Auftragsverarbeitung nach Art. 28 DSGVO

Vereinbarung

zwischen

Musterkrankenhaus

Beispielstraße 123

45678 Musterhausen

– Verantwortlicher, nachfolgend „Auftraggeber“ genannt –

und

MEDLINQ Softwaresysteme GmbH

Wentorfer Straße 62

21029 Hamburg

– Auftragsverarbeiter, nachfolgend „Auftragnehmer“ genannt –

Auftraggeber und Auftragnehmer jeweils einzeln als „Partei“ und gemeinsam als „Parteien“ bezeichnet.

1. Vertragsgegenstand

Im Rahmen der Leistungserbringung ist es erforderlich, dass der Auftragnehmer als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO fungiert (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Hauptvertrag zwischen dem Auftraggeber und dem Auftragsverarbeiter (im folgenden „Hauptvertrag“ genannt) beschriebenen Auftragsverarbeitung ergeben. Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen können.

2. Art und Zweck, Dauer der Auftragsverarbeitung

2.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nur nach Weisung des Auftraggebers. Der Auftraggeber bleibt gemäß Art. 5 Abs. 2 DSGVO im datenschutzrechtlichen Sinn Verantwortlicher („Herr der Daten“).

2.2 Die Verarbeitung der Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erfolgt entsprechend den in **Anlage 1** zu diesem Vertrag enthaltenen Festlegungen zu Art und Zweck der Verarbeitung. Sie bezieht sich auf die in **Anlage 1** festgelegte Art der Auftraggeber-Daten und auf die dort bestimmten Kategorien betroffener Personen.

2.3 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau in Bosnien und Herzegowina wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c) und d) DSGVO).

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

3. Weisungsrechte des Auftraggebers

3.1 Der Auftragnehmer verwendet die Auftraggeber-Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie abschließend in den Bestimmungen dieses Vertrags Ausdruck finden. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens.

3.2 Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt, wird er den Auftraggeber möglichst zeitnah darauf hinweisen. Außerdem ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen.

3.3 Soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist, die personenbezogenen Daten auch ohne Weisung des Auftraggebers zu verarbeiten, teilt der Auftragnehmer dem Auftraggeber die entsprechenden rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.4 Weisungen des Auftraggebers sind mindestens in Textform (z. B. E-Mail) zu erteilen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform (z. B. E-Mail).

3.5 Sofern gegen den Auftragnehmer wegen eines Verstoßes gegen die DSGVO Ansprüche auf Zahlung von Schadenersatz gemäß Art. 82 DSGVO geltend gemacht werden, ohne dass der Auftragnehmer gegen eine vom Auftraggeber erlassene Weisung verstoßen hat, stellt der Auftraggeber den Auftragnehmer auf erstes Anfordern von allen Ansprüchen frei. Der Auftraggeber übernimmt hierbei auch die Kosten der notwendigen Rechtsverteidigung des Auftragnehmers einschließlich sämtlicher Gerichts- und Anwaltskosten. Die Freistellungspflicht gilt nicht, soweit eine Weisung rechtswidrig und dies für den Auftragnehmer offensichtlich war oder der Schadenersatzanspruch auf die Verletzung einer speziell den Auftragsverarbeitern auferlegten Pflicht aus der DSGVO gestützt wird.

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

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

4.3 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.4 Soweit sich der Auftragnehmer gegen einen Anspruch auf Schadenersatz nach Art. 82 DSGVO, gegen ein drohendes oder bereits verhängtes Bußgeld nach Art. 83 DSGVO oder sonstige Sanktionen im Sinne des Art. 84 DSGVO mit rechtlichen Mitteln verteidigen will, erlaubt der Auftraggeber dem Auftragnehmer Details der Auftragsverarbeitung inklusive erlassener Weisungen zum Zweck der Verteidigung offenzulegen.

4.5 Der Auftraggeber unterstützt den Auftragnehmer bei Kontrollen durch eine Aufsichtsbehörde, bei Ordnungswidrigkeits- oder Strafverfahren, bei der Geltendmachung eines Haftungsanspruchs einer betroffenen Person oder eines Dritten oder bei der Geltendmachung eines anderen Anspruchs im Rahmen des Zumutbaren und Erforderlichen, soweit ein Zusammenhang mit dieser Auftragsverarbeitung besteht.

