogenen Daten. Die in Nr. 6 genannten Dateien werden nicht bei diesem Unterauftragsverarbeiter gespeichert.
Verarbeitungsort	Deutschland

---

2. Versand transaktionaler E-Mails

Unternehmen	**Brevo SAS**
Anschrift	106 Boulevard Haussmann, 75008 Paris, Frankreich
Leistung	Versand transaktionaler E-Mails
Zweck	Versand von Systembenachrichtigungen, Passwort-Reset-E-Mails, Einladungen, Benachrichtigungen und sonstigen systemseitigen E-Mails
Datenkategorien	E-Mail-Adresse, Name (soweit vorhanden), Inhalte der versendeten Nachricht, technische Versandinformationen
Verarbeitungsort	Europäische Union

---

3. Unternehmenskommunikation

Unternehmen	**Zoho Corporation B.V.**
Anschrift	Beneluxlaan 4B, 3527 HT Utrecht, Niederlande
Leistung	Bereitstellung des E-Mail-Dienstes für die Unternehmenskommunikation
Zweck	Bearbeitung von Kundenanfragen und Supportkommunikation per E-Mail
Datenkategorien	E-Mail-Adresse, Name, Kommunikationsinhalte
Verarbeitungsort	Europäische Union

---

4. KI-Modellverarbeitung

Unternehmen	**Amazon Web Services EMEA SARL**
Anschrift	38 Avenue John F. Kennedy, L-1855 Luxemburg
Leistung	Bereitstellung von Sprachmodellen über Amazon Bedrock (Modell Claude Sonnet 5.5, EU-Inferenzprofil)
Zweck	Verarbeitung von Anfragen im KI-Assistenten (Web) sowie Auswertung von Auftragszettel-Bildern zur Erfassungsunterstützung
Datenkategorien	Nachrichten und Gesprächsverläufe, Namen von Patienten, Praxen und Mitarbeitern, Auftrags-, Zahn- und Abrechnungsangaben, Bilder von Auftragszetteln; auch Gesundheitsdaten
Verarbeitungsort	Europäische Union (Frankfurt, Stockholm, Paris, Mailand, Spanien, Irland)

Die Modellverarbeitung erfolgt in den genannten Regionen. Eingaben und Ausgaben werden dort nach den Einstellungen im Konto des Auftragnehmers nicht gespeichert (Aufbewahrungsmodus „keine Aufbewahrung“); die Protokollierung der Modellaufrufe ist ausgeschaltet. Der Anbieter des Sprachmodells erhält nach der Dokumentation von AWS keinen Zugriff auf die Inhalte und ist kein Unterauftragsverarbeiter des Auftragnehmers. Nutzungsmetadaten ohne Inhalte können nach den

Service Terms von AWS an den Modellanbieter weitergegeben werden.

---

5. Versand transaktionaler E-Mails (Lettermint)

Unternehmen	**Lettermint B.V.**
Anschrift	Willemsvaart 16 B, 8019 AB Zwolle, Niederlande
Leistung	Versand transaktionaler E-Mails einschließlich Zustell-, Bounce- und Beschwerdeverarbeitung
Zweck	Versand von Systembenachrichtigungen, Passwort-Reset-E-Mails, Einladungen, Benachrichtigungen und sonstigen systemseitigen E-Mails
Datenkategorien	Absender- und Empfängeradressen, Namen, Betreff, Nachrichteninhalte und Anhänge sowie technische Versanddaten; je nach Nachricht auch Gesundheitsdaten
Verarbeitungsort	Europäische Union. Die aktuelle Dienstleisterkette für E-Mail-Daten umfasst UpCloud (Niederlande, Hosting), OVH (Deutschland, verschlüsselte Sicherungen) und Postmastery (Niederlande, Überwachung der Zustellbarkeit).

Nach dem Data Processing Agreement des Anbieters (Fassung vom 9. Oktober 2026, abgerufen am 31. Oktober 2026) werden Nachrichteninhalte und Anhänge grundsätzlich 28 Tage nach Erstellung der Nachricht aufbewahrt, soweit im Dienst keine andere Frist konfiguriert ist. Für Versandereignisse und Sicherungskopien gelten die in Anlage 3 beschriebenen Fristen.

