AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

nach Art. 28 DSGVO

Stand: 22.01.2026

zwischen

Auftraggeber (Kunde)
Daten aus dem Registrierungsprozess

und

Auftragnehmerin / Auftragsverarbeiterin
Digital Health Data Labs GmbH

Kaiser-Franz-Josef Straße 4
6020 Innsbruck
Österreich

FN 635970 a

vertreten durch: Mattias Köck, Geschäftsführer

gemeinsam „***Parteien***“.

Präambel.

Dieser Auftragsverarbeitungsvertrag (AVV) konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Zusammenhang mit der Nutzung der Softwarelösung GOÄ-Direkt.de. Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO.

1. Gegenstand, Umfang und Zweck der Verarbeitung

1.1. Die Auftragnehmerin verarbeitet personenbezogene Daten im Auftrag des Auftraggebers zur Erbringung der Leistungen im Zusammenhang mit der Nutzung der Web-Applikation „GOÄ-Direkt.de“ (SaaS-Betrieb inkl. Wartung und Support) sowie zur Bereitstellung der abrechnungsbezogenen Funktionen der Anwendung.

1.2. Da die Auftragnehmerin in Erfüllung seiner Aufgaben, Daten im Auftrag, nach Weisung und im Interesse des Auftraggebers verarbeitet bzw. ein Zugriff auf personenbezogene Daten bei der Auftragserfüllung nicht ausgeschlossen werden kann, erfolgt die Dienstleistung als Auftragsverarbeitung nach den für den Auftraggeber einschlägigen Datenschutzgesetzen.

1.3. Art der Verarbeitung umfasst, soweit jeweils zur Vertragserfüllung erforderlich, insbesondere das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung (ausschließlich auf Weisung des Auftraggebers), Abgleichen oder Verknüpfen, Einschränken, Löschen und Vernichten.

1.4. Zweck der Verarbeitung ist die technische Bereitstellung und Durchführung der vom Auftraggeber veranlassten Prozesse zur Privatliquidation nach GOÄ, einschließlich der Erstellung, Ausgabe und des Versands (zB per E-Mail, Post oder über System-Schnittstellen) von Rechnungen, Zahlungserinnerungen/Mahnungen und sonstiger abrechnungsbezogener Schreiben nach Weisung des Auftraggebers, der Systemadministration, Nutzer- und Berechtigungsverwaltung, Protokollierung, IT-Sicherheitsmaßnahmen sowie der Fehleranalyse und Weiterentwicklung im Rahmen von Wartung/Support (jeweils ohne eigenständige Zwecke der Auftragnehmerin).

2. Datenarten und betroffene Personenkategorien

2.1. Datenarten: Patientenstammdaten; Gesundheitsdaten im Sinne von Art 9 DSGVO; Kontakt- und Kommunikationsdaten; Abrechnungs-, Leistungs- und Zahlungsdaten; Dokumenten-/Korrespondenzdaten (zB Rechnungen, Zahlungserinnerungen/Mahnungen, sonstige abrechnungsbezogene Schreiben); Nutzer-, Zugriffs- und Protokolldaten (zB Audit-Logs).

2.2. Betroffene Personen: Patientinnen und Patienten des Auftraggebers; Rechnungsempfänger und Rechnungszahlende (einschließlich abweichender Rechnungsempfänger/Zahler); Beschäftigte und sonstige Beauftragte des Auftraggebers, die das System nutzen.

3. Dauer

3.1. Dieser Vertrag zur Auftragsverarbeitung (AVV) tritt mit Abschluss des zugrundeliegenden Dienstleistungsvertrages und der elektronischen Zustimmung im Bestellprozess (Checkbox) in Kraft und ist vom Bestand des zugrundeliegenden Dienstleistungsvertrages abhängig. Endet der Dienstleistungsvertrag, so endet auch dieser AVV, ohne dass es einer gesonderten Kündigung bedarf.

3.2. Nach Beendigung der Auftragsverarbeitung hat die Auftragnehmerin, sämtliche personenbezogenen Daten (einschließlich etwaiger Kopien) an den Auftraggeber herauszugeben oder zu löschen. Die Löschung hat unverzüglich, spätestens innerhalb von 14 Tagen nach entsprechender Weisung des Auftraggebers zu erfolgen, sofern der Löschung keine gesetzlichen Aufbewahrungs- oder Nachweispflichten entgegenstehen; in diesem Fall darf die Auftragnehmerin die betreffenden Daten nur zu diesen Zwecken speichern und hat sie nach Wegfall des Grundes unverzüglich zu löschen. Die Auftragnehmerin bestätigt dem Auftraggeber die Löschung auf Verlangen in geeigneter Form.

3.3. Die Auftragnehmerin ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über Personen, Geschäftsgeheimnisse und Datensicherheitsmaßnahmen auch nach Beendigung des Vertrages vertraulich zu behandeln.

4. Weisungsrecht

4.1. Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisungen des Auftraggebers. Weisungen erfolgen mindestens in Textform (E-Mail ausreichend) und sind auf die im Dienstleistungsvertrag vereinbarten Leistungen sowie die von der Anwendung vorgesehenen Konfigurations- und Nutzungsmöglichkeiten beschränkt.

4.2. Als Weisungen gelten insbesondere (i) die Nutzung und Konfiguration der Anwendung durch den Auftraggeber bzw seiner Nutzer (zB Anlage/Änderung/Löschung von Nutzern und Rollen, Vorlagen, Versandarten und Empfängern), (ii) Support- und Betriebsanfragen (zB Datenexporte, Berichtigungen, Sperren/Entsperren, Wiederherstellungen im Rahmen der vereinbarten Leistungen) sowie (iii) Weisungen zur Herausgabe oder Löschung nach Vertragsende.

4.3. Weisungen, die über den Leistungsumfang oder die technischen Möglichkeiten der Anwendung hinausgehen oder für die Auftragnehmerin mit unverhältnismäßigem Aufwand verbunden sind, bedürfen einer gesonderten Vereinbarung. Die Auftragnehmerin wird den Auftraggeber hierüber unverzüglich informieren.

4.4. Die Auftragnehmerin informiert den Auftraggeber unverzüglich, wenn sie der Ansicht ist, dass eine Weisung gegen anwendbare Datenschutzvorschriften verstößt. In diesem Fall ist die Auftragnehmerin berechtigt, die Ausführung der Weisung bis zur Bestätigung, Änderung oder Aufhebung der Weisung durch den Auftraggeber auszusetzen, soweit dies erforderlich ist.

5. Pflichten des Auftragnehmers

5.1. Die Auftragnehmerin bestätigt, dass ihr die anwendbaren datenschutzrechtlichen Vorschriften bekannt sind. Sie gestaltet die innerbetriebliche Organisation in ihrem Verantwortungsbereich so, dass die Anforderungen der DSGVO sowie, soweit einschlägig, der Berufsgeheimnisschutz des Auftraggebers gewahrt werden.

5.2. Die Auftragnehmerin stellt sicher, dass die bei ihr mit der Verarbeitung befassten Personen auf Vertraulichkeit verpflichtet und in den für sie maßgeblichen Datenschutzanforderungen geschult sind. Die Verpflichtung gilt auch nach Beendigung des Beschäftigungsverhältnisses fort. Die Auftragnehmerin weist dem Auftraggeber diese Verpflichtungen auf Verlangen in geeigneter Form nach.

5.3. Die Auftragnehmerin stellt eine angemessene Mandantentrennung sicher, sodass personenbezogene Daten des Auftraggebers nicht unbefugt mit Daten anderer Kunden vermischt oder Dritten zugänglich werden. Dies erfolgt insbesondere durch Zugriffskontrollen, Berechtigungskonzepte und technische/organisatorische Maßnahmen zur logischen Trennung in der Anwendung und den zugrunde liegenden Systemen.

5.4. Soweit gesetzlich erforderlich, benennt die Auftragnehmerin eine/n Datenschutzbeauftragte/n. Die Kontaktdaten werden dem Auftraggeber zur direkten Kontaktaufnahme mitgeteilt. Änderungen teilt die Auftragnehmerin unverzüglich mit.

