

1. Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Zwischen

Auftraggeber (Verantwortlicher):

[Behandelnder Arzt]

Und

Auftragnehmer (Auftragsverarbeiter):

Ruma GmbH
Aachener Str. 338
50933 Köln

Präambel

(1) Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich durch die Nutzung des Ruma Digital System Pro ergeben. Sie findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Dritte mit personenbezogenen oder vertraulichen Daten des Auftraggebers in Berührung kommen können. Die Bestimmungen dieses Vertrages gelten entsprechend, wenn die Prüfung, Wartung bzw. Fernwartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch den Auftragnehmer oder durch von ihm beauftragte Dritte im Auftrag vorgenommen wird und dabei die Kenntnisnahme personenbezogener Daten möglich ist.

(2) Sollte es nach Beendigung des Hauptvertrages zu einem Folgeauftrag kommen, gelten die Bestimmungen dieser Vereinbarung auch für den Folgevertrag, ohne dass es einer expliziten Verlängerung oder eines Neuabschlusses dieses Vertrages bedarf. Der Folgevertrag ersetzt inhaltlich und begrifflich sodann vollumfänglich den Hauptvertrag im Sinne dieses Vertrages. Dies vorausgeschickt vereinbaren die Parteien Folgendes:

1.1. [Gegenstand und Dauer der Vereinbarung](#)

(1) Der Auftrag umfasst Folgendes: Nutzung des Ruma Digital System Pro durch den behandelnden Arzt sowie des Ruma Digital System durch den Patienten; Erfassen von Videos von Einnahmeprozessen durch den Patienten; Bewerten der aufgenommenen Videos durch den behandelnden Arzt; verschlüsselte Speicherung des Private Keys des Arztes auf seinem Endgerät; verschlüsselte Datenübertragungen und Speicherungen bei Dienstleistern zur Sicherstellung der Funktionalität des Ruma Digital System (Pro).

(2) Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Datenschutzvertrages.

(3) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in Deutschland erbracht.

1.2. Weisung

(1) Eine Weisung durch den behandelnden Arzt erfolgt nicht. Der gesamte Verarbeitungsprozess ist vollautomatisiert.

1.3. Dauer des Auftrags

(1) Der Vertrag gilt für die Nutzung des Ruma Digital System (Pro).

2. Art der personenbezogenen Daten

- Anonymisierte Patientendaten
 - Einwilligung des Patienten und Versionierung des Einwilligungstextes
 - Kennung der Patienten-App, verschlüsselt, mit Zeitstempel
 - Kennung der ausgegebenen Marker, verschlüsselt, mit Zeitstempel
 - Verweis auf verschlüsselte Video-Datei, mit Zeitstempel
 - Ergebnis der Bewertung des Arztes nach Ansicht des Videos, mit Zeitstempel
- Kontaktdaten des behandelnden Arztes
- Private Key des behandelnden Arztes

2.1. Kategorien betroffener Personengruppen

- Patienten
- Behandelnder Arzt
- Mitarbeiter des behandelnden Arztes

2.2. Rechte und Pflichten des Auftraggebers

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

(2) 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.

(3) Dem Auftraggeber wird ausdrücklich untersagt, das für Ruma Digital-System Pro genutzte Tablet für private Zwecke zu nutzen. Das Gerät ist nur in den Praxisräumlichkeiten und nur von Praxispersonal zu benutzen sowie mit einem Code zu sichern, um gegen Verlust und unbefugte Benutzung geschützt zu sein.

2.3. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

(1) Es sind keine weisungsberechtigten Personen benannt. Die gesamte Verarbeitung erfolgt voll automatisiert.

3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich voll automatisiert im Rahmen der von der Ruma Digital System App vorgegebenen Parameter.

(2) Der Auftragnehmer sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

- (3) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutzfolgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO). Er hat die dazu erforderlichen Angaben dem Auftraggeber unverzüglich weiterzuleiten.
- (4) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.
- (5) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
- (6) Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
- (7) Beim Auftragnehmer ist als Beauftragter für den Datenschutz Martin Lemke, Cyclops GmbH, martin.lemke@cyclops.de bestellt.
- (8) Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

4. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

- (1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich - spätestens jedoch innerhalb von zwei Stunden - Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger schriftlicher Weisung gem. Ziff. 4 dieses Vertrages durchführen.
- (2) Es ist bekannt, dass für vorgenannte Meldepflichten des Auftraggebers bzw. dessen Auftraggebern Fristen von 72 Stunden gemäß GVO bzw. 24 Stunden gemäß TKG bestehen.

5. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

- (1) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere müssen der Auftraggeber, dessen

Geschäftspartner und von ihnen beauftragte Dritte berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen.

(2) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden.

(3) Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) angemessen zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

(4) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

(5) Zurzeit sind für den Auftragnehmer die in Anlage „Subunternehmer“ mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

(6) Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

6. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

(1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden mindestens die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität der Systeme und Dienste, sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

(2) Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine angemessene Risikobewertung durch den Auftragnehmer nachweisbar durchgeführt, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt.

(3) Das zu diesem Vertrag einsehbare Datenschutz- und IT-Sicherheitskonzept des Ruma Digital System stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

(4) Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages und weitere drei Jahre aufzubewahren.

7. Haftung

(1) Es wird grundsätzlich auf Art. 82 DSGVO verwiesen. Im Übrigen stellt der Auftragnehmer den Auftraggeber von jeder Haftung für Datenschutzverstöße, die im Einflussbereich des Auftragnehmers liegen, frei.

8. Sonstiges

(1) Für Nebenabreden ist die Schriftform erforderlich, was auch für die Aufhebung derselben gilt.

(2) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(3) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Vertragsparteien sind im Falle einer unwirksamen Bestimmung dieses Vertrags verpflichtet, über eine Ersatzregelung zu verhandeln, die dem von den Vertragsparteien mit der unwirksamen Bestimmung verfolgten wirtschaftlichen Zweck am nächsten kommt und die rechtlich zulässigen Inhalt hat.

(4) Es gilt deutsches Recht.

[Behandelnder Arzt
Musterstadt]

Ruma GmbH
Köln

Elektronisch eingewilligt am:
[Datum]

Elektronisch eingewilligt am:
[Datum]