Mit der Lettermint B.V. besteht ein Vertrag zur Auftragsverarbeitung (Data Processing Agreement gemäß Art. 28 DSGVO) sowie eine Vertraulichkeitsvereinbarung im Hinblick auf § 203 StGB.

---

6. Speicherung von Dateien (Objektspeicher)

Unternehmen	**Amazon Web Services EMEA SARL**
Anschrift	38 Avenue John F. Kennedy, L-1855 Luxemburg
Leistung	Bereitstellung von Objektspeicher (Amazon Simple Storage Service, Amazon S3)
Zweck	Speicherung und Bereitstellung der in DentaTool hochgeladenen und erzeugten Dateien
Datenkategorien	Inhalt der abgelegten Dateien, insbesondere Fotos, Scans, digitale Abdrücke und Bilddaten (STL, PLY, OBJ, JPG, PNG), Auftragszettel, PDF-Dokumente, Rechnungen und sonstige Anhänge; je nach Datei Patientenbezug und Gesundheitsdaten
Verarbeitungsort	Deutschland (AWS-Region Europa Frankfurt, eu-central-1)

Die Dateien werden ausschließlich in der genannten Region gespeichert und dort serverseitig verschlüsselt (AES-256). Der öffentliche Zugriff auf den Speicher ist technisch gesperrt; der Zugriff erfolgt nur über die DentaTool-Anwendung mit einem eigenen Dienstkonto, das ausschließlich Lese-, Schreib-, Lösch- und Auflistungsrechte für diesen Speicher besitzt. Der Speicher ist versioniert: Gelöschte oder überschriebene Dateien werden nach der Löschung in DentaTool noch bis zu 30 Tage als nicht abrufbare Vorversion vorgehalten und danach endgültig gelöscht (siehe Anlage 3).

Die in Nr. 4 genannte Beauftragung desselben Unternehmens für die KI-Modellverarbeitung bleibt unberührt. Für die Speicherung gilt das AWS Data Processing Addendum; die Hinweise zu internationalen Datenübermittlungen unten gelten entsprechend.

Wechsel oder Hinzunahme weiterer Unterauftragsverarbeiter

Der Auftragnehmer ist berechtigt, weitere Unterauftragsverarbeiter einzusetzen oder bestehende Unterauftragsverarbeiter zu ersetzen, soweit dies zur Erbringung der vertraglich geschuldeten Leistungen erforderlich ist.

Der Auftraggeber wird hierüber mindestens 30 Kalendertage vor dem geplanten Einsatz in Textform informiert.

Dem Auftraggeber steht innerhalb dieser Frist ein Widerspruchsrecht aus wichtigem datenschutzrechtlichem Grund zu.

Erfolgt innerhalb der Frist kein Widerspruch, gilt die Zustimmung als erteilt.

Datenschutzrechtliche Verpflichtung

Der Auftragnehmer stellt sicher, dass sämtliche Unterauftragsverarbeiter

- ausschließlich auf dokumentierte Weisung des Auftragnehmers tätig werden,
- zur Vertraulichkeit verpflichtet sind,
- geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO umgesetzt haben,
- personenbezogene Daten ausschließlich zur Erfüllung der beauftragten Leistungen verarbeiten,
- die Anforderungen der DSGVO einhalten.

Internationale Datenübermittlungen

Der Auftragnehmer setzt Unterauftragsverarbeiter grundsätzlich innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums ein.

Soweit in Einzelfällen eine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt oder ein Unterauftragsverarbeiter Konzernstrukturen außerhalb dieses Gebiets nutzt, stellt der Auftragnehmer sicher, dass die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO eingehalten werden. Hierzu werden insbesondere geeignete Garantien, wie ein Angemessenheitsbeschluss der Europäischen Kommission oder die jeweils gültigen Standardvertragsklauseln (Standard Contractual Clauses – SCC), herangezogen.

