medo.check®

Health and Fitness
Software Solutions

Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO – medo.core

(Datum ..... / zum Lizenzvertrag .....)

Auftragnehmer

Heidötting & Winter GbR, Alfred-Herrhausen-Str. 44, 58455 Witten

Umsatzsteuer-Identifikationsnummer: DE253306487

Gläubiger-Identifikationsnummer im SEPA-Lastschriftverfahren: DE31ZZZ00000030160

vertreten durch: Herrn Tino Heidötting

– nachfolgend Auftragnehmer genannt –

Auftraggeber

Firma / Name:

vertreten durch:

– nachfolgend Auftraggeber genannt –

§ 1 Gegenstand des Auftrags

Der Gegenstand des Auftrags ergibt sich aus dem Lizenzvertrag ....., auf den hier verwiesen wird (im Folgenden Lizenzvertrag). Der Auftragnehmer stellt dem Auftraggeber die browserbasierte Plattform medo.core® als Software-as-a-Service (SaaS) bereit. Im Rahmen der Leistungserbringung verarbeitet der Auftragnehmer personenbezogene Daten, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend Auftraggeber-Daten). Eingeschlossen sind die Datenflüsse aus und an die medo.coach-App sowie – bei aktiviertem Hybrid-Modus – aus medo.check® (Windows). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Bezug auf den Umgang des Auftragnehmers mit den Auftraggeber-Daten zur Durchführung des Lizenzvertrags.

Hinweis Hybrid-Modus: Koppelt der Auftraggeber medo.check® (Windows) im Hybrid-Modus an medo.core, verarbeitet der Auftragnehmer auch die über die medo.core-API übermittelten Stammdaten und Dokumente aus medo.check. Für die medo.check-Cloud-Datenhaltung selbst gilt separat die Auftragsverarbeitungsvereinbarung medo.check Cloud (ADV 1).

§ 2 Dauer des Auftrages

2.1 Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Lizenzvertrages. Eine Kündigung des Lizenzvertrages bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

2.2 Ergänzend zu §2.1 steht dem Auftraggeber ein jederzeitiges außerordentliches Kündigungsrecht bezüglich dieses Vertrags sowie des Lizenzvertrages aus wichtigem Grund zu. Ein wichtiger Grund liegt für den Auftraggeber insbesondere vor, wenn

- der Auftragnehmer gegen eine wesentliche Pflicht aus diesem Vertrag verstößt,
- der Auftragnehmer die Auftraggeber-Daten nicht wie in §3.1 beschrieben verwendet,
- der Auftragnehmer eine Weisung des Auftraggebers nach §3 dieses Vertrags nicht oder nur teilweise ausführt,
- der Auftragnehmer die Ausübung der Kontrollrechte des Auftraggebers nach §10 dieses Vertrags verweigert oder nicht nur unerheblich behindert oder
- der Auftragnehmer Unterauftragnehmer entgegen §11 ohne vorherige schriftliche Zustimmung des Auftraggebers einschaltet.

2.3 Der Lizenzvertrag darf im Falle einer Beendigung dieses Vertrags nur fortgeführt werden, wenn ausgeschlossen ist, dass der Auftragnehmer Auftraggeber-Daten verwendet oder darauf zugreift.

§ 3 Konkretisierung des Auftragsinhalts

3.1 Umfang, Art und Zweck der Datenverarbeitung

Umfang, Art und Zweck der Datenverarbeitung durch den Auftragnehmer für den Auftraggeber beziehen sich auf den Betrieb der medo.core-Plattform einschließlich der angebundenen medo.coach-App, des Online-Buchungssystems und – bei aktiviertem Hybrid-Modus – der Schnittstelle zu medo.check® (Windows). Zweck ist die Bereitstellung einer browserbasierten Managementplattform für den Auftraggeber zur Verwaltung von Mitgliedern, Terminen, Training, Kommunikation, Zugangskontrolle und Abrechnung im Fitness- und Gesundheitsbereich. Die nachfolgende Tabelle gibt einen Überblick über die verarbeiteten Datenkategorien:

Datenkategorie	Art. 9?	Herkunft / Datenfluss
Mitgliederstammdaten (Name, Adresse, Kontakt, Geburtsdatum)	Nein	Auftraggeber → medo.core
Account- und Zugangsdaten (Login, Scopes, Rollen)	Nein	medo.core (identification-Service, IONOS)
Termine und Buchungsdaten (inkl. Kontingente/Zehnerkarten)	Nein	Auftraggeber / medo.coach → medo.core
Studioauslastungsdaten	Nein	medo.core → medo.coach
Zutritts- und Anwesenheitsprotokolle	Nein	medo.core (access-Service)
Chat-Nachrichten (Trainer ↔ medo.coach-Nutzer)	Nein	bidirektional medo.core ↔ medo.coach
Trainingspläne	Ja	Auftraggeber → medo.core → medo.coach
Gesundheits- und Vitaldaten (Körperanalyse, Check-Up, Diagnostik)	Ja	Auftraggeber → medo.core
Anamnese-Auswertungen und medizinische Dokumente	Ja	Auftraggeber → medo.core → medo.coach
Manuell erfasste Gesundheitsdaten aus medo.coach (Gewicht, Puls, Temperatur u. a.)	Ja	medo.coach → medo.core
Apple HealthKit- / Health Connect-Daten (Vitalparameter, Herzfrequenz u. a.)	Ja	medo.coach → medo.core [geplant]
Trainingsdaten aus medo.coach (absolvierte Sessions)	Ja	medo.coach → medo.core
Rechnungs- und Vertragsdaten	Nein	medo.core (payment-Service)
IBAN / SEPA-Mandate (für SEPA-Sammler-Generierung)	Nein	Auftraggeber → medo.core
Zahlungsstatusinformationen (Stripe-Webhooks: Status, Beträge, Referenz-IDs)	Nein	Stripe → medo.core

Datenkategorie	Art. 9?	Herkunft / Datenfluss
Dokumente (Verträge, sonstige Uploads)	Nein / ggf. Ja	Auftraggeber / medo.coach ↔ medo.core
E-Mail-Adressen (medo.coach-Einladungsprozess)	Nein	Auftraggeber → medo.core → SendGrid
Verbindungs- und Sessiondaten (IP-Adresse, Browser-Informationen)	Nein	Endnutzer-Browser → Vercel / medo.core
Hardware- und Betriebssysteminformationen (Fehleranalyse)	Nein	medo.core / medo.coach → Sentry
Daten im Hybrid-Modus: aus medo.check übermittelte Stammdaten und Dokumente	teils Ja	medo.check → medo.core API

Jede davon abweichende oder darüber hinausgehende Erhebung, Verarbeitung oder Nutzung von Auftraggeber-Daten ist dem Auftragnehmer untersagt, insbesondere eine Verwendung der Auftraggeber-Daten zu eigenen Zwecken.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO): Gesundheits-, Vital-, Trainings- und Anamnese-Daten, medizinische Auswertungen, manuell erfasste Vitalparameter sowie Apple HealthKit- und Health Connect-Daten stellen besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO dar. Ihre Verarbeitung erfolgt auf Grundlage der ausdrücklichen Einwilligung der betroffenen Personen gemäß Art. 9 Abs. 2 lit. a DSGVO oder, soweit einschlägig, zum Zweck der Gesundheitsversorgung gemäß Art. 9 Abs. 2 lit. h DSGVO. Die Einholung und Dokumentation der erforderlichen Rechtsgrundlage obliegt dem Auftraggeber als verantwortlicher Stelle.

3.2 Zusammenfassend kann man sagen, dass der Auftragnehmer im Auftrag und nach Weisung des Auftraggebers i. S. v. Artikel 4 Abs. 2 DSGVO Daten verarbeitet. Der Auftraggeber bleibt nach Artikel 4 Abs. 7 DSGVO im datenschutzrechtlichen Sinn verantwortliche Stelle (Herr der Daten).

3.3 Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Für Dienstleister mit Sitz außerhalb der EU (vgl. §11.1) sind die Serverstandorte vertraglich auf die EU beschränkt; zusätzlich bestehen Standardvertragsklauseln (SCC) und/oder EU-US Data Privacy Framework-Zertifizierungen (DPF) als Garantie gemäß Art. 46 DSGVO. Jede darüber hinausgehende Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers.

3.4 Der Auftragnehmer erwirbt an den Auftraggeber-Daten keine Rechte und ist auf Verlangen des Auftraggebers jederzeit auf erstes Anfordern zur Herausgabe der Auftraggeber-Daten in einer für den Auftraggeber lesbaren und weiterverarbeitbaren Form verpflichtet. Zurückbehaltungsrechte in Bezug auf Auftraggeber-Daten und die dazugehörigen Datenträger sind ausgeschlossen.

§ 4 Technisch-organisatorische Maßnahmen

4.1 Der Auftragnehmer garantiert, dass er vor Beginn der Verarbeitung der Auftraggeber-Daten die im Folgenden beschriebenen technischen und organisatorischen Maßnahmen umsetzt und diese während der Vertragserfüllung aufrechterhält.

4.2 Übertragungssicherheit

Alle Datenübertragungen zwischen dem Endnutzer-Browser und der medo.core-Plattform erfolgen ausschließlich über verschlüsselte HTTPS/TLS-Verbindungen. API-Endpunkte sind durch Access-Token-Authentifizierung abgesichert; unautorisierter Zugriff wird serverseitig abgewiesen. Die Übertragung personenbezogener Daten im Klartext ist ausgeschlossen.

4.3 Serverseitige Speicherung – Digital Ocean (Frankfurt/FRA1)

Die Backend-Microservices von medo.core laufen auf Managed Kubernetes der DigitalOcean, LLC mit Serverstandort Frankfurt/FRA1 (EU). Die primäre Produktivdatenbank ist eine Managed-MySQL-8.0-Instanz bei DigitalOcean (Frankfurt/FRA1). Dateien, Dokumente und Medien werden in einem S3-kompatiblen ObjectStore (DigitalOcean Spaces, Frankfurt/FRA1) gespeichert. Für Caching kommt Managed Redis bei DigitalOcean (Frankfurt/FRA1) zum Einsatz. Der Zugriff auf Produktivdaten ist auf autorisierte Dienste und Mitarbeiter des Auftragnehmers beschränkt (rollenbasierte Zugriffskontrolle).

4.4 Benutzerdatenbank – IONOS (Deutschland)

Account- und Zugangsdaten werden in einer separaten Datenbank auf IONOS-Servern in Deutschland gespeichert (identification-Service). Dieser Service ist zugleich für den medo.coach-Einladungsprozess zuständig und wird geteilt mit der medo.check-Cloud-Infrastruktur. Der Zugriff auf die Benutzerdatenbank erfolgt ausschließlich durch den identification-Service des Auftragnehmers.

4.5 Frontend-Auslieferung – Vercel

Das Web-Frontend von medo.core wird über die Edge-Plattform Vercel Inc. bereitgestellt (EU-Region). Vercel verarbeitet transient Verbindungsdaten (IP-Adresse, User-Agent, Request-Logs) der Endnutzer im Rahmen der Frontend-Auslieferung. Ein direkter Zugriff von Vercel auf personenbezogene Produktivdaten findet nicht statt. Eine Auftragsverarbeitungsvereinbarung sowie eine Drittland-Garantie gemäß Art. 46 DSGVO liegen vor.

4.6 Fehler-Monitoring – Sentry

Für die Protokollierung, Korrektur und Vermeidung kritischer Fehler in medo.core und der medo.coach-App wird der Dienst Sentry der Functional Software Inc. beauftragt (sentry.io/legal/dpa/). Der Serverstandort liegt innerhalb der EU; eine Auftragsverarbeitungsvereinbarung sowie eine Drittland-Garantie gemäß Art. 46 DSGVO (SCC und/oder EU-US Data Privacy Framework) liegen vor. Übermittelte Fehlermeldungen enthalten Kontextinformationen (Servicename, Fehlermeldungstext); personenbezogene Nutzdaten werden verschlüsselt übermittelt und sind nur durch den Auftragnehmer entschlüsselbar.

4.7 E-Mail-Versand – SendGrid / Twilio

Transaktionale E-Mails (Terminbenachrichtigungen, medo.coach-Einladungen, Systemmeldungen) werden über den Dienst SendGrid der Twilio Inc. versendet. Übermittelte Daten: E-Mail-Adresse, Name, Nachrichteninhalt. Der Serverstandort liegt innerhalb der EU; eine Auftragsverarbeitungsvereinbarung sowie eine Drittland-Garantie gemäß Art. 46 DSGVO liegen vor. Eine Nutzung der übermittelten Daten zu eigenen Zwecken ist vertraglich ausgeschlossen.

4.8 Push-Benachrichtigungen – Google Firebase / FCM

Push-Benachrichtigungen an die medo.coach-App werden über Firebase Cloud Messaging (FCM) der Google Ireland Ltd. übermittelt. Dabei werden ausschließlich Geräte-Push-Token und der Benachrichtigungstext übertragen. Die Übermittlung gesundheitsbezogener Inhalte (Art. 9 DSGVO) in Push-Payloads ist ausgeschlossen. Eine Auftragsverarbeitungsvereinbarung sowie eine Drittland-Garantie gemäß Art. 46 DSGVO liegen vor.

