VEREINBARUNG ÜBER DIE DATENVERARBEITUNG IM AUFTRAG NACH ART. 28 DS-GVO

Version 2.0

Zwischen dem Kunden eines Dampsoft-Produktes

(„Verantwortlicher“ nach Art. 4 Nr. 7 DSGVO)

- Auftraggeber –

Und dem Auftragsverarbeiter

DAMPSOFT GmbH
Vogelsang 1
24351 Damp

- Auftragnehmer -

Pionier der Zahnarzt-Software.
Seit 1986.

DAMPSOFT
Die Zahnarzt-Software

Inhaltsverzeichnis

Präambel

Die Vertragsparteien sind sich darüber einig, dass in diesem Vertrag zur Auftragsverarbeitung („AV-Vertrag“) nur datenschutzrechtliche Regelungen zur Auftragsdatenverarbeitung getroffen werden. Gleichwohl gelten bei der Verarbeitung von Patientendaten die strafrechtlichen Bestimmungen, die aus §203 StGB resultieren.

Die Verantwortung für die Wahrung der ärztlichen Schweigepflicht obliegt dem Auftraggeber, da sowohl diese Verantwortung als auch die datenschutzrechtliche Verantwortung nicht vom Auftraggeber an den Auftragnehmer delegiert werden kann.

Der Auftragnehmer sichert dem Auftraggeber zu, dass er bei der Verpflichtung des von ihm eingesetzten Personals und eingesetzten Subunternehmern auf die Vertraulichkeit und zur Geheimhaltung, auf die hohe Schutzwürdigkeit von Patientendaten sowie auf die eventuell aus dem Gesetz gegen den unlauteren Wettbewerb resultierenden strafrechtlichen Folgen einer unbefugten Offenbarung hinweist.

Dieser AV-Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den mit dem Auftragnehmer geschlossenen Nutzungs- und Softwarewartungs- bzw. Dienstleistungsvertrag ergeben. Dieser AV-Vertrag gilt für alle Dampsoft-Produkte und Erweiterungen.

Die beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit einem Nutzungs- und Softwarewartungs- bzw. Dienstleistungsvertrag in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

§ 1 Definition

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DS-GVO, §2 UWG, §2 TMG und § 3 TKG. Soweit die Spezialgesetze selbst Regelungen und Begrifflichkeiten festgelegt haben, gelten diese vor dem BDSG (Subsidiarität).

§ 2 Gegenstand und Dauer

(1) Der Gegenstand des Auftrags ergibt sich aus dem jeweiligen Nutzungs- und Softwarewartungs- bzw. Dienstleistungsvertrag sowie aus Anlage 3.
(2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

§ 3 Art, Umfang und Zweck der Verarbeitung

(1) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem Nutzungs- und Softwarewartungs- bzw. Dienstleistungsvertrag und den dazugehörigen Leistungsbeschreibungen. Hierbei handelt es insbesondere um Störungsbeseitigung (einschließlich Datensicherung), Pflege und Wartung der Produkte. Bei dieser Art der Verarbeitung besteht theoretisch eine Zugriffsmöglichkeit für den Auftragnehmer. Eine beiläufige Kenntnisnahme durch den Auftragnehmer ist – falls nicht vermeidbar – möglich, jedoch nicht gewollt und kann neben Beschäftigtendaten auch Patientendaten betreffen. Konkrete weitere Verarbeitungsarten ergeben sich aus der Anlage 3.
(2) Der Auftragnehmer erfasst die Angaben über die Software sowie zur Nutzung der Software durch den Kunden und seine Mitarbeiter (nachfolgend insgesamt „Nutzungsdaten“) – nicht jedoch Patientendaten - und verarbeitet diese Informationen zum Zwecke der Erbringung von Fehlerbeseitigungs- und anderen Serviceleistungen (einschließlich der Fehlerdiagnose und -behebung sowie Leistungsabsicherung). Zu diesem Zweck wird der Auftragnehmer die Nutzungsdaten anonymisieren und in dieser Form verarbeiten. Dem Auftragnehmer bleibt es vorbehalten, anonymisierte Nutzungsdaten für eigene Zwecke zu verarbeiten. Die Parteien stimmen darin überein, dass dieser Vertrag nicht auf die Verarbeitung von anonymisierten Nutzungsdaten Anwendung findet. Eine Verarbeitung von Nutzungsdaten in nicht anonymisierter Form für eigene Zwecke vom Auftraggeber im Rahmen des datenschutzrechtlich Zulässigen (insbesondere etwa zur Erfüllung von gesetzlichen Pflichten, Verwaltungs- und Abrechnungszwecken, Bereitstellung von Schnittstellen oder Schnittstellendatenbanken) bleibt hiervon unberührt.

§ 4 Technische und 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 Unterstützung bei Betroffenenrechten

(1) 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 DSGVO genannten Pflichten.

(2) Der Auftragnehmer wird insbesondere:

- den Auftraggeber unverzüglich informieren, falls sich eine betroffene Person mit einem Antrag auf Wahrnehmung ihrer Rechte in Bezug auf Auftraggeber-Daten unmittelbar an den Auftragnehmer wenden sollte;
- dem Auftraggeber auf Anfrage alle bei ihm vorhandenen Informationen über die Verarbeitung von Auftraggeber-Daten geben, die der Auftraggeber zur Beantwortung des Antrags einer betroffenen Person benötigt und über die der Auftraggeber nicht selbst verfügt.

§ 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:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Die Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- 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.
- 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 Auftraggeber genehmigt hiermit in allgemeiner Weise die Inanspruchnahme weiterer Auftragsverarbeiter durch den Auftragnehmer. Die gegenwärtig vom Auftragnehmer eingesetzten weiteren Auftragsverarbeiter sind im Anhang genannt.

(3) Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter

informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potenziellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus sachlichem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 28 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

(4) Der Auftragnehmer wird jedem weiteren Auftragsverarbeiter vertraglich dieselben Datenschutzpflichten auferlegen, die in dieser Anlage in Bezug auf den Auftragnehmer festgelegt sind.

(5) Der Auftragnehmer wird vor jeder Beauftragung sowie regelmäßig während der Beauftragung überprüfen, dass die weiteren Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergriffen haben und diese so durchgeführt werden, dass die Verarbeitung der Auftraggeber-Daten gemäß dieser Anlage erfolgt.

§ 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 VDS 3473).

(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, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen, 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) Der Auftragnehmer wird die Auftraggeber-Daten ausschließlich im Auftrag und gemäß den dokumentierten Weisungen des Auftraggebers verarbeiten, sofern der Auftragnehmer nicht gesetzlich dazu verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(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 so lange 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.

(3) 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.

§ 12 Schriftformklausel

Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

§ 13 Salvatorische Klausel

1. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

2. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

§ 14 Anlage(n)

Anlage 1: Nachweis der allgemeinen technischen und organisatorischen Maßnahmen entsprechend Art. 32 DS-GVO.
Anlage 2: Unterauftragsverhältnisse (Subunternehmer)
Anlage 3: Gegenstand und Art der Verarbeitung

Ort / Datum: Damp, 14.07.2023

_____
Unterschrift Auftragnehmer

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a. Zutrittskontrolle
Es existieren folgende Maßnahmen zur Zutrittskontrolle:
- Elektronisches Schließsystem
- Schlüsselregelung
- Verschlossene Serverräume
- Besucherregelung

b. Zugangskontrolle
Es existieren folgende Maßnahmen zur Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte:
- Benutzerprofile
- Rechte zu Benutzerprofilen
- Passwortrichtlinie
- Begrenzung der Anmeldeversuche
- Authentifikation mit Benutzername / Passwort
- Verschlüsselung von Festplatten
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz von Intrusion-Detection-Systemen
- Logische Trennung von Netzwerken
- Einsatz von VPN-Technologie.

c. Datenträgerkontrolle
Es existieren folgende Maßnahmen zur Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern:
- Getrennte Übermittlungswege für verschlüsselte Datensicherungen und dem dazugehörigen Passwort.
- Verschlüsselter up- und download

d. Zugriffskontrolle
Es existieren folgende Maßnahmen zur Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben:
- Umsetzung Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Sichere Aufbewahrung von Datenträgern mit Datensicherungen
- physische Löschung von Datenträgern vor Wiederverwendung
- Einsatz von Aktenvernichtern
- Verschlüsselung von Datenträgern
- Löschen von zur Verfügung gestellten Daten 4 Wochen nach Abschluss der Anfrage.

e. Trennbarkeit
Es existieren folgende Maßnahmen zur Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit):
- Festlegung und Dokumentation von Art und Zweck der jeweiligen Verarbeitung
- Logische Trennung der Daten durch separate Datenbanken oder strukturierte Dateiablage
- Steuerung über ein Berechtigungskonzept

f. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Es existieren folgende Maßnahmen zur Pseudonymisierung von personenbezogenen Daten:
- Beim Erstellen der Datensicherung hat der Auftraggeber die Möglichkeit diese zu pseudonymisieren.

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

g. Weitergabekontrolle
Es existieren folgende Maßnahmen zur Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:
- Weitergabe von Daten in anonymisierter o. pseudonymisierter Form (obliegt dem Auftraggeber bei Datensicherung)
- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- Authentifizierung von Mitarbeiter und Anwender bei Remoteuntertützung
- Protokollierung der Remoteunterstützung durch den Auftragnehmer
- Alle Mitarbeiter sind auf das Datengeheimnis nach § 5 BDSG verpflichtet
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung

h. Transportkontrolle
Es existieren folgende Maßnahmen zur Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:
- Verschlüsselter up- und download
- Handlungsempfehlungen für den Auftraggeber

i. Eingabekontrolle
Es existieren folgende Maßnahmen zur Eingabekontrolle:
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (Bei eingeschalteter Mitarbeiterverwaltung. Verantwortung liegt hier beim Auftraggeber)
- Protokollierung der Remoteunterstützung.

j. Wiederherstellbarkeit
Es existieren folgende Maßnahmen zur Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können:
- Datensicherungskonzept
- Tägliche Backups
- Kontrolle des Sicherungsvorgangs
- Regelmäßige Kontrolle der Backups

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Es existieren folgende Maßnahmen zur Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Berücksichtigung des Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Es existieren folgende Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung:

- Datenschutz-Managementsystem
- Bestellung eines Datenschutzbeauftragten
- Informationssicherheitsmanagementsystem (VDS 3473)
- 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.