Die Amazon Web Services EMEA SARL gehört zu einer Unternehmensgruppe mit Sitz in den USA. Dies betrifft sowohl die KI-Modellverarbeitung (Nr. 4) als auch die Dateispeicherung (Nr. 6). Für einen Zugriff von Konzerngesellschaften außerhalb der Europäischen Union stützt sich die Übermittlung auf die Standardvertragsklauseln des AWS Data Processing Addendum (Ziff. 12, abgerufen am 31. Oktober 2026 unter d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf). AWS verarbeitet die Daten nur in der gewählten Region, soweit nicht zur Erbringung der Dienste oder aufgrund Gesetzes etwas anderes nötig ist (Ziff. 12.1). Im Zusatz zum AWS Data Processing Addendum verpflichtet sich AWS außerdem, Anfragen von Behörden an den Kunden zu verweisen, ihn über Anfragen zu informieren, übermäßige oder mit EU-Recht unvereinbare Anfragen anzufechten und nur die erforderliche Mindestmenge herauszugeben (Ziff. 1), und sichert zu, keinen Grund zur Annahme zu haben, dass die für sie geltende Rechtslage die Erfüllung der Pflichten verhindert (Ziff. 3).

Anlage 3

Lösch- und Aufbewahrungskonzept

Stand: Version 1.3 (15. November 2026)

Diese Anlage beschreibt die Grundsätze zur Löschung, Aufbewahrung und Rückgabe personenbezogener Daten, die im Rahmen der Nutzung der DentaTool-Plattform verarbeitet werden.

Die Regelungen ergänzen die Bestimmungen des Auftragsverarbeitungsvertrages.

1. Grundsatz der Datenlöschung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich für die Dauer des zwischen den Parteien bestehenden Vertragsverhältnisses oder solange eine gesetzliche Verpflichtung zur Speicherung besteht.

Nach Beendigung des Vertragsverhältnisses werden personenbezogene Daten entsprechend den nachfolgenden Regelungen gelöscht oder anonymisiert, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

2. Rückgabe der Daten

Vor der endgültigen Löschung erhält der Auftraggeber auf Wunsch Gelegenheit, seine innerhalb der DentaTool-Plattform gespeicherten Daten über die bereitgestellten Exportfunktionen oder in einem geeigneten maschinenlesbaren Format zu exportieren.

Ein Anspruch auf Herausgabe von Quellcode, Datenbankschemata, internen Systemkonfigurationen oder sonstigen Geschäftsgeheimnissen des Auftragnehmers besteht nicht.

3. Löschung produktiver Daten

Nach Vertragsbeendigung werden die produktiven Daten des Auftraggebers grundsätzlich rund 30 Kalendertage nach Vertragsende gelöscht, sofern

- keine gesetzliche Aufbewahrungspflicht besteht,
- keine berechtigten Ansprüche aus dem Vertragsverhältnis mehr geltend gemacht werden können und
- der Auftraggeber keine abweichende Weisung erteilt hat.

Die Löschung umfasst sämtliche personenbezogenen Daten des jeweiligen Mandanten einschließlich der zugehörigen Dokumente und Dateianhänge.

4. Datensicherungen (Backups)

Zur Gewährleistung der Systemsicherheit erstellt der Auftragnehmer regelmäßig Datensicherungen.

Diese Datensicherungen dienen ausschließlich

- der Wiederherstellung nach technischen Störungen,
- der Absicherung gegen Datenverlust sowie
- der Sicherstellung der Betriebsfähigkeit der Plattform.

Datensicherungen werden rund 30 Tage vorgehalten und danach automatisch gelöscht. Daten aus gelöschten Unterhaltungen oder gelöschten Mandanten verschwinden damit rund 30 Tage nach der

Löschung auch aus den Sicherungen.

Eine gezielte Löschung einzelner Datensätze aus bestehenden Datensicherungen erfolgt grundsätzlich nicht.

Personenbezogene Daten werden spätestens mit der regulären Überschreibung der jeweiligen Datensicherung endgültig entfernt.

Datensicherungen werden nicht produktiv genutzt und ausschließlich im Rahmen technischer Wiederherstellungsverfahren verarbeitet.