4.9 KI-gestützte Funktionen – OpenAI und Pinecone

Die semantische Übungssuche im medo.core-Portal nutzt die OpenAI API (Text-Embeddings, Tag-Generierung) sowie Pinecone als Vektor-Datenbank (EU-Region). Dabei werden Nutzer-Suchanfragen (Freitext) und Übungs-Metadaten übermittelt. Es werden keine expliziten Gesundheitsdaten gemäß Art. 9 DSGVO in diesem Prozess weitergeleitet. Die Nutzung der übermittelten Daten für das Training von KI-Modellen ist vertraglich ausgeschlossen. Für beide Dienstleister liegen Auftragsverarbeitungsvereinbarungen sowie Drittland-Garantien gemäß Art. 46 DSGVO vor.

4.10 Video-Transkodierung – AWS MediaConvert

Die serverseitige Transkodierung von Übungs- und Trainingsvideos erfolgt über AWS MediaConvert der Amazon Web Services EMEA SARL (Region: eu-central-1, Frankfurt). Die Verarbeitung erfolgt ausschließlich in

der EU. Eine Auftragsverarbeitungsvereinbarung sowie eine Drittland-Garantie gemäß Art. 46 DSGVO liegen vor.

4.11 Zahlungsabwicklung – Stripe Connect

Die Zahlungsabwicklung für den Auftraggeber und seine Endkunden erfolgt über einen Stripe-Connect-Unteraccount unter dem medo.check-Plattform-Account bei Stripe Payments Europe, Ltd. Sensible Zahlungsdaten (Karteninhaberdaten, PAN) werden ausschließlich bei Stripe gespeichert und nicht durch medo.core weitergeleitet oder gespeichert. medo.core empfängt über Stripe-Webhooks ausschließlich Transaktionsstatus und Referenz-IDs. SEPA-Sammler werden aus den in medo.core gespeicherten IBAN-Daten erzeugt und dem Auftraggeber zur manuellen Einreichung bei seiner Bank bereitgestellt; die Bank des Auftraggebers ist kein Unterauftragnehmer des Auftragnehmers. Eine Auftragsverarbeitungsvereinbarung liegt vor.

4.12 Physische Sicherheit

Die Büroräume der Firma medo.check befinden sich im Forschungs- und Entwicklungszentrum der Universität Witten-Herdecke. Die Büroräume sind zwischen 8 und 18 Uhr besetzt und niemand kann unbefugt diese Räume betreten. Nach Verlassen der Räumlichkeiten werden alle Türen verschlossen. Zu Nachtzeiten und am Wochenende ist das Gebäude verschlossen und alarmgesichert; ein Wachdienst kontrolliert regelmäßig.

4.13 Anpassung der Maßnahmen

Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es dem Auftragnehmer nach vorheriger schriftlicher Zustimmung des Auftraggebers gestattet, alternative und adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird solche Änderungen dokumentieren und den Auftraggeber unverzüglich informieren, wenn er Anhaltspunkte für die Unzulänglichkeit bestehender Maßnahmen hat.

§ 5 Pflichten des Auftragnehmers

5.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 DSGVO).

5.2 Der Auftragnehmer stellt sicher und kontrolliert regelmäßig, dass die Datenerhebung, -verarbeitung und -nutzung der Auftraggeber-Daten in Übereinstimmung mit diesem Vertrag und den Weisungen des Auftraggebers erfolgt und die technischen und organisatorischen Maßnahmen und Voraussetzungen gemäß §4 dieses Vertrages eingehalten werden.

5.3 Der Auftragnehmer darf ohne vorherige schriftliche Zustimmung durch den Auftraggeber im Rahmen der Auftragsdatenverarbeitung keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen. Hiervon ausgenommen sind Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß des Lizenzvertrags (einschließlich der Datensicherung) erforderlich sind, sowie Kopien zur Einhaltung gesetzlicher Aufbewahrungspflichten.

5.4 Der Auftragnehmer hat den Auftraggeber unverzüglich darüber zu informieren, wenn das Eigentum des Auftraggebers oder seine sonstigen Rechte an den Auftraggeber-Daten beim Auftragnehmer durch Maßnahmen Dritter (z. B. Pfändung, Beschlagnahme, Insolvenz oder Vergleichsverfahren) oder durch sonstige Ereignisse gefährdet wird.

