Auftragsverarbeitungsvertrag (Stand: 22.01.2025)

zwischen Auftraggeber und RED Medical Systems GmbH, Lutzstraße 2, 80687 München - Auftragnehmer -

§ 1 Allgemeines

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

2. Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

§ 2 Gegenstand des Auftrags

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Der Auftragnehmer erbringt für den Auftraggeber eine oder mehrere der nachfolgenden Leistungen:
- Bereitstellung eines Informationssystems (Software-as-a-Service) zur Verwaltung von Kundendaten, die entweder dem Berufsgeheimnis (§ 203 StGB) unterliegen oder aufgrund ihrer Sensibilität ein besonderes Schutzbedürfnis haben
- Bereitstellung eines Videosprechstunden-Systems (siehe auch Anlage 3)

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:
- Kundendaten (Ende-zu-Ende-verschlüsselt)
- administrative Daten des Auftragsgebers (Termine, Ressourcen etc.)
- administrative Daten des Systems (Nutzer, Berechtigungen etc.)

Kreis der von der Datenverarbeitung Betroffenen:
- Angestellte des Auftragsgebers
- Kunden (allerdings nur insofern als das ihre Daten verschlüsselt bzw. pseudonymisiert gespeichert werden - eine Entschlüsselung und/oder Zuordnung der Daten zu realen Personen ist dem Auftragnehmer nicht möglich)

§ 3 Rechte und Pflichten des Auftraggebers

1. Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

2. Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

3. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

4. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

5. Der Auftraggeber kann weisungsberechtigte Personen benennen. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

6. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

7. Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

8. Dem Auftragnehmer ist es nicht gestattet, im Rahmen einer Videosprechstunde Werbung zu schalten.

§ 4 Rechte und Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. 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. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

2. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

3. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

4. Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

5. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

6. Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig.

7. Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

8. Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

9. Es besteht keine explizite Notwendigkeit, dass der Auftragnehmer sich zur Verschwiegenheit gemäß § 203 StGB (Berufsgeheimnis) verpflichtet, da alle diesbezüglichen Daten Ende-zu-Ende verschlüsselt werden und der Auftragnehmer keinen Zugriff auf die entsprechenden Schlüssel und Klartextdaten hat. Sollten dem Auftragnehmer dennoch im Einzelfall entsprechende Daten zur Kenntnis gelangen (z. B. im Rahmen eines Service-Einsatzes) verpflichtet er sich, diese Daten gemäß § 203 StGB geheim zu halten und seine Beschäftigten und seine Mitwirkenden entsprechend zu Vertraulichkeit und Verschwiegenheit zu verpflichten.

10. Der Auftragnehmer wird den Auftraggeber gelegentlich per E-Mail kontaktieren, um über zusätzliche Funktionen und Produktneuheiten zu informieren. Der Auftraggeber stimmt dieser Form der Kontaktaufnahme explizit zu.

§ 5 Datenschutzbeauftragter des Auftragnehmers

1. Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

Kontaktdaten: Alarmstufe Red GmbH, Bettina Sandrock, St. Georg Str. 44, 86911 Dießen,
b.sandrock@alarmstufe-red.de,
08807 949596, www.alarmstufe-red.de

§ 6 Meldepflichten des Auftragnehmers

1. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

2. Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

3. Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:
- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

§ 7 Mitwirkungspflichten des Auftragnehmers

1. Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

2. Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

§ 8 Kontrollbefugnisse

1. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren.

2. Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

3. Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen.

4. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 2 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments i.S.d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.

5. Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine

Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren. Für Auftraggeber, die der evangelischen Datenschutzaufsichtsbehörde unterliegen, unterwirft sich der Auftragsverarbeiter gemäß § 30 Absatz 5 Satz 3 DSG-EKD der kirchlichen Datenschutzaufsicht. Dies erstreckt sich auf die Aufgaben und Befugnisse der kirchlichen Datenschutzaufsicht nach §§ 43, 44 EKD-Datenschutzgesetz.

§ 9 Unterauftragsverhältnisse

1. Der Auftragnehmer ist berechtigt, die in der Anlage 1 zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Abs. 2 genannten Voraussetzungen zulässig.

2. Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, ob dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber vier Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information“ erfolgt, gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

3. Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.

4. Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

5. Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

6. Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

7. Der Auftragnehmer haftet dem Auftraggeber gegenüber für Datenschutzverstöße des Unterauftragnehmers.

8. Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

§ 10 Vertraulichkeitsverpflichtung nach DSGVO

1. Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

2. Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

3. Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

§ 10a Verschwiegenheitsverpflichtung für Berufsgeheimnisträger

1. Sofern der Auftraggeber zu einer der nachfolgenden Berufsgruppen gehört, beauftragt er den den Auftragnehmer mit der Erbringung einer Dienstleistung gemäß § 2 im Sinne des
- für Rechtsanwälte: § 43e Bundesrechtsanwaltsordnung (BRAO)
- für Notare: § 26a Bundesnotarordnung (BNotO)
- für Patentanwälte: § 39c Patentanwaltsordnung
- für Steuerberater: § 62a Steuerberatungsgesetz (StBerG)
- für Wirtschaftsprüfer: § 50a Wirtschaftsprüferordnung (WPO)
- für die evangelische Kirche: § 30 Datenschutzgesetz Evangelische Kirche Deutschlands (DSG-EKD)
- für die katholische Kirche: § 29 Gesetz über den Kirchlichen Datenschutz (KDG)

In diesem Zusammenhang wird der Auftraggeber dem Auftragnehmer, soweit dies zur Inanspruchnahme der Dienstleistungen erforderlich ist, ggf. den Zugang zu Tatsachen eröffnen, auf die sich die Verpflichtung des Auftraggebers zur Verschwiegenheit nach
- für Rechtsanwälte: § 43a Absatz 2 Satz 1 BRAO
- für Notare: § 18 BNotO
- für Patentanwälte: § 39a Absatz 2 Patentanwaltsordnung
- für Steuerberater: § 57 Absatz 1 StBerG
- für Wirtschaftsprüfer: § 50a Wirtschaftsprüferordnung (WPO)
- für die evangelische Kirche: § 3 DSG-EKD
- für die katholische Kirche: § 5 KDG

bezieht.

2. Der Auftragnehmer ist zur Verschwiegenheit über alle Tatsachen verpflichtet, die dem Auftraggeber bei der Ausübung seines Amtes/Berufes bekannt geworden sind und zu denen der Auftraggeber ihm den Zugang eröffnet hat. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Er ist ferner verpflichtet, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist. Der Auftragnehmer ist verpflichtet, von ihm beschäftigte Personen, die er zur Vertragserfüllung heranzieht, in schriftlicher Form zur Verschwiegenheit zu verpflichten. Der Auftragnehmer ist befugt, weitere Personen zur Vertragserfüllung heranzuziehen. In diesem Fall ist der Auftragnehmer verpflichtet, auch diese Personen in schriftlicher Form zur Verschwiegenheit zu verpflichten.

3. Auf die strafrechtlichen Folgen der Verletzung dieser Pflichten wurde hingewiesen, insbesondere auf §§ 203 und 204 Strafgesetzbuch. Dem Auftragnehmer ist bekannt, dass diese Strafvorschrift auch für ihn und seine Mitarbeiter gilt.

4. Der Auftragnehmer verpflichtet sich in Abhängigkeit von der jeweiligen Lizenz, auf Anforderung des Auftraggebers einen Auftragsverarbeitungsvertrag in Schriftform mit dem vorliegenden Inhalt zu treffen.

§ 11 Wahrung von Betroffenenrechten

1. Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

2. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

3. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

§ 12 Geheimhaltungspflichten

1. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 13 Vergütung

Bezüglich der Vergütung des Auftragnehmers gilt die jeweils aktuelle Preisliste des Auftragnehmers. Diese wird dem Auftraggeber zusammen mit diesem Vertrag übergeben. Änderungen der Preisliste sind möglich und müssen mit einer Frist von drei Monaten zum Quartalsende dem Auftraggeber bekannt gemacht werden.

§ 14 Technische und organisatorische Maßnahmen zur Datensicherheit

1. Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

2. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 2 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

3. Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

§ 15 Dauer des Auftrags

1. Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.

2. Die Kündigungsfrist ist - soweit nicht anders vereinbart - in § XII der AGB des Auftragnehmers geregelt.

3. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

§ 16 Beendigung

1. Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren.

17. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

18. Schlussbestimmungen

1. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

2. Für Nebenabreden ist die Schriftform erforderlich.

3. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlage 1 - Unterauftragnehmer
Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer"). Wie in § 4.9 beschrieben, werden alle dem Berufsgeheimnis unterliegenden Daten Ende-zu-Ende verschlüsselt. Weder der Auftragnehmer noch seine Unterauftragnehmer haben Zugriff auf die entsprechenden Schlüssel und Klartextdaten. Bei den Unterauftragnehmern handelt es sich um nachfolgende Unternehmen:

Hosting App-Server und Datenbanken:
gridscale GmbH
Oskar-Jäger-Straße 173
50825 Köln

Hosting Turnserver:
Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen

SMS-Versand:
Kloppe Media GmbH
Ansbacher Str. 85
91541 Rothenburg ob der Tauber

Durchführung von Testverfahren:
Hogrefe Verlag GmbH & Co. KG
Merkelstraße 3
37085 Göttingen, Germany

Anlage 2 - Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO
Zur Gewährleistung der Sicherheit und Vertraulichkeit der Daten wird RED Medical alle erforderlichen technischen und organisatorischen Maßnahmen, insbesondere die durch die einschlägigen anwendbaren, rechtlichen Rahmenbedingungen festgelegten Maßnahmen treffen und aufrechterhalten. Die technischen und organisatorischen Maßnahmen beziehen sich auf sämtliche im Rahmen der Auftragsverarbeitung verarbeiteten Datenkategorien. Die Maßnahmen des Auftragnehmers beinhalten insbesondere:

Zutrittskontrolle, d.h. Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet und genutzt werden, zu verwehren. Der Auftragnehmer gewährleistet die Zutrittskontrolle durch den Einsatz folgender Maßnahmen: eines elektronischen Zutrittskontrollsystems mittels Chipkarten und dazugehörigem Berechtigungswesen, Einbruchmeldeanlage, Pförtner, Besucherbuch; Protokoll der Besucher; Besucher in Begleitung durch Mitarbeiter.

Zugangskontrolle, d.h. es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
Der Auftragnehmer gewährleistet die Zugangskontrolle durch die Vergabe separater Passwörter für die Betriebssystems-, Applikations- und Datenbank-Ebene. Innerhalb des Datenbanksystems ist die entsprechende Datenbank selbst durch Passwörter geschützt. Es ist gewährleistet, dass die entsprechenden Passwörter nur berechtigten Personen zugänglich sind. Folgende technischen Maßnahmen sind umgesetzt: Sperren von externen Schnittstellen, Einsatz einer Antivirus-Software auf den Servern und an den Arbeitsplätzen, Installation von Firewallsystemen.

Zugriffskontrolle, d.h. es ist dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen und personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert oder verändert werden können.
Der Auftragnehmer gewährleistet die Zugriffkontrolle analog zur Zugangskontrolle mittels individueller Berechtigung der Administratoren und Anweisung im Umgang mit vertraulichen Daten, zugriffsbeschränkender Maßnahmen, Einsatz von Verschlüsselungsverfahren, sicherer Aufbewahrung von Datenträgern, Einsatz von Aktenvernichtern, sowie technische Trennung der RED Medical-Umgebungen.

Weitergabekontrolle, d.h. es ist dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
Der Auftragnehmer gewährleistet die Weitergabekontrolle durch eine ausschließlich per TLS 1.2 abgesicherte Verbindung zwischen Client und Server. Dabei werden die Vorgaben der BSI TR-02161 beachtet. Darüber hinaus werden Daten nicht dauerhaft gespeichert, sondern nur an den adressierten Empfänger durchgeleitet. Eine Weitergabe an Dritte findet nicht statt. Sofern im Rahmen des Systems personenbezogene Klartextdaten auf der Clientseite gespeichert werden (z. B. bei der Abrechnung oder der Anbindung medizinische-technischer Geräte), werden diese nach Abschluss der jeweiligen Aktion sicher und vollständig gelöscht, es sei denn, sie wurden im Laufe der Verarbeitung sicher verschlüsselt (z.B. durch das KBV-Kryptomodul).

Verfügbarkeitskontrolle, d.h. es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Der Auftragnehmer gewährleistet die Einhaltung der Verfügbarkeitskontrolle mittels einem mehrstufigem Sicherungskonzept, dass u. a. die Echtzeit sowie Verzögerte Replikation der Datenbanken vorsieht und in dessen Rahmen tägliche Snapshots der Datenbanken gemacht werden. Außerdem existiert eine Notfallplanung zur Prävention und Bewältigung von Notfällen, Brandschutzmaßnahmen im Serverraum; Temperaturüberwachung der Server, Failover für die Serverinfrastruktur, Klimatisierung des Serverraums; unterbrechungsfreie Stromversorgung, Einsatz von Virenscannern, Einsatz von USV- und RAID-Systemen.

Trennungskontrolle, d.h. es ist dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
Der Auftragnehmer gewährleistet die Einhaltung der Trennungskontrolle durch ein entsprechendes Datenmodell und Datenbank-Konzept.

RED Medical wird insbesondere sicherstellen, dass Daten gegen unberechtigte oder versehentliche Zerstörung, versehentlichen Verlust durch technische Mängel, Verfälschung, Diebstahl, unberechtigte Veränderung oder Vervielfältigung sowie andere Formen von unberechtigtem Zugang und unberechtigter Nutzung geschützt werden. Sie wird Datensicherungs- und Backup-Konzepte umsetzen, die einen Schutz der Daten vor Verlust durch systembedingte Störungen sicherstellen.

Darüber hinaus liegen folgende Maßnahmen ebenfalls in der Verantwortung von RED Medical:

Eingabekontrolle, d.h. es ist dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Der Auftragnehmer gewährleistet die Eingabekontrolle durch entsprechende Logging-Mechanismen seitens der Applikationen.

Pseudonymisierung, d. h. Daten werden vom Auftraggeber nur in pseudonymisierter Form zur Verfügung gestellt.

Auftragskontrolle, d.h. es ist dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers von RED Medical verarbeitet werden können. Der Auftragnehmer gewährleistet die Auftragskontrolle durch entsprechende Logging-Mechanismen seitens der Applikationen.

Verfahrensverzeichnis: RED Medical führt ein Verzeichnis der Verfahren gem. Art. 30 DSGVO. Dieses Verzeichnis enthält u. a. die Prozesse der Datenverarbeitung, ein Löschkonzept sowie die Umsetzung der Melde- und Auskunftsverpflichtungen. Neben der Geschäftsleitung zeigen sich die Mitarbeiter verantwortlich für die Umsetzung der Verfahren und die Wahrung der Betroffenenrechte. Als zentrale E-Mail-Adresse steht für Anfragen info@redmedical.de zur Verfügung. Dieses Verfahrensverzeichnis wird regelmäßig überprüft und ggf. an technische oder organisatorische Änderungen angepasst. Die Mitarbeiter werden in regelmäßigen Schulungen über die Vorgaben der DSGVO informiert.

Datenschutzkonzept: Das Datenschutzmanagement-System des Auftragnehmers gewährleistet, dass die getroffenen Maßnahmen regelmäßig auf Sicherheit und Zweckerfüllung im Hinblick auf den jeweiligen Stand der Technik überprüft werden. Die Mitarbeiter des Auftragnehmers werden zur Geheimhaltung und Vertraulichkeit verpflichtet und in Schulungen über aktuelle Themen informiert. Der Auftragnehmer definiert in Richtlinien den Umgang mit personenbezogenen Daten. Ein Datenschutzbeauftragter ist bestellt und es findet eine regelmäßige Überprüfung der getroffenen Maßnahmen und des Verfahrensverzeichnis statt. Bei Änderungen der Prozesse wird der externe Datenschutzbeauftragte in der Planung einbezogen, so dass eine DSGVO-konforme Ausgestaltung gewährleistet ist. Die Umsetzung des Datenschutzmanagement-Systems wird in jährlichen Berichten dokumentiert.

Anlage 3 - Technische Hinweise zum Videosprechstunden-System
Das zertifizierte Videosprechstunden-System des Auftragnehmers bietet den höchsten Sicherheitsstandard für Videokonferenzen. Die Verbindungen werden direkt zwischen den Endgeräten der Gesprächsteilnehmer (peer-to-peer) hergestellt. Die gesamte Videokonferenz wird dabei Ende-zu-Ende verschlüsselt. Somit ist technisch ausgeschlossen, den Datenstrom mitzulesen oder zu speichern. Alle Personen-identifizierenden Daten werden zusätzlich clientseitig mit einem Schlüssel verschlüsselt, den nur der Auftraggeber kennt.