5. Protokolldaten

System- und Sicherheitsprotokolle werden ausschließlich zur Gewährleistung des sicheren Betriebs der Plattform verarbeitet.

Hierzu zählen insbesondere

- Anmeldeprotokolle,
- Fehlermeldungen,
- Sicherheitsereignisse,
- technische Betriebsprotokolle.

Protokolldaten werden nur so lange gespeichert, wie dies zur Gewährleistung der Informationssicherheit, Fehleranalyse oder zur Erfüllung gesetzlicher Verpflichtungen erforderlich ist.

6. Supportdaten

Personenbezogene Daten, die im Rahmen von Supportanfragen verarbeitet werden, werden nur für die Bearbeitung der jeweiligen Anfrage sowie für eine angemessene Dokumentation der Supportleistung gespeichert.

Nach Wegfall des jeweiligen Zwecks werden diese Daten gelöscht, soweit keine gesetzlichen Aufbewahrungspflichten bestehen.

7. Gesetzliche Aufbewahrungspflichten

Soweit gesetzliche Aufbewahrungspflichten einer Löschung entgegenstehen, werden die betreffenden Daten bis zum Ablauf der jeweiligen Fristen ausschließlich zu diesem Zweck aufbewahrt.

Während dieser Zeit erfolgt keine Verarbeitung zu anderen Zwecken.

Nach Ablauf der gesetzlichen Aufbewahrungsfrist werden die Daten gelöscht.

8. Anonymisierung

Soweit eine vollständige Löschung technisch oder rechtlich nicht möglich oder unverhältnismäßig ist, können personenbezogene Daten anonymisiert werden.

Die Anonymisierung erfolgt so, dass ein Personenbezug dauerhaft ausgeschlossen ist.

Anonymisierte Daten gelten nicht mehr als personenbezogene Daten im Sinne der DSGVO.

9. Nachweis der Löschung

Der Auftragnehmer dokumentiert Löschvorgänge im erforderlichen Umfang.

Über die Löschung eines Mandanten führt der Auftragnehmer ein Löschprotokoll mit Zeitpunkt und Zählern; es enthält keine Inhalte der gelöschten Daten.

Auf Wunsch des Auftraggebers bestätigt der Auftragnehmer die Löschung personenbezogener Daten in geeigneter Form.

10. Regelmäßige Überprüfung

Der Auftragnehmer überprüft dieses Lösch- und Aufbewahrungskonzept regelmäßig und passt es bei technischen oder rechtlichen Änderungen an.

11. KI-Assistenten (Amazon Bedrock)

Für die KI-Funktionen (Web-Assistent und KI-Auftragszettelerfassung) gelten zusätzlich folgende Fristen:

- **Unterhaltungen des Web-Assistenten** (Nachrichten, Tool-Zeilen und Dokumente) werden nach der vom Auftraggeber gewählten Frist gelöscht: 7 Tage (Standard), 30 Tage oder 12 Monate seit der letzten Nachricht. Die Löschung erfolgt durch einen täglichen automatischen Lauf. Aufträge und am Auftrag abgelegte Dateien bleiben bestehen.
- **Anfragen und Antworten beim Modellanbieter** werden nicht gespeichert (Aufbewahrungsmodus „keine Aufbewahrung“, Protokollierung der Modellaufrufe ausgeschaltet).
- **Auftragszettel-Scans, bestätigt:** Original und erkannte Daten werden wie der zugehörige Auftrag aufbewahrt; das Bild wird am Auftrag abgelegt.
- **Auftragszettel-Scans, nicht bestätigt:** Es gibt keine automatische Löschfrist. Original und erkannte Daten verbleiben bis zur Löschung durch den Auftraggeber oder bis zur Löschung des Mandanten.
- **Testphase ohne Vertrag:** Die im Test verarbeiteten Daten werden rund 30 Tage nach dem Ende der Testphase gelöscht, einschließlich der KI-Unterhaltungen und Auftragszettel-Scans.

12. Versand von E-Mails

Bei Lettermint (Anlage 2, Nr. 5) werden Nachrichteninhalte, Anhänge, Empfängeradressen und Nachrichtenmetadaten grundsätzlich 28 Tage nach Erstellung der Nachricht aufbewahrt, soweit im Dienst keine andere Frist konfiguriert ist. Zustellereignisse und daraus gebildete Auswertungssummen werden nach Angaben des Anbieters höchstens 90 Tage aufbewahrt; Restkopien können nach der Löschung aus aktiven Systemen bis zu 14 Tage in verschlüsselten und zugriffsbeschränkten Sicherungen verbleiben (Data Processing Agreement, Ziff. 3.1 und 11.5, Fassung vom 9. Oktober 2026). Öffnungs- und Klicktracking werden für den transaktionalen Versand nicht eingesetzt.

Das lokale E-Mail-Protokoll in DentaTool ist hiervon getrennt. Es speichert die zur Zuordnung und Zustellanzeige erforderlichen Angaben, insbesondere Empfänger, Betreff, Nachrichtenkennung, Status und Ereigniszeit. Für diese Protokolle besteht derzeit keine automatische zeitbasierte Löschfrist; sie werden spätestens mit der Löschung des Mandanten entfernt. Vollständige Lettermint-Webhook-Payloads werden dort nicht gespeichert.

13. Dateispeicher (Objektspeicher)

Hochgeladene und erzeugte Dateien (Anlage 2, Nr. 6) werden im versionierten Objektspeicher von Amazon Web Services in der Region Frankfurt gespeichert. Für sie gilt zusätzlich:

- **Löschung in DentaTool:** Wird eine Datei in DentaTool gelöscht, ist sie für Benutzer und Anwendung sofort nicht mehr abrufbar.
- **Vorversion im Speicher:** Technisch verbleibt die gelöschte oder überschriebene Datei bis zu 30 Tage als nicht abrufbare Vorversion im Objektspeicher und wird danach automatisch endgültig gelöscht. Eine Wiederherstellung erfolgt nur durch den Auftragnehmer bei versehentlicher Löschung oder technischen Störungen.
- **Löschung eines Mandanten:** Die Dateien des Mandanten werden nach Ziffer 3 gelöscht. Auch hier verbleiben Vorversionen bis zu 30 Tage und werden danach endgültig entfernt; diese Frist entspricht der Vorhaltezeit der Datensicherungen nach Ziffer 4.
- **Abgebrochene Uploads:** Unvollständig übertragene Dateien werden spätestens nach 7 Tagen automatisch verworfen.

Anlage 4

Beschreibung der Datenverarbeitung

Stand: Version 1.2 (31. Oktober 2026)

Diese Anlage beschreibt die wesentlichen Verarbeitungsvorgänge, die der Auftragnehmer im Rahmen der Bereitstellung und des Betriebs der DentaTool-Plattform im Auftrag des Auftraggebers durchführt.

Die nachfolgende Übersicht dient ausschließlich der Beschreibung der Auftragsverarbeitung und begründet keine eigenständigen Verarbeitungszwecke des Auftragnehmers.