5.5 Ist der Auftraggeber gegenüber einer staatlichen Stelle, einem Betroffenen oder einer anderen Person verpflichtet, Auskünfte über die Auftraggeber-Daten zu erteilen, ist der Auftragnehmer verpflichtet, den

Auftraggeber bei der Erteilung solcher Auskünfte auf erstes Anfordern zu unterstützen, insbesondere durch unverzügliches Zurverfügungstellen sämtlicher relevanter Informationen und Dokumente.

5.6 Der Auftragnehmer hat dem Auftraggeber auf Anforderung unverzüglich eine jeweils aktuelle Übersicht über die in Art. 12 Abs. 1 DSGVO genannten Angaben sowie über die zugriffsberechtigten Personen zur Verfügung zu stellen.

5.7 Der Auftragnehmer hat die bei der Erhebung, Verarbeitung oder Nutzung von Auftraggeber-Daten beschäftigten Personen gemäß Art. 28 DSGVO schriftlich auf das Datengeheimnis zu verpflichten und in die gesetzlichen Bestimmungen über den Datenschutz einzuweisen. Der Auftragnehmer wird diese Verpflichtungen schriftlich dokumentieren und sie auf Verlangen des Auftraggebers diesem vorlegen.

5.8 Der Auftragnehmer ist verpflichtet, einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten nach Art. 38 DSGVO zu bestellen, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind.

§ 6 Rechte und Pflichten des Auftraggebers

6.1 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

6.2 Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

6.3 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

6.4 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

6.5 Der Auftraggeber ist Eigentümer der Auftraggeber-Daten und Inhaber aller etwaigen Rechte, die die Auftraggeber-Daten betreffen.

§ 7 Weisungsrechte des Auftraggebers

7.1 Der Auftragnehmer erhebt, verarbeitet und nutzt die Auftraggeber-Daten ausschließlich in Übereinstimmung mit den in diesem Lizenzvertrag enthaltenen Bestimmungen und den sonstigen Weisungen des Auftraggebers. Der Auftraggeber besitzt insoweit gegenüber dem Auftragnehmer ein umfassendes Weisungsrecht über Art, Umfang, Zweck und Verfahren der Erhebung, Verarbeitung und Nutzung von Auftraggeber-Daten.

7.2 Die Weisungen des Auftraggebers sollen grundsätzlich in Schrift- oder Textform erfolgen.

7.3 Der Auftragnehmer ist verpflichtet, die Weisungen des Auftraggebers unverzüglich auszuführen. Der Auftraggeber ist berechtigt, dem Auftragnehmer hierfür im Einzelfall eine jeweils angemessene Frist zu setzen, die der Auftragnehmer einzuhalten hat.

7.4 Ist der Auftragnehmer der begründeten Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder geltendes Datenschutzrecht verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber (mindestens 14 Tage vorher) berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen. Bestätigt der Auftraggeber die Weisung, ist der Auftragnehmer verpflichtet, sie zu befolgen.

§ 8 Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

§ 9 Mitteilungs- und Unterstützungspflichten bei Datensicherheitsvorfällen

9.1 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er oder ein Mitarbeiter bei der Erhebung, Verarbeitung oder Nutzung von Auftraggeber-Daten gegen datenschutzrechtliche Vorschriften, gegen Festlegungen aus diesem Vertrag oder gegen eine vom Auftraggeber erteilte Weisung verstoßen hat, wenn Anhaltspunkte dafür bestehen, dass ein Dritter unrechtmäßig Kenntnis von Auftraggeber-Daten erlangt haben könnte, oder wenn in sonstiger Weise eine Gefährdung für die Integrität oder Vertraulichkeit der Auftraggeber-Daten eingetreten ist („Datensicherheitsvorfall").

9.2 Die Information über den Datensicherheitsvorfall hat Angaben über den Zeitpunkt und die Art des Vorfalls (einschließlich einer Information, welche und wie Auftraggeber-Daten betroffen sind), das betroffene EDV-System, die betroffenen Personen, den Zeitpunkt der Entdeckung, alle denkbaren nachteiligen Folgen sowie die vom Auftragnehmer ergriffenen Maßnahmen zu enthalten.

9.3 Eine erste Information des Auftraggebers hat unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung von dem Datensicherheitsvorfall, zu erfolgen. Eine weitere, detaillierte Unterrichtung des Auftraggebers hat innerhalb von sieben Tagen nach Kenntniserlangung zu erfolgen.

9.4 Der Auftragnehmer ist verpflichtet, den Auftraggeber im Falle eines Datensicherheitsvorfalls bei seinen diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen, einschließlich aller Handlungen zur Erfüllung gesetzlicher Verpflichtungen, auf erstes Anfordern auf angemessene Weise zu unterstützen.

9.5 Der Auftragnehmer ist verpflichtet, unverzüglich nach Kenntniserlangung von einem Datensicherheitsvorfall eine technische Analyse durchzuführen, diese zu dokumentieren und dem Auftraggeber die Dokumentation auf Verlangen auszuhändigen. Stellt der Auftraggeber fest, dass die bisherigen technischen und organisatorischen Maßnahmen nicht ausreichend waren, ist der Auftragnehmer verpflichtet, ohne zusätzliche Kosten solche zusätzlichen Maßnahmen umzusetzen, die nach Ansicht des Auftraggebers erforderlich sind.

§ 10 Kontrollrechte des Auftraggebers

10.1 Der Auftraggeber ist dazu berechtigt, jederzeit die Erhebung, Verarbeitung und Nutzung von Auftraggeber-Daten durch den Auftragnehmer einschließlich der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen und die Ordnungsmäßigkeit der Datenverarbeitungsprozesse und -programme des Auftragnehmers zu prüfen.

10.2 Zur Durchführung von Kontrollen nach §10.1 ist der Auftraggeber berechtigt, jederzeit sämtliche Geschäftsräume des Auftragnehmers zu betreten und dort Vor-Ort-Kontrollen durchzuführen. Der Auftraggeber wird dem Auftragnehmer solche Vor-Ort-Kontrollen rechtzeitig vorher ankündigen. Der Auftragnehmer gewährt dem Auftraggeber sämtliche für die Durchführung der Kontrolle benötigten Zugangs-, Auskunfts- und Einsichtsrechte.

10.3 Zur Ermöglichung von Kontrollen nach §10.1 ist der Auftragnehmer außerdem verpflichtet, dem Auftraggeber unverzüglich sämtliche Zertifikate, Auditberichte und sonstige Ergebnisse von Überprüfungen im Hinblick auf die Erhebung und Verwendung personenbezogener Daten ungekürzt vorzulegen.

10.4 Der Auftraggeber ist berechtigt, von dem betrieblichen Datenschutzbeauftragten des Auftragnehmers Auskunft über sämtliche Aspekte der Erhebung, Verarbeitung oder Nutzung von Auftraggeber-Daten, einschließlich der getroffenen technischen und organisatorischen Maßnahmen, zu erhalten.

10.5 Der Auftraggeber ist berechtigt, die Kontrollhandlungen nach diesem Paragraphen selbst oder durch einen zur Geheimhaltung verpflichteten Bevollmächtigten vorzunehmen. Der Auftragnehmer ist verpflichtet, die Kontrollhandlungen eines solchen Bevollmächtigten in derselben Weise zu dulden und zu unterstützen wie Kontrollen durch den Auftraggeber.

10.6 Gemäß den anwendbaren Datenschutzvorschriften unterliegen der Auftraggeber und der Auftragnehmer Kontrollen durch die zuständige Aufsichtsbehörde. Auf Verlangen des Auftraggebers wird der Auftragnehmer den Auftraggeber im Rahmen von behördlichen Aufsichtsverfahren nach Kräften unterstützen, wenn und soweit die Erhebung, Verarbeitung oder Nutzung von Auftraggeber-Daten Gegenstand des Aufsichtsverfahrens ist.

§ 11 Unterauftragsverhältnisse

11.1 Der Auftragnehmer darf Unterauftragsverhältnisse hinsichtlich der Erhebung, Verarbeitung oder Nutzung von Auftraggeber-Daten nur nach vorheriger schriftlicher Zustimmung des Auftraggebers begründen. Zum Zeitpunkt der Vertragsschließung bestehen folgende Unterauftragsverhältnisse, mit deren Beauftragung sich der Auftraggeber durch Unterzeichnung dieses Vertrags einverstanden erklärt:

Dienstleister	Verarbeitungszweck	Serverstandort	Drittland-Garantie
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur	Benutzerdatenbank (identification-Service, medo.coach-Einladungsprozess)	Deutschland (EU)	Nicht erforderlich (EU-Anbieter)
DigitalOcean, LLC, 101 Ave of the Americas, New York, NY, USA	Managed Kubernetes, MySQL 8.0, Redis, ObjectStore (Spaces) – alle Microservices und Produktivdaten	Frankfurt/FRA1 (EU)	SCC und/oder EU-US Data Privacy Framework
Vercel Inc., 340 Pine Street, San Francisco, CA, USA	Frontend-Hosting und Deployment (medo.core Web-App)	EU-Region	SCC und/oder EU-US Data Privacy Framework
Functional Software Inc. (Sentry), 45 Fremont St., San Francisco, CA, USA	Fehler-Monitoring (medo.core und medo.coach)	EU	SCC und/oder EU-US Data Privacy Framework
Stripe Payments Europe, Ltd., 1 Grand Canal Street Lower, Dublin, Irland	Zahlungsabwicklung (Stripe Connect)	EU / Irland	SCC (EU-Vertragsrechtsträger)
OpenAI Ireland Ltd. / OpenAI, LLC [Adresse zu ergänzen]	KI-Funktionen: semantische Übungssuche, Tag-Generierung (exercises-api)	EU [zu bestätigen]	SCC und/oder EU-US Data Privacy Framework
Twilio Inc. / SendGrid, 375 Beale St., San Francisco, CA, USA	E-Mail-Versand (Benachrichtigungen, medo.coach-Einladungen)	EU-Region	SCC und/oder EU-US Data Privacy Framework
Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Irland	Push-Benachrichtigungen (Firebase Cloud Messaging) für medo.coach	EU	SCC und/oder EU-US Data Privacy Framework
Amazon Web Services EMEA SARL, 38 Av. John F. Kennedy, Luxemburg	Video-Transkodierung (AWS MediaConvert)	eu-central-1 Frankfurt (EU)	SCC und/oder EU-US Data Privacy Framework
Pinecone Systems, Inc. [Adresse zu ergänzen]	Vektor-Datenbank für semantische Übungssuche	EU-Region [zu bestätigen]	SCC und/oder EU-US Data Privacy Framework

Der Auftragnehmer wird dem Auftraggeber auf Anforderung eine aktuelle Übersicht über die eingeschalteten Unterauftragnehmer übergeben.

11.2 Nicht als Unterauftragsverhältnis im Sinne des §11.1 sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

11.3 Zur Prüfung einer Zustimmung nach §11.1 hat der Auftragnehmer dem Auftraggeber den Entwurf des Unterauftragsdatenverarbeitungsvertrags zwischen ihm und dem Unterauftragnehmer ungekürzt in Kopie zur Verfügung zu stellen. Ferner muss der Auftragnehmer dem Auftraggeber schriftlich bestätigen, dass er den

Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat. Ein Anspruch auf Erteilung der Zustimmung durch den Auftraggeber besteht nicht.

11.4 Der Auftragnehmer hat den Unterauftragnehmer in dem Unterauftragsdatenverarbeitungsvertrag schriftlich ebenso zu verpflichten, wie auch der Auftragnehmer aufgrund dieses Vertrags gegenüber dem Auftraggeber verpflichtet ist. Dem Auftraggeber sind im Unterauftragsdatenverarbeitungsvertrag gegenüber dem Unterauftragnehmer unmittelbar sämtliche Kontrollrechte gemäß §10 dieses Vertrags einzuräumen. In dem Unterauftragsdatenverarbeitungsvertrag sind die Verantwortlichkeitssphären klar voneinander abzugrenzen. Der Auftragnehmer haftet für ein Verschulden seiner Unterauftragnehmer wie für eigenes Verschulden.

11.5 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber den Unterauftragnehmern gelten.

11.6 Der Auftragnehmer hat abgeleitete Kontrollpflichten gegenüber den Unterauftragnehmern und muss hierfür die in diesem Vertrag beschriebenen Kontrollbefugnisse des Auftraggebers wahrnehmen. Der Auftraggeber bleibt berechtigt, die Ausübung der Kontrollbefugnisse durch den Auftragnehmer uneingeschränkt zu überwachen und kann jederzeit auch selbst diese Kontrolle gegenüber dem Unterauftragnehmer ausüben.

11.7 Die Mitteilungspflichten des Auftragnehmers gemäß §9 gelten entsprechend für Datensicherheitsvorfälle, die sich bei seinen Unterauftragnehmern ereignen.

§ 12 Rechte der Betroffenen

12.1 Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen.

12.2 Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Auskunft, Berichtigung, Löschung oder Sperrung der ihn betreffenden Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und ohne entsprechende Einzelweisung des Auftraggebers nicht mit dem Betroffenen in Kontakt treten. Der Auftragnehmer darf Auskünfte an Betroffene nur nach vorheriger Weisung durch den Auftraggeber erteilen.

12.3 Für den Fall, dass eine betroffene Person ihre Rechte auf Berichtigung, Löschung oder Sperrung von Auftraggeber-Daten oder auf Auskunft über die gespeicherten Auftraggeber-Daten geltend macht, hat der Auftragnehmer den Auftraggeber auf erstes Anfordern im zumutbaren Umfang zu unterstützen. Insbesondere wird der Auftragnehmer dem Auftraggeber unverzüglich, längstens aber innerhalb von fünf Werktagen, die erforderlichen Informationen mitteilen.

12.4 Der Auftragnehmer ist verpflichtet, Auftraggeber-Daten auf Weisung des Auftraggebers unverzüglich, spätestens aber innerhalb einer Frist von fünf Werktagen, zu berichtigen, zu löschen oder zu sperren. Der Auftragnehmer wird dem Auftraggeber die weisungsgemäße Berichtigung, Sperrung oder Löschung jeweils auf Verlangen schriftlich bestätigen.

§ 13 Auskunft an Dritte

Soweit der Auftragnehmer aufgrund gesetzlicher Bestimmungen Dritten Auskunft über Auftraggeber-Daten erteilen muss, ist der Auftragnehmer verpflichtet, den Auftraggeber rechtzeitig vor Auskunftserteilung über Empfänger, Zeitpunkt und Inhalt der zu erteilenden Auskunft und deren Rechtsgrundlage schriftlich zu informieren.

§ 14 Rückgabe und Löschung überlassener Daten und Datenträger

14.1 Dem Auftragnehmer ist es untersagt, nach Beendigung dieses Vertrags Auftraggeber-Daten aktiv zu erheben, zu verarbeiten und zu nutzen; nur eine weitere Speicherung der Auftraggeber-Daten bleibt zugelassen, bis der Auftragnehmer diese an den Auftraggeber herausgegeben oder gelöscht bzw. vernichtet hat; in diesem Fall gelten die Bestimmungen dieses Vertrags auch nach Beendigung bis zu dem Zeitpunkt weiter, in dem der Auftragnehmer über keinerlei Auftraggeber-Daten mehr verfügt.

14.2 Der Auftragnehmer hat sämtliche ihm vom Auftraggeber überlassenen sowie sämtliche im Zuge der Vertragsdurchführung hinzugewonnenen Auftraggeber-Daten und alle Verarbeitungs- und Nutzungsergebnisse hieraus vollständig und unwiederbringlich zu löschen bzw. zu vernichten, sobald ihre Kenntnis für die Erfüllung des Zwecks der jeweiligen Erhebung und Verwendung nicht mehr erforderlich ist, spätestens nach Beendigung der vertragsgegenständlichen Leistungserbringung.

14.3 Mindestens 18 Werktage vor jeder Löschung oder Vernichtung nach §14.2 hat der Auftragnehmer den Auftraggeber unter detaillierter Angabe der betroffenen Auftraggeber-Daten und Ergebnisse schriftlich über die bevorstehende Löschung bzw. Vernichtung zu informieren. Der Auftraggeber kann innerhalb dieser Frist vom Auftragnehmer die Herausgabe der betroffenen Auftraggeber-Daten verlangen.

14.4 Soweit Auftraggeber-Daten auf Datenträgern enthalten sind, sind diese Datenträger unter Einhaltung einer angemessenen Sicherheitsstufe zu vernichten.

14.5 Die Bestimmungen der §14.2–14.4 gelten auch für Vervielfältigungen der Auftraggeber-Daten (insbesondere Archivierungs- und Sicherungsdateien) in allen Systemen des Auftragnehmers sowie für Test- und Ausschussdaten.

14.6 Über eine Löschung bzw. Vernichtung von Auftraggeber-Daten hat der Auftragnehmer ein Protokoll zu erstellen, das dem Auftraggeber auf Anforderung unverzüglich vorzulegen ist.

14.7 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 15 Verhältnis zum Hauptvertrag

Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

Dieser Vertrag kommt mit Unterzeichnung durch den Auftraggeber und Zugang beim Auftragnehmer zustande; einer Gegenzeichnung durch den Auftragnehmer bedarf es nicht.

Unterschriften

Ort, Datum

Auftraggeber (Unterschrift)

Ort, Datum

Heidötting & Winter GbR, vertreten durch Tino Heidötting