5.5. Die Auftragnehmerin verarbeitet personenbezogene Daten grundsätzlich im Europäischen Wirtschaftsraum. Eine Verarbeitung in einem Drittland oder eine Drittlandübermittlung erfolgt nur, wenn die Voraussetzungen der Art 44 ff DSGVO eingehalten sind (insbesondere geeignete Garantien wie Standardvertragsklauseln) und nach Maßgabe der Regelungen dieses AVV zu Unterauftragsverarbeitern bzw Übermittlungen.

5.6. Die Auftragnehmerin unterstützt den Auftraggeber im Rahmen der gesetzlichen Pflichten bei der Erfüllung von Betroffenenrechten sowie sonstigen Pflichten nach Kapitel III und IV DSGVO, soweit die Unterstützung im Zusammenhang mit der Auftragsverarbeitung steht. Erhält die Auftragnehmerin ein Ersuchen eines Betroffenen, leitet sie dieses unverzüglich an den Auftraggeber weiter. Auskünfte gegenüber Betroffenen oder Dritten erteilt die Auftragnehmerin nur auf Weisung des Auftraggebers, soweit gesetzlich zulässig.

5.7. Die Auftragnehmerin unterstützt den Auftraggeber bei Datenschutz-Folgeabschätzungen (Art 35 DSGVO) und bei einer etwa erforderlichen Konsultation der Aufsichtsbehörde (Art 36 DSGVO), soweit die Verarbeitung im Rahmen dieses AVV betroffen ist.

5.8. Die Auftragnehmerin meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden und stellt die zur Erfüllung der Melde- und Benachrichtigungspflichten nach Art 33 und 34 DSGVO erforderlichen Informationen zur Verfügung.

5.9. Der Auftragnehmerin ist bekannt, dass der Auftraggeber Berufsgeheimnisträger sein kann und Verstöße gegen die Verschwiegenheit strafbewehrt sein können. Die Auftragnehmerin verpflichtet sich, alle im Rahmen dieses AVV erlangten Informationen entsprechend vertraulich zu behandeln.

6. Technische und organisatorische Maßnahmen (TOMs)

6.1. Die Auftragnehmerin verpflichtet sich, für die zu verarbeitenden Daten angemessene und dem Stand der Technik entsprechende technische und organisatorische Sicherheitsmaßnahmen (TOMs) nach den für den Auftraggeber einschlägigen Datenschutzgesetzen, insbesondere gemäß Art. 32 DSGVO, zu treffen.

6.2. Die TOM sind in Anlage 1 beschrieben. Anpassungen sind zulässig, sofern das Schutzniveau nicht unterschritten wird.

6.3. Die Auftragnehmerin führt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art 30 Abs 2 DSGVO für die im Rahmen dieses AVV erfolgenden Verarbeitungen und stellt es der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung.

7. Unterauftragsverarbeiter

7.1. Der Auftraggeber erteilt der Auftragnehmerin die allgemeine Genehmigung, Unterauftragsverarbeiter im Sinne von Art 28 Abs 2 DSGVO zur Erbringung der Leistungen einzusetzen.

7.2. Die Auftragnehmerin stellt sicher, dass sie mit Unterauftragsverarbeitern Vereinbarungen abschließt, die mindestens gleichwertige Datenschutzpflichten wie dieser AVV enthalten. Die Auftragnehmerin bleibt gegenüber dem Auftraggeber für die Erfüllung der Pflichten der Unterauftragsverarbeiter verantwortlich.

7.3. Die Auftragnehmerin teilt dem Auftraggeber die jeweils aktuellen Unterauftragsverarbeiter auf Anfrage in Textform mit.

8. Meldung von Datenschutzverletzungen und Sicherheitsvorfällen

8.1. Die Auftragnehmerin informiert den Auftraggeber unverzüglich, nachdem sie Kenntnis erlangt hat, über (i) eine Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den im Auftrag verarbeiteten Daten sowie (ii) Sicherheitsvorfälle oder Störungen, die voraussichtlich zu einer solchen Verletzung führen können. Gleiches gilt, wenn die Auftragnehmerin wesentliche Schwachstellen feststellt, aufgrund derer die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten gefährdet sein kann.