Übersicht der Verarbeitungstätigkeiten

Verarbeitungstätigkeit	Zweck	Kategorien personenbezogener Daten	Betroffene Personen
Benutzerverwaltung	Verwaltung von Benutzerkonten und Zugriffsrechten	Name, E-Mail-Adresse, Benutzerkennung, Rollen, Passworthash	Mitarbeiter des Auftraggebers
Authentifizierung	Anmeldung an der Plattform	Benutzerkennung, Passworthash, Login-Zeitpunkt, IP-Adresse	Benutzer
Kundenverwaltung	Verwaltung von Zahnarztpraxen und Ansprechpartnern	Kontaktdaten, Kommunikationsdaten	Zahnärzte, Praxispersonal
Patientenverwaltung	Verwaltung zahntechnischer Aufträge	Patientendaten, Gesundheitsdaten	Patienten
Auftragsverwaltung	Planung und Bearbeitung zahntechnischer Arbeiten	Auftragsdaten, Termine, Notizen	Patienten, Zahnärzte
Dokumentenverwaltung	Speicherung und Bereitstellung von Dokumenten	PDF, Fotos, CAD-Dateien, Scans, Rechnungen	Patienten, Zahnärzte
Uploads	Speicherung digitaler Dateien	STL, PLY, OBJ, JPG, PNG, PDF, XML und weitere Dateiformate	Patienten
Kommunikation	Austausch zwischen Labor und Zahnarztpraxis	Nachrichten, Kommentare, Rückfragen	Zahnärzte, Praxispersonal
Benachrichtigungen und Dokumentenversand	Versand transaktionaler E-Mails und Verarbeitung von Zustellmeldungen	Absender- und Empfängeradressen, Namen, Betreff, Inhalte, Anhänge und technische Versanddaten; je nach Nachricht auch Gesundheitsdaten	Benutzer, Zahnärzte, Praxispersonal, Patienten, soweit in der Nachricht genannt
Rechnungswesen	Erstellung und Verwaltung von Rechnungen und Kostenvoranschlägen	Rechnungsdaten, Kontaktdaten	Auftraggeber, Zahnärzte
Materialverwaltung	Dokumentation eingesetzter Materialien	Chargeninformationen, Materialdaten	Patienten

Verarbeitungstätigkeit	Zweck	Kategorien personenbezogener Daten	Betroffene Personen
MDR-Dokumentation	Erfüllung gesetzlicher Dokumentationspflichten	Produkt-, Chargen- und Patientenzuordnung	Patienten
Kalender- und Terminverwaltung	Organisation von Terminen und Fristen	Termininformationen	Benutzer
Arbeitszeiterfassung (optional)	Verwaltung von Arbeitszeiten und Abwesenheiten	Mitarbeiterdaten, Zeitbuchungen	Mitarbeiter des Auftraggebers
Protokollierung	Gewährleistung der Systemsicherheit	Logdaten, IP-Adresse, Zeitstempel, Browserinformationen	Benutzer
Datensicherung	Wiederherstellung der Plattform nach technischen Störungen	Sämtliche im Auftrag verarbeiteten Daten	Alle betroffenen Personen
Support	Bearbeitung von Supportanfragen und Fehleranalysen	Je nach Einzelfall erforderliche personenbezogene Daten	Benutzer
KI-Assistent (Web), soweit beauftragt	Beantwortung von Anfragen, Abruf auftragsbezogener Daten und Ausführung von Aktionen im Rahmen der Berechtigungen des Benutzers	Nachrichten, Gesprächsverläufe, Namen von Patienten, Praxen und Mitarbeitern, Auftrags-, Zahn- und Abrechnungsangaben, Aktionsprotokolle; auch Gesundheitsdaten	Patienten, Zahnärzte, Praxispersonal, Mitarbeiter des Auftraggebers
KI-Auftragszettelerfassung, soweit beauftragt	Auswertung von Bildern von Auftragszetteln zu Erfassungsvorschlägen, die der Benutzer prüft	Bilder von Auftragszetteln mit Patienten-, Auftrags- und Gesundheitsdaten; Name des Labors, Namen der Praxen, Produktbezeichnungen	Patienten, Zahnärzte, Praxispersonal

Kommunikation per E-Mail

DentaTool versendet Systembenachrichtigungen, Passwort-Reset-E-Mails, Einladungen und beauftragte Dokumente, etwa Rechnungen oder Kostenvoranschläge. Für den Versand und die Zustell-, Bounce- und Beschwerdeverarbeitung wird Lettermint (Anlage 2, Nr. 5) eingesetzt. Der Anbieter verarbeitet die hierfür erforderlichen Nachrichten einschließlich Anhängen sowie die Versandmetadaten innerhalb der Europäischen Union. Versandereignisse werden dem lokalen E-Mail-Protokoll zugeordnet. Öffnungs- und Klicktracking werden nicht eingesetzt. Die Aufbewahrung beim Anbieter und im lokalen Protokoll ist in Anlage 3, Ziffer 12 beschrieben.