Unterauftragnehmer	Anschrift/Land	Leistung	Relevant für Produkt oder Dienstleistung
Telekom Deutschland GmbH	Landgrabenweg 151, 5322 7 Bonn Deutschland	Cloud	Online Terminmanagement / Anamnese@Home / DS4 Cloud
CM.com Germany GmbH	Wiesenhüttenstraße 11 60329 Frankfurt am Main Deutschland	Übermittlung von SMS-Terminerinnerungen	SMS-Cockpit
CellmatiQ GmbH	Poststr. 20 20354 Hamburg Deutschland	Analyse von Röngtenbildern mittels KI	Analyse-Now
solvi GmbH	Am Südhang 28 65510 Hünstetten Deutschland	Cloud BI-Dienst	Controlling-Cockpit
Microsoft Ireland Operations Ltd	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Teams	Fernwartung
EHealth Experts GmbH	Emil-Figge-Straße 85 44227 Dortmund Deutschland	Cloud	e-Health
MEDKONNEKT GmbH	Landsberger Straße 155 80687 München Deutschland	TI-Services	e-connect
Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großpro-jektberatung GmbH	Concorde Business Park F 2320 Schwechat Österreich	TI-Services	e-connect KIM
Lab5 GmbH	Glockenstraße 20 40476 Düsseldorf Deutschland	Einrichtung/Wartung von TI (cloudbasiert)	e-connect
Nostic Solutions AG	Kantonsstrasse 150 8807 Freienbach Schweiz	Analyse von Röntgenbildern mittels KI	Athena KI Addon
TeamViewer GmbH	Jahnstr. 30 73037 Göppingen Deutschland	Fernwartung	Allg. Support und Remote-Schulungen
ITECH GCV (openport.io)	Goethestraat 10 2050 Antwerpen Belgien	Fernwartung	Allg. Support Athena
GoTo Technologies Ireland Unlimited Company	The Reflector 10 Hanover Quay Dublin 2 D02R573 Irland	Remote-Schulungen	Remote-Schulungen
Userlike UG	Probsteigasse 44-46 50670 Köln Deutschland	Chat-Tool	Allg. Anfragen über Website
VisionmaxX GmbH	Figline-Valdarno-Ring 11 64319 Pfungstadt Deutschland	Wartungsleistungen	e-connect
Docebo Dach GmbH	Am Zirkus 2 10117 Berlin Deutschland	E-Learning/Webinare	Allg. Schulungen / Webinare

Produkt/Erweiterung	Art & Zweck der Verarbeitung	Art der personenbezogenen Daten	Kategorien betroffener Personen
Alle Produkte	Störungsbeseitigung (einschließlich Datensicherung), Pflege und Wartung der Produkte	Alle in den Produkten/Erweiterungen befindlichen Daten	Patienten, Beschäftigte
Athena Analyse Now	Übermittlung über Server, Analyse von Röntgenbildern mittels KI	Röntgenbilder	Patienten
Athena Anamnese@Home	Übermittlung von Patientendaten via Dampsoftserver vor Praxisbesuch	Personenstammdaten, Kontaktdaten, Termindaten, Gesundheitsdaten	Patienten
Athena KI	Übermittlung über Server, Analyse von Röntgenbildern mittels KI	Röntgenbilder	Patienten
Controlling Cockpit	Auswertung der Praxisdaten	Aggregierte Patientendaten, Leistungsdaten der Behandler	Patienten, Beschäftigte
e-connect	TI-Konnektor als Cloudlösung	TI-relevante Daten je nach Anwendung, i.d.R. Gesundheitsdaten	Patienten
Online Terminmanagement	Terminplanungstool	Personenstammdaten, Kontaktdaten, Termindaten, Gesundheitsdaten	Patienten, Beschäftigte
SMS-Cockpit	Übermittlung von SMS	Personenstammdaten, Kontaktdaten, Termindaten, Gesundheitsdaten	Patienten, Beschäftigte
DS 4 Cloud	Cloudlösung	Alle in den Produkten/Erweiterungen befindlichen Daten	Patienten, Beschäftigte
KIM	Datenaustausch – Kommunikation im Medizinwesen	TI-relevante Daten je nach Anwendung, i.d.R. Gesundheitsdaten	Patienten, Beschäftigte

DAMPSOFT GmbH
Vogelsang 1 / 24351 Damp

T 04352 9171-16 / F 04352 9171-90
info@dampsoft.de / www.dampsoft.de