8.2. Die Mitteilung erfolgt in Textform (E-Mail ausreichend) und enthält, soweit verfügbar, mindestens:
a) eine Beschreibung der Art der Verletzung (einschließlich Kategorien betroffener Daten und betroffener Personen) sowie – soweit möglich – Angaben zur ungefähren Zahl der betroffenen Personen und Datensätze
b) Name und Kontaktdaten einer Anlaufstelle bei der Auftragnehmerin (zB Datenschutzkontakt)
c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung
d) eine Beschreibung der von der Auftragnehmerin ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Minderung möglicher nachteiliger Auswirkungen.

8.3. Die Auftragnehmerin stellt dem Auftraggeber auf Anfrage weitere Informationen zur Verfügung, soweit dies zur Erfüllung der Pflichten des Auftraggebers nach Art 33 und 34 DSGVO erforderlich ist.

9. Kontrollrechte des Auftraggebers

9.1. Der Auftraggeber ist berechtigt, die Einhaltung dieses AVV und der anwendbaren Datenschutzvorschriften durch die Auftragnehmerin im erforderlichen Umfang zu überprüfen. Die Kontrolle erfolgt grundsätzlich durch die Einholung von Auskünften und die Zurverfügungstellung geeigneter Nachweise (insbesondere Beschreibung der technischen und organisatorischen Maßnahmen, Sicherheitskonzepte, Protokolle über durchgeführte Kontrollen, Zertifizierungen oder Prüfberichte, soweit vorhanden).

9.2. Soweit eine Kontrolle über den in Abs 1 vorgesehenen Umfang hinausgeht oder besondere Aufwände verursacht, trägt der Auftraggeber die dadurch entstehenden angemessenen Kosten der Auftragnehmerin.

10. Haftung

10.1. Auf Art. 82 EU-DSGVO wird hingewiesen.

11. Schlussbestimmungen

11.1. Die Vertragsparteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Vertragspartei vertraulich zu behandeln. Geschäftsgeheimnisse sind alle auf ein Unternehmen bezogene

Tatsachen, Umstände und Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Geheimnisträger ein berechtigtes Interesse hat. Datensicherheitsmaßnahmen sind alle technischen und organisatorischen Sicherheitsmaßnahmen, die eine Partei nach den für den Auftraggeber einschlägigen Datenschutzgesetzen getroffen hat. Diese Geheimhaltungspflicht besteht nach Beendigung dieses Vertrags fort.

11.2. Für Vertragsänderungen und Nebenabreden ist die Textform erforderlich.

11.3. Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

11.4. Maßgeblich ist die im Bestellprozess verlinkte Fassung dieses AVV (Version/Stand). Die Auftragnehmerin protokolliert Zeitpunkt und Version der Zustimmung.

11.5. Dieser AVV wird elektronisch geschlossen; eine handschriftliche Unterschrift ist nicht erforderlich.

Anlage 1 – TOM (Kurzbeschreibung)

- Zutrittskontrolle: Zugang zu Betriebsstätten/Serverstandorten nur für berechtigte Personen.
- Zugangskontrolle: individuelle Benutzerkonten, starke Passwortrichtlinie, MFA für administrative Zugänge, Session-Timeout, Serverzugriff über SSH mittels Schlüssel-Authentifizierung (keine Passwort-Logins)
- Zugriffskontrolle: Rollen- und Rechtekonzept (Least Privilege), Protokollierung administrativer Zugriffe.
- Weitergabekontrolle: verschlüsselte Datenübertragung (HTTPS)
- Speicherung: Verschlüsselung at rest; Schlüsselmanagement nach Stand der Technik.
- Eingabekontrolle: Audit-Logs für wesentliche Ereignisse (Login, Änderungen, Dokumentenerzeugung).
- Verfügbarkeit: Backups, Monitoring, Wiederherstellungsprozesse
- Trennung: Mandantentrennung je Praxis; getrennte Berechtigungen und Datenzugriffe.
- Incident Response: definierter Prozess inkl. Eskalation und Benachrichtigung.