KI-gestützte Funktionen

Web-Assistent: Ein angemeldeter Benutzer des Labors oder der Praxis stellt eine Anfrage im Browser. Der Assistent sendet die Nachricht, den bisherigen Gesprächsverlauf der Unterhaltung, den Namen des Labors und der Praxis, das Datum und die für die Anfrage nötigen Abfrageergebnisse (zum Beispiel Auftrag, Patientenname, Zahnangaben, Status, Termine) an das Sprachmodell bei Amazon Bedrock (EU) und speichert Anfrage, Antwort und Aktionsprotokoll im Mandanten. Der Assistent kann im Rahmen der Berechtigungen Daten ändern, Dokumente bereitstellen und Kostenvoranschläge samt Auftrag anlegen. Betroffene: Patienten, Mitarbeiter und Ärzte der Praxen, Mitarbeiter des Labors.

KI-Auftragszettelerfassung: Ein Benutzer des Labors lädt das Foto oder den Scan eines Auftragszettels hoch. Das Original wird im Mandanten gespeichert. Eine verkleinerte Bildkopie wird

zusammen mit dem Namen des Labors, den Namen der aktiven Kunden (Praxen) und den Produktbezeichnungen an das Sprachmodell bei Amazon Bedrock (EU) gesendet. Das Ergebnis sind strukturierte Vorschläge, die der Benutzer prüft und in einen Auftrag übernimmt. Bilder können Patientendaten und Gesundheitsdaten enthalten.

Eingaben und Ausgaben werden beim Modellanbieter nicht gespeichert; die Verarbeitung erfolgt in den EU-Regionen gemäß Anlage 2, Nr. 4. Eine Nutzung der Daten zum Training von KI-Modellen erfolgt nicht.

Kategorien personenbezogener Daten

Im Rahmen der beschriebenen Verarbeitungsvorgänge können insbesondere folgende Kategorien personenbezogener Daten verarbeitet werden:

- Stammdaten
- Kontaktdaten
- Benutzerkonten
- Patientendaten
- Gesundheitsdaten gemäß Art. 9 DSGVO
- Zahntechnische Auftragsdaten
- Kommunikationsdaten
- KI-Gesprächsverläufe und Aktionsprotokolle (soweit der KI-Assistent genutzt wird)
- Rechnungsdaten
- Material- und Chargendaten
- Dokumente und Dateianhänge
- Protokoll- und Sicherheitsdaten

Kategorien betroffener Personen

Von den beschriebenen Verarbeitungsvorgängen können insbesondere folgende Personengruppen betroffen sein:

- Patienten
- Zahnärzte
- Mitarbeiter von Zahnarztpraxen
- Mitarbeiter des Auftraggebers
- Ansprechpartner des Auftraggebers
- Lieferanten und Geschäftspartner (soweit im Auftragssystem erfasst)

Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zur Erfüllung der zwischen Auftraggeber und Auftragnehmer bestehenden vertraglichen Leistungen. Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers erfolgt nicht.

Insbesondere erfolgt keine Verarbeitung

- zu Werbezwecken,
- zur Profilbildung,
- zum Verkauf personenbezogener Daten,

zum Training von KI-Modellen oder vergleichbaren Systemen,
- zur Erstellung kundenübergreifender personenbezogener Analysen.

Besondere Kategorien personenbezogener Daten

Je nach Nutzung der DentaTool-Plattform verarbeitet der Auftragnehmer besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO, insbesondere Gesundheitsdaten.

Diese Verarbeitung erfolgt ausschließlich auf Weisung des Auftraggebers und zur Erfüllung der vertraglich vereinbarten Leistungen.

Für diese Daten gelten erhöhte technische und organisatorische Schutzmaßnahmen gemäß Anlage 1 dieses Vertrages.

Grundsätze der Datenverarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich nach den folgenden Grundsätzen:

- Verarbeitung ausschließlich auf dokumentierte Weisung des Auftraggebers,
- Datenminimierung,
- Zweckbindung,
- Integrität und Vertraulichkeit,
- Speicherbegrenzung,
- Mandantentrennung,
- Stand der Technik,
- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß Art. 25 DSGVO.