On-Lab GmbH ° Heinrich Hertz Str. 8 ° 77656 Offenburg

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

On-Lab GmbH
Heinrich-Hertz-Str. 8
77656 Offenburg

- nachfolgend "Auftragnehmer "genannt -

und (komplette Anschrift eintragen)

- nachfolgend "Auftