medXso UG (haftungsbeschränkt)
Straße der Befreiung 14
06128 Halle (Saale)
Geschäftsführer: Tommy Mentz
Sitz der Gesellschaft: Halle (Saale)

Web: medxso.de
Mail: info@medxso.de
Telefon: 0345 68 53 62 14
Mobil: 0176 62 90 20 61
Registergericht: Amtsgericht Stendal HRB: 37714

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen dem/der

.....

.....

– Verantwortlicher – nachstehend „Auftraggeber“ genannt

und der

medXso UG (haftungsbeschränkt), Geschäftsführer Tommy Mentz, Straße der Befreiung 14, 06128 Halle (Saale)

– Auftragsverarbeiter – nachstehend „Auftragnehmer“ genannt

1. Gegenstand und Dauer des Auftrags

(1) **Gegenstand:** Der Gegenstand des Auftrags ergibt sich aus dem zwischen den Parteien geschlossenen Softwarepflegevertrag (im Folgenden „Leistungsvereinbarung“), auf den hier verwiesen wird. Der Auftragnehmer erbringt Leistungen im Rahmen des Supports, der Fernwartung und des Betriebs der vertragsgegenständlichen Software, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(2) **Dauer:** Die Laufzeit dieses Vertrages entspricht der Laufzeit der Leistungsvereinbarung. Eine Beendigung der Leistungsvereinbarung führt automatisch zur Beendigung dieses Vertrages.

2. Konkretisierung des Auftragsinhalts

(1) **Art und Zweck der Verarbeitung:** Der Auftragnehmer erbringt im Rahmen der Leistungsvereinbarung folgende Tätigkeiten, die eine Verarbeitung personenbezogener Daten umfassen können:

- Unterstützung und Hilfeleistung bei der Installation der vertragsgegenständlichen Anwendungssoftware
- Installation von Software auf Weisung und Wunsch des Auftraggebers
- Unterstützung bei Bedienungsproblemen mit der Anwendungssoftware (Hotline, Support)
- Fehleranalyse und Fehlerbehebung im Rahmen der Fernwartung (Remote Support)

Die Verarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) **Art der Daten:** Gegenstand der Verarbeitung im Rahmen des Supports/der Fernwartung sind folgende Datenkategorien:

- Personenstammdaten (z. B. Name, Vorname, Titel)

- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Vertragsstammdaten und Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- **Patientenstammdaten sowie Gesundheitsdaten (besondere Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO)**
- Software-Lizenzdaten und Versionsdaten
- Technische Hard- und Softwareinformationen des Ziel-Systems

(3) **Kategorien betroffener Personen:** Die von der Verarbeitung betroffenen Personen umfassen:

- Kunden und Interessenten des Auftraggebers
- Beschäftigte und Lieferanten des Auftraggebers
- **Patienten des Auftraggebers**

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen (TOM) vor Beginn der Verarbeitung zu dokumentieren und umzusetzen. Die konkreten Maßnahmen sind der **Anlage 1** zu diesem Vertrag zu entnehmen und bilden einen wesentlichen Bestandteil dieser Vereinbarung.

(2) Der Auftragnehmer gewährleistet die Datensicherheit gemäß Art. 28 Abs. 3 lit. c, Art. 32 DS-GVO. Es handelt sich um Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, Integrität, 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 Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO berücksichtigt.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Dem Auftragnehmer ist es gestattet, alternative adäquate Maßnahmen umzusetzen, sofern das vereinbarte Sicherheitsniveau dadurch nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber auf Verlangen anzuzeigen.

4. Berichtigung, Einschränkung und Löschung von Daten

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

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu den Regelungen dieses Vertrages die gesetzlichen Pflichten gemäß Art. 28 bis 33 DS-GVO einzuhalten; er gewährleistet insbesondere:

- **a) Vertraulichkeit und Berufsgeheimnis:** Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die schriftlich auf die Vertraulichkeit (Art. 28 Abs. 3 S. 2 lit. b,

Art. 29, Art. 32 Abs. 4 DS-GVO) sowie – **aufgrund des Umgangs mit Patientendaten – explizit auf die Wahrung des Berufsgeheimnisses gemäß § 203 Strafgesetzbuch (StGB)** verpflichtet und mit den Bestimmungen zum Datenschutz vertraut gemacht wurden.

- **b) Technische Maßnahmen:** Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Anlage 1.
- **c) Aufsichtsbehörden:** Die Zusammenarbeit mit den Datenschutz-Aufsichtsbehörden auf Anfrage.
- **d) Unverzügliche Information:** Die sofortige Information des Auftraggebers über Kontrollhandlungen oder Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen (einschließlich Ermittlungsverfahren).
- **e) Unterstützung des Auftraggebers:** Den Auftraggeber nach besten Kräften zu unterstützen, falls dieser behördlichen Kontrollen, Haftungsansprüchen Betroffener oder sonstigen Verfahren im Zusammenhang mit dieser Auftragsverarbeitung ausgesetzt ist.
- **f) Eigenkontrolle:** Die regelmäßige Überprüfung der internen Prozesse und der TOM, um die Rechtskonformität der Verarbeitung dauerhaft sicherzustellen.

6. Unterauftragsverhältnisse (Subunternehmer)

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Unterauftragsverarbeiter einzusetzen. Zum Zeitpunkt des Vertragsschlusses sind die in der folgenden Tabelle aufgeführten Subunternehmer für Teilleistungen involviert. Der Auftraggeber stimmt deren Einsatz hiermit ausdrücklich zu:

Name und Anschrift des Subunternehmers	**Beschreibung der Teilleistungen**
1&1 IONOS SE Elgendorfer Str. 57, 56410 Montabaur	Bereitstellung von Infrastruktur-/Telekommunikationsleistungen für die Online-Terminvergabe, TimeControl und das E-Mail-Modul von TimeControl.
Alfahosting GmbH Ankerstraße 3b, 06108 Halle (Saale)	Hosting und Cloud-Infrastruktur für die Online-Terminvergabe-App.
Lox24 GmbH Seestraße 109, 13353 Berlin	SMS-Gateway-Dienstleister für den automatisierten Versand von Terminerinnerungen per SMS.
GTX GmbH Erftstraße 19a, 50672 Köln	SMS-Gateway-Dienstleister für den automatisierten Versand von Terminerinnerungen per SMS.

Name und Anschrift des Subunternehmers	**Beschreibung der Teilleistungen**
pcvisit Software AG Manfred-von-Ardenne-Ring 20, 01099 Dresden	Bereitstellung der Fernwartungssoftware für Remote Support und gesicherten Fernzugriff.
TeamViewer Germany GmbH Bahnhofsplatz 2, 73033 Göppingen	Bereitstellung der Fernwartungssoftware für Remote Support und gesicherten Fernzugriff.

(2) Beabsichtigt der Auftragnehmer, weitere Subunternehmer hinzuzuziehen oder bestehende zu ersetzen, wird er den Auftraggeber darüber rechtzeitig im Voraus (mindestens zwei Wochen vorab) in Textform informieren. Der Auftraggeber hat das Recht, gegen die Änderung Einspruch zu erheben. Erfolgt kein Einspruch innerhalb von 14 Tagen nach Zugang der Mitteilung, gilt die Änderung als genehmigt. Ein Einspruch darf nur aus wichtigen, nachweisbaren datenschutzrechtlichen Gründen erhoben werden.

(3) Der Auftragnehmer ist verpflichtet, mit den Subunternehmern Vereinbarungen zu treffen, die den datenschutzrechtlichen Anforderungen dieses Vertrages entsprechen (Art. 28 Abs. 4 DS-GVO).

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende, unabhängige Prüfer (die nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen) durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung im Geschäftsbetrieb des Auftragnehmers zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass der Nachweis der Einhaltung der TOM auch wie folgt erbracht werden kann:

- Durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. externe Datenschutzauditoren, IT-Sicherheitsabteilungen, Wirtschaftsprüfer).
- Durch eine anerkannte Zertifizierung im Bereich IT-Sicherheit oder Datenschutz (z. B. ISO 27001 oder BSI-IT-Grundschutz).

(3) Für die Ermöglichung und Begleitung von Vor-Ort-Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen, aufwandsbasierten Vergütungsanspruch geltend machen, es sei denn, die Kontrolle erfolgt aufgrund eines nachgewiesenen Pflichtverstoßes des Auftragnehmers.

8. Mitteilung bei Verstößen und Unterstützungspflichten

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten (Datensicherheit, Meldepflichten bei Datenpannen, Datenschutz-

Folgenabschätzungen und vorherige Konsultationen mit Aufsichtsbehörden). Hierzu gehört insbesondere:

- a) Die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten (Datenpannen) unverzüglich nach Bekanntwerden an den Auftraggeber in Textform zu melden.
- b) Dem Auftraggeber sämtliche zur Meldung der Datenpanne erforderlichen Informationen unverzüglich bereitzustellen.
- c) Die Unterstützung des Auftraggebers bei eventuell anfallenden Datenschutz-Folgenabschätzungen (DSFA) im Zusammenhang mit der genutzten Software.

Für Unterstützungsleistungen, die nicht auf ein Fehlverhalten oder einen Pflichtverstoß des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers. Mündliche Weisungen hat der Auftraggeber unverzüglich mindestens in Textform (z. B. per E-Mail) zu bestätigen.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen die DS-GVO oder andere Datenschutzvorschriften der Union oder der Mitgliedstaaten. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt, angepasst oder freigegeben wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige temporäre Zwischenspeicherungen oder Sicherheitskopien (Backups), soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung zwingend erforderlich sind.

(2) Nach Abschluss der vertraglichen Arbeiten oder nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Datenbestände, Unterlagen und Verarbeitungsresultate dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzkonform und unwiederbringlich zu löschen bzw. zu vernichten. Ein entsprechendes Löschprotokoll ist dem Auftraggeber auf Verlangen vorzulegen.

(3) Gesetzliche Aufbewahrungspflichten des Auftragnehmers nach unionsrechtlichen oder nationalen Vorschriften bleiben hiervon unberührt.

11. Informationspflichten, Textform

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, Insolvenzverfahren oder sonstige Maßnahmen Dritter gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird die beteiligten Dritten unverzüglich darüber aufklären, dass die Datenhoheit ausschließlich beim Auftraggeber liegt.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

12. Haftung

Für den Ersatz von Schäden, die eine Partei durch eine unzulässige oder unrichtige Datenverarbeitung im Rahmen dieses Auftragsverhältnisses erleidet, gilt die Haftungsregelung des Art. 82 DS-GVO. Im Innenverhältnis der Parteien richtet sich die Haftung nach den Regelungen des Hauptvertrages (Leistungsvereinbarung), sofern nicht zwingende gesetzliche Vorgaben der DS-GVO entgegenstehen.

13. Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der Vereinbarung im Übrigen unberührt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame Regelung zu ersetzen, die dem wirtschaftlichen und datenschutzrechtlichen Zweck der unwirksamen Regelung am nächsten kommt.

	Halle (Saale), den 01.08.2026
.....	.....
(Datum, Ort)	*(Datum, Ort)*
.....	Mentz .....
Auftraggeber (Praxis / Einrichtung)	**Auftragnehmer (medXso UG)**

Anlage 1 – Technisch-organisatorische Maßnahmen (TOM)

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

- **Zutrittskontrolle:** Verwehrung des Zutritts zu Verarbeitungsanlagen und Serverräumen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.
    - *Maßnahmen:* Organisatorisch festgelegte Zutrittsberechtigungen für Beschäftigte, Schließsysteme, Schlüsselregelung und Vergabe nach Dokumentation, Überwachung von Besuchern.
- **Zugangskontrolle:** Verwehrung des Zugangs zu Datenverarbeitungssystemen für Unbefugte.
    - *Maßnahmen:* Authentifizierung mittels Benutzername und sicherem Kennwort (Passwort-Richtlinien), automatisierte Sperrung von Client-Systemen bei Inaktivität, Einsatz von verschlüsselten VPN-Verbindungen bei Fernwartungszugriffen.
- **Zugriffskontrolle:** Gewährleistung, dass Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (kein unbefugtes Lesen, Kopieren, Verändern).
    - *Maßnahmen:* Rollenbasiertes Berechtigungskonzept, Verbot von Sammel-Accounts (jeder Techniker nutzt ein personalisiertes Konto), lückenlose Protokollierung von System- und Fernwartungszugriffen.
- **Trennungsgebot:** Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
    - *Maßnahmen:* Logische Mandatstrennung in den Systemen und Datenbanken des Auftragnehmers; strikte Trennung von Test- und Produktivdaten.

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

- **Eingabekontrolle:** Gewährleistung, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
    - *Maßnahmen:* Protokollierung von Administrations- und Supportvorgängen inklusive Zeiterfassung und Benutzer-ID.
- **Übertragungskontrolle:** Gewährleistung, dass bei der Übertragung personenbezogener Daten die Vertraulichkeit und Integrität geschützt sind.
    - *Maßnahmen:* Durchgehende Transportverschlüsselung (z. B. TLS/HTTPS, SSH, AES-256-verschlüsselte Fernwartungs-Sessions über pcvisit/TeamViewer).

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

- **Verfügbarkeitskontrolle:** Gewährleistung, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
    - *Maßnahmen:* Backup-Strategie mit regelmäßigen Backups, getrennte und gesicherte Aufbewahrung der Datensicherungen, Einsatz moderner, zentral verwalteter Anti-Viren-Software und aktiver Firewalls auf allen Systemen.
- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO):** Gewährleistung, dass installierte Systeme im Störungsfall zeitnah wiederhergestellt werden können.
    - *Maßnahmen:* Ausfallsichere Speichersysteme (z. B. RAID-Verbund) bei den Hosting-Partnern, regelmäßige Tests der Rücksicherungsprozesse (Restore-Tests).

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

- **Datenschutz-Management & Auftragskontrolle:** Gewährleistung einer datenschutzkonformen Abwicklung und Auswertung.
    - *Maßnahmen:* Verpflichtung des Technikerpersonals auf den Datenschutz und § 203 StGB, regelmäßige interne Audits und Schulungen der Mitarbeiter, Vorhalten eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DS-GVO). Datenschutzfreundliche Voreinstellungen (Privacy by Design / Privacy by Default) finden bei der Softwareentwicklung Berücksichtigung.