4.6 Der Auftraggeber stellt dem Auftragnehmer eine verschlüsselte Fernwartung nach dem aktuellen Stand des technischen Fortschrittes zur Verfügung, um Support auf den Systemen des Auftraggebers durchzuführen.

4.7 Der Auftraggeber weißt seine Mitarbeiter oder Beauftragte Dritte an, keine personengebunden Daten an den Auftragnehmer außerhalb verschlüsselter Kommunikationswege zu übertragen, sofern eine Übertragung an den Auftragnehmer überhaupt notwendig ist und im jeweiligen Einzelfall zwischen den beiden Parteien vereinbart wurde. Der Auftragnehmer stellt dem Auftraggeber ein verschlüsseltes Supportportal zur Verfügung, über das im Einzelfall und nach vorheriger beidseitiger Zustimmung, Daten übertragen werden können.

5. Pflichten des Auftragnehmers

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

5.2 Der Auftragnehmer unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde, bei Ordnungswidrigkeits- oder Strafverfahren, bei der Geltendmachung eines Haftungsanspruchs einer betroffenen Person oder eines Dritten oder bei der Geltendmachung eines anderen Anspruchs im Rahmen des Zumutbaren und Erforderlichen, soweit ein Zusammenhang mit dieser Auftragsverarbeitung besteht.

5.3 Der Auftragnehmer hat die bei der Verarbeitung von Auftraggeber-Daten beschäftigten Personen gemäß Art. 28 Abs. 3 Satz 2 lit. b) DSGVO schriftlich auf die Vertraulichkeit zu verpflichten und sie zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut zu machen. Dies ist nicht erforderlich, wenn die bei der Verarbeitung von Auftraggeber-Daten beschäftigten Personen bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Bei der Durchführung der Arbeiten der Gesundheitsdaten betreffend setzt der Auftragnehmer nur Beschäftigte ein, die auf die ärztliche Schweigepflicht gemäß § 203 StGB belehrt und verpflichtet wurden.

5.4 Sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind, ist der Auftragnehmer verpflichtet, einen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis fachkundigen, für die Aufgaben nach Art. 39 DSGVO fähigen und zuverlässigen betrieblichen Datenschutzbeauftragten schriftlich zu bestellen, der seine Tätigkeit gemäß Art. 38, 39 DSGVO und § 38 Abs. 2 BDSG ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mindestens in Textform (z. B. E-Mail) mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt. Sollte keine Bestellpflicht für einen betrieblichen Datenschutzbeauftragten bestehen, benennt der Auftragnehmer gegenüber dem Auftraggeber mindestens in Textform (z. B. E-Mail) einen Ansprechpartner für datenschutzrechtliche Belange und teilt dem Auftraggeber dessen Kontaktdaten mit. Sollte der Auftragnehmer seinen Sitz außerhalb der EU haben, benennt er gegenüber dem Auftraggeber einen Vertreter nach Art. 27 Abs. 1 DSGVO in der EU und teilt dem Auftraggeber dessen Kontaktdaten mit. Der vom Auftragnehmer bestellte betriebliche Datenschutzbeauftragte ist:
RA David Oberbeck, Datenschutzkanzlei
Hallerstraße 76, 20146 Hamburg, Telefon 040 228691140, E-Mail

datenschutz@medlinq.com

5.5 Der Auftragnehmer unterliegt der behördlichen Aufsicht nach § 40 BDSG sowie den Bußgeld- und Strafvorschriften in § 42, 43 BDSG sowie in Art. 83 Abs. 4-6 DSGVO nach Maßgabe von § 41 BDSG.

5.6 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der nach **Anlage 2** zu treffenden technischen und organisatorischen Maßnahmen im Rahmen der Kontrollrechte nach Ziffer 8 dieses Vertrages nachzuweisen.

6. Technische und organisatorische Maßnahmen

6.1 Der Auftragnehmer hat vor Beginn der Verarbeitung der Auftraggeber-Daten die in **Anlage 2** dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c), Art. 32 DSGVO zu implementieren und während des Vertrags aufrechtzuerhalten. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

6.2 Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in **Anlage 2** festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers und sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

7. Unterstützung des Auftragnehmers zur Einhaltung der Pflichten des Auftraggebers nach Art. 32-36 DSGVO

7.1 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Hierzu gehören

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

b) die Unterstützung des Auftraggebers im Falle einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 DSGVO,

c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht nach Art. 34 DSGVO gegenüber einem Betroffenen zu unterstützen,

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzungen i. S. d. Art. 35 DSGVO,

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde nach Art. 36 DSGVO.

7.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Hauptvertrages enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

8. Kontrollrechte des Auftraggebers

8.1 Der Auftraggeber ist berechtigt, im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers, in denen Auftraggeber-Daten verarbeitet werden, zu betreten, um sich von der Einhaltung der aus dieser Vereinbarung ergebenden Pflichten, insbesondere der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** zu diesem Vertrag, zu überzeugen. Der Auftragnehmer weist dem Auftraggeber auf Anforderung die Umsetzung der technischen und organisatorischen Maßnahmen nach.

8.2 Der Auftragnehmer gewährt dem Auftraggeber die zur Durchführung der Kontrollen nach Ziffer 8.1 erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.

8.3 Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

8.4 Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 8 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.

8.5 Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** anstatt einer Vor-Ort-Kontrolle auch durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren nach Art. 42 DSGVO, 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 durch IT-Sicherheits- oder Datenschutzaudit – z. B. nach

BSI-Grundschutz – („Prüfungsbericht“) 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.

8.6 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

9. Unterauftragsverhältnisse

9.1 Der Auftragnehmer darf Unterauftragsverhältnisse (Unterauftragnehmer) hinsichtlich der Verarbeitung oder Nutzung von Auftraggeber-Daten begründen. Zurzeit sind für den Auftragnehmer die in **Anlage 3** mit Namen, Anschrift und Auftragsinhalt bezeichneten Unterauftragnehmer beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragnehmers. Sofern der Auftraggeber keine Einwände gegen neue Unterauftragnehmer innerhalb von 2 Wochen ab Zugang der Mitteilung über den neuen Unterauftragnehmer erhebt, gilt dessen Einschaltung als durch den Auftraggeber genehmigt.

9.2 Nicht als Unterauftragsverhältnis im Sinne dieser Regelung 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 sofern dabei keine personenbezogenen Daten verarbeitet werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

9.3 Die Verpflichtung des Unterauftragnehmers muss schriftlich erfolgen, was auch in einem elektronischen Format erfolgen kann (z. B. E-Mail). Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer stellt bei jeder Unterbeauftragung sicher, dass die in Art. 28 Abs. 2 und Abs. 4 DSGVO genannten Bedingungen eingehalten werden.

9.4 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Die Ausübung der Kontrollrechte des Auftraggebers nach Ziffer 8 muss gegenüber dem Unterauftragnehmer grundsätzlich möglich sein. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, von dem Auftragnehmer Auskunft über den datenschutzwesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

9.5 Die Regelungen in dieser Ziffer 9 gelten auch, wenn ein Unterauftragnehmer in einem Drittstaat eingeschaltet wird. Der Auftragnehmer stellt in einem solchen Fall die datenschutzrechtliche Zulässigkeit durch geeignete Rechtsinstrumente, beispielsweise EU-Standardvertragsklauseln, sicher.

Der Auftragnehmer hat zur Sicherheit der personenbezogenen Daten des Auftraggebers geeignete Garantien in Form von Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c) bzw. d) DSGVO vorgesehen. Der Auftraggeber ermächtigt hiermit den Auftragnehmer dazu, Standarddatenschutzklauseln gem. Art. 46 Abs. 2 lit. c) bzw. d) DSGVO als Vertreter im Namen des Auftraggebers abzuschließen. Zu diesem Zweck befreit der Auftraggeber den Auftragnehmer von der Beschränkung des § 181 BGB bei der Unterzeichnung der Standardvertragsklauseln.

9.6 Die Weitergabe von Auftraggeber-Daten an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

10. Rechte der Betroffenen

10.1 Die Rechte der durch die Datenverarbeitung betroffenen Personen nach Kapitel 3 DSGVO (Art. 12-23 DSGVO) unter Berücksichtigung von Teil 2, Kapitel 2 BDSG (§§ 32-37 BDSG), insbesondere auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch der gespeicherten Auftraggeber-Daten, sind gegenüber dem Auftraggeber geltend zu machen.

10.2 Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks der unter Ziffer 10.1 aufgeführten Rechte wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

10.3 Für den Fall, dass eine betroffene Person ihre Rechte im Sinne von Ziffer 10.1 geltend macht, hat der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Ansprüche angesichts der Art der Verarbeitung in angemessenem und für den Auftraggeber erforderlichen Umfang mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen.

10.4 Der Auftragnehmer wird es dem Auftraggeber ermöglichen, Auftraggeber-Daten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

11. Rückgabe und Löschung überlassener Daten und Datenträger

11.1 Der Auftragnehmer hat sämtliche Auftraggeber-Daten nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Hauptvertrags) oder früher nach Aufforderung durch den Auftraggeber datenschutzgerecht zu löschen und von dem Auftraggeber erhaltene Datenträger, die zu diesem Zeitpunkt noch Auftraggeber-Daten enthalten, an den Auftraggeber zurückzugeben. Gleiches gilt für Test- und Ausschussmaterial. Dies gilt nicht, sofern nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

11.2 Für personenbezogene Daten, die nicht hauptsächlich zur Verarbeitung überlassen wurden, sondern nur der Behebung von Softwarefehlern dienen, wird hinsichtlich der Löschung folgendes vereinbart: Widerspricht der Auftraggeber im Einzelfall nicht, dann löscht der Auftragnehmer diese personenbezogenen Daten 72 Stunden nach erfolgreicher Behebung des Fehlers, ohne dass es einer weiteren Information des Auftragsgebers bedarf.

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

11.4 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.

12. 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.

13. Kirchliches Datenschutzgesetz (KDG)

Fällt der Auftraggeber in den Zuständigkeitsbereich des Kirchlichen Datenschutzes (KDG), dann gilt anstelle der Datenschutzgrundverordnung das Gesetz über den Kirchlichen Datenschutz (KDG). Sofern im vorliegenden Vertrag auf Vorschriften der DSGVO verwiesen wird, sind sich die Parteien daher einig, dass an deren Stelle die entsprechenden Normen des KDG gemeint sind.

14. Vorrangklausel

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

	Hamburg,
_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer

Anlagen:

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen
Anlage 2: Technische und organisatorische Maßnahmen
Anlage 3: Unterauftragnehmer
Anlage 4: Meldewege

Anlage 1: Art und Zweck der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen

In der folgenden Aufstellung werden alle Produkte der MEDLINQ Softwaresysteme GmbH mit der Art und dem Zweck der Datenverarbeitung aufgeführt. Welche Produkte der MEDLINQ Softwaresysteme GmbH im Einzelnen beim Kunden verwendet werden, und für die die hier vorliegende Auftragsverarbeitung nach Art. 28 Datenschutz-Grundverordnung (DSGVO) gilt, ergibt sich aus dem Hauptvertrag mit Aufstellung der eingesetzten Produkte.

Übersicht Produkte der MEDLINQ Softwaresysteme GmbH:

- MEDLINQ-Anästhesie Classic und MEDLINQ-Anästhesie Online
- MEDLINQ-Intensiv Classic
- MEDLINQ-Schmerzvisite Online
- MEDLINQ-Notarzt Classic
- MEDLINQ-Befragung Classic
- MEDLINQ-Schnittstelle
- MEDLINQ-Speisenversorgung Classic & MEDLINQ-Speisenversorgung Suite
  - MEDLINQ-Kasse
  - MEDLINQ-Küche
  - MEDLINQ-Einkaufsportal/Webshop
- MEDLINQ-BD-online
- MEDLINQ-PP-online

Art und Zweck der Datenverarbeitung:

Für die Produkte MEDLINQ-Anästhesie Classic und MEDLINQ-Anästhesie Online, MEDLINQ-Intensiv Classic, MEDLINQ-Schmerzvisite Online, MEDLINQ-Notarzt Classic erfolgt eine Datenverarbeitung bezogen auf die Behandlung von Patienten des Auftraggebers.

Art der personenbezogenen Daten:

<u>Patienten-/Gesundheitsdaten:</u>

Name, Geburtsdatum, Geschlecht, Größe, Gewicht, Adressdaten, Vitalparameter, Medikationsdaten, Anamnese, Narkosedaten, Behandlungsdaten und Behandlungsplan mit Op-Daten, abrechnungssrelevante Daten (Controlling)

<u>Personen-/Mitarbeiterdaten:</u>

Name, Geburtsdatum, Stations- und Organisationszugehörigkeit mit Firmenadressdaten, Berufliche Qualifikation, Benutzerberechtigungen, Kontaktdaten mit E-Mail, Telefon, Fax

Kategorien betroffener Personen:

Patienten des Auftraggebers und Mitarbeiter und Angestellte des Auftraggebers

Art und Zweck der Datenverarbeitung:
Für das Produkt MEDLINQ-Befragung Classic erfolgt eine Datenverarbeitung bezogen auf die Qualitäts- und Zufriedenheitsbefragung von Patienten des Auftraggebers.
Art der personenbezogenen Daten:
Patienten-/Gesundheitsdaten: Name, Geburtsdatum, Behandlungsaufenthalt, Fragen zur Zufriedenheit bezüglich der Behandlung und des Aufenthalts Personen-/Mitarbeiterdaten: Name, Geburtsdatum, Stations- und Organisationszugehörigkeit mit Firmenadressdaten, Benutzerberechtigungen, Kontaktdaten mit E-Mail, Telefon, Fax
Kategorien betroffener Personen:
Patienten des Auftraggebers und Mitarbeiter und Angestellte des Auftraggebers

Art und Zweck der Datenverarbeitung:
Für das Produkt MEDLINQ-Schnittstelle erfolgt eine Datenverarbeitung bezogen auf die Patientendaten für weitere MEDLINQ-Produkte des Auftraggebers.
Art der personenbezogenen Daten:
Patienten-/Gesundheitsdaten: Name, Geburtsdatum, Behandlungsaufenthalt mit Stationszugehörigkeit, Verlegungen, Entlassungen, Kostform des Patienten Personen-/Mitarbeiterdaten: Name, Geburtsdatum, Stations- und Organisationszugehörigkeit mit Firmenadressdaten, Benutzerberechtigungen, Kontaktdaten mit E-Mail, Telefon, Fax
Kategorien betroffener Personen:
Patienten des Auftraggebers und Mitarbeiter und Angestellte des Auftraggebers

Art und Zweck der Datenverarbeitung:

Für die Produkte MEDLINQ-Speisenversorgung Classic und MEDLINQ-Speisenversorgung Suite

- MEDLINQ-Kasse
- MEDLINQ-Küche
- MEDLINQ-Einkaufsportal/Webshop

erfolgt eine Datenverarbeitung bezogen auf Patientendaten und Kundendaten für Bestell- und Zahlungsvorgänge des Auftraggebers.

Art der personenbezogenen Daten:

Patienten-/Gesundheitsdaten:

Name, Geburtsdatum, Behandlungsaufenthalt mit Stationszugehörigkeit, Verlegungen, Entlassungen, Kostform des Patienten, Diätetik mit geplanten Ernährungswerten, bestellte und verzehrte Mahlzeiten, Zahlungsdaten

Personen-/Mitarbeiterdaten:

Name, Geburtsdatum, Stations- und Organisationszugehörigkeit mit Firmenadressdaten, Benutzerberechtigungen, Kontaktdaten mit E-Mail, Telefon, Fax, Zahlungsdaten

Kundendaten:

Name, Zahlungsdaten, Kontakt- und Zugangsdaten bei externen Bestellungen

Kategorien betroffener Personen:

Patienten des Auftraggebers, Mitarbeiter und Angestellte des Auftraggebers, externe Kunden des Auftraggebers

Art und Zweck der Datenverarbeitung:
Für die Produkte MEDLINQ-BD-online und MEDLINQ-PP-online erfolgt eine Datenverarbeitung bezogen auf die Dienstplanung von Angestellten oder Mitgliedern (niedergelassene Ärzte) des Auftraggebers.
Art der personenbezogenen Daten:
Mitglieder (niedergelassene Ärzte) Name, Geburtsdatum, Adress- und Kontaktdaten mit E-Mail, Telefon, Fax, Benutzerberechtigungen, Dienstplanungstermine, Abrechnungsdaten Personen-/Mitarbeiterdaten: Name, Geburtsdatum, Adress- und Kontaktdaten mit E-Mail, Telefon, Fax, Benutzerberechtigungen, Dienstplanungstermine, Abrechnungsdaten
Kategorien betroffener Personen:
Mitarbeiter, Angestellte und Mitglieder des Auftraggebers

Anlage 2: Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Zutrittskontrolle
Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

- Zutrittskontrollsystem mit interner Dienstanweisung
- Schlüssel/Schlüsselvergabe zentral geregelt
- Türsicherung, Elektronische Türöffner
- Überwachungseinrichtung, Alarmanlage, Videoüberwachung
- Empfang von Besuchern
- Besucher/Externe werden begleitet bzw. abgeholt und stets beaufsichtigt
- Sicherheitsdienst
- Videoüberwachung mit Aufzeichnung an der Eingangstür

Zugangskontrolle/Verschlüsselung
Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von mobilen Datenträgern (Hardwareverschlüsselung)
- Abschottung des Netzwerkes gegen ungewollte Zugriffe von außen (Firewall)
- Zugang ist besonders gesichert (Verschlüsselung, VPN)
- Alle IT-Programme laufen auf dem eigenen Server im Rechenzentrum (Housing) oder eigene Server im Hetzner-Rechenzentrum
- Antivirenschutz aller Clients und Server
- Es wird sichergestellt, dass nach Ausscheiden eines Mitarbeiters bekannte Passwörter geändert werden
- *Hinweis: Der zur Verfügung stehende Supportzugang zum Kunden ist teilweise nicht personalisiert, sondern es wurde ein Firmenzugang durch den Kunden für die Firma MEDLINQ GmbH vergeben*

Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

- internes Berechtigungskonzept mit Zugriffsbefugnissen (Profile, Rollen, Transaktionen und Objekte)
- Checklisten für Einrichtung, Abmeldung und Sperrung von Benutzerkonten und anderen Zugängen
- Zugriffsberechtigungen werden aufgabenbezogen und nach dem Need-to-know-Prinzip erteilt
- Regelmäßige Überprüfung der Zugriffsberechtigungen. Nicht mehr erforderliche Berechtigungen werden unverzüglich entzogen
- Daten auf mobilen IT-Systemen sind verschlüsselt (komplettes System, Hardwareverschlüsselung)
- Aufzeichnung von Zugriffen auf das IT-System

- *Hinweis: Der zur Verfügung stehende Fernwartungszugang ist durch den Kunden an die Firma MEDLINQ GmbH vergeben und vorgegeben.*

Trennungskontrolle/Zweckbindungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- "Interne Mandantenfähigkeit" der eingesetzten und entwickelten Softwaresysteme/ Zweckbindung
- Funktionstrennung/Produktion-/Beta-/Testsysteme

Physikalische Sicherheit
Sämtliche personenbezogenen Daten sind nur auf dem externen Server eines Unterauftragnehmers gespeichert (z. Zt. Hetzner Online GmbH).

- Physisch getrennte Speicherung
- Überspannungsschutz
- Notstromversorgung
- Brandmeldeanlage
- Klimatisierte Serverräume
- Löschtechnik (z. B. Elektronisches Feuerlösch-System)

2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

Weitergabekontrolle
Maßnahmen, die gewährleisten, 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Verschlüsselung/Tunnelverbindung (VPN = Virtual Private Network)
- Protokollierung
- Transportsicherung
- Datenspeicherung und -verarbeitung erfolgt auf IT-Systemen im Rechenzentrum. Verbindung zwischen Clients und Server ist besonders gesichert (Verschlüsselung, VPN)
- Mitbringen und Verwenden privater Datenträger ist untersagt. Es dürfen nur verschlüsselte betriebliche Datenträger genutzt werden
- Kontrollierte Vernichtung von Datenträgern mit Protokollierung (physische Vernichtung, zertifizierter Entsorger)
- Besucher haben keinen Zugriff auf betriebliches LAN/WLAN – getrenntes Gäste-WLAN

Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

- automatisierte Protokollierung der Dateneingabe, Änderung oder Löschung je nach eingesetztem Verfahren
- Dokumentation der Eingabeprogramme
- Sicherung der Protokolldaten gegen Verlust oder Veränderung in bestehenden

Serversicherungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO), rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DSGVO

Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers):

- Notfallkonzept (Dokumentation zur Datensicherung und Ausfallsicherheit)
- Backup-Verfahren, Spiegeln von Festplatten (RAID-Verfahren) und Backup-Rechenzentrum
- Versionierte Daten- und Systembackups nach Backup-Plan (täglich/wöchentlich/monatlich).
- Getrennte Aufbewahrung
- Schadsoftwareschutz. Sicherheitsrelevante Updates und Patches werden regelmäßig und zeitnah eingespielt
- Erhaltene und auszuliefernde Datenträger werden Schadsoftwarecheck unterzogen
- Unterbrechungsfreie Stromversorgung (USV)
- MEDLINQ gestaltet die Softwareprodukte derart, dass eine rasche Wiederherstellung unter Nutzung technischer Möglichkeiten sichergestellt ist. Die Durchführung der Wiederherstellung ist nicht Bestandteil dieser TOMs.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO, Art. 25 Abs. 1 DSGVO)

Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können:

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Auftragsformular)
- Kriterien zur Auswahl der Auftragnehmer. Auftragnehmer werden sorgfältig ausgesucht
- Klare und unzweifelhafte vertragliche Regelungen zur Datenverarbeitung
- Kontrolle des Auftragnehmers durch die Geschäftsführung oder den Datenschutzbeauftragten
- Kontrolle der Vertragsausführung
- Pflicht zur Vorbewertung

Datenschutz-Management

- Internes Datenschutz- und Sicherheitskonzept ist vorhanden (DSMS)
- Innerhalb von Dienstanweisung weitere Regelungen zu Umgebung und Anwendung
- Regelmäßige interne Audits und Kontrollen
- Datenschutzfreundliche Voreinstellungen
- Mitarbeiterschulungen
- Verschwiegenheitsverpflichtungen der Mitarbeiter
- Vernichtung von Papierdokumenten und -akten
- Verschlüsselung von E-Mails und ihrer Anhänge
- Richtlinien zur Aufbewahrung, Löschung und Sperrung von personenbezogenen Daten
- Dokumentation der schriftlichen Weisungen für Auftragnehmer

• Dokumentationen von Weisungen
5. Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO, Art. 25 Abs. 1 DSGVO) Maßnahmen, die gewährleisten, dass personenbezogene Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.
• Nutzung von Referenzlisten und Kennnummern, wenn personenbezogene Bearbeitung nicht erforderlich ist.

Anlage 3: Unterauftragnehmer			
Name	**Anschrift/Land**	**Auftragsinhalt**	**Vertrag**
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen, Deutschland	Rechenzentrum	AV
Inmedias.it GmbH	Friedensallee 25, 22765 Hamburg, Deutschland	Server-, Client- und Fernwartungsbetreuung (technischer helpdesk)	AV
Dr. Thomas Bogner	Hermelinweg 11, 22159 Hamburg, Deutschland	Softwareentwicklung im Bereich Anästhesie Online	AV
Otto Dörner GmbH & Co. KG	Lederstraße 24, 22525 Hamburg, Deutschland	Aktenvernichtung und Entsorgung	AV
MSS Medical Softwerk Solutions d.o.o.	Jevrejska 24, 78000 Banja Luka, Bosnien und Herzegowina	Softwareentwicklungen und Softwaretests für alle Produkte, Support für den Bereich Speisenversorgung und Anästhesie Online	Standardvertrags-klauseln 12.2021 TIA 12.2023

Stand: 08.01.2024

Anlage 4: Meldewege

Mängelmeldungen können auf folgenden Wegen an MEDLINQ gemeldet werden:

Telefonisch

Unsere telefonische Hotline ist für die verschiedenen Produkte unter folgenden Rufnummern zu erreichen:

MEDLINQ-Anästhesie Classic MEDLINQ-Intensiv Classic	040 416266-200
MEDLINQ-Anästhesie Online	040 416266-210
MEDLINQ-Küche MEDLINQ-Einkaufsportal MEDLINQ-Kasse	040 416266-220
MEDLINQ-BD-online MEDLINQ-PP-online	040 416266-230
MEDLINQ-Schmerzvisite Online	040 416266-211
MEDLINQ-Schnittstelle	040 416266-240

Per E-Mail

Sie erreichen unseren Produktsupport unter folgenden E-Mail-Adressen:

MEDLINQ-Anästhesie Classic MEDLINQ-Intensiv Classic	anaesthesie-classic@medlinq.com its-classic@medlinq.com
MEDLINQ-Anästhesie Online	anaesthesie-online@medlinq.com
MEDLINQ-Küche MEDLINQ-Einkaufsportal MEDLINQ-Kasse	kueche@medlinq.com einkaufsportal@medlinq.com kasse@medlinq.com
MEDLINQ-BD-online MEDLINQ-PP-online	bdonline@medlinq.com pponline@medlinq.com
MEDLINQ-Schmerzvisite Online	schmerzvisite@medlinq.com
MEDLINQ-Schnittstelle	schnittstelle@medlinq.com

Per Post

MEDLINQ Softwaresysteme GmbH
- Produktsupport -
Wentorfer Straße 62
21029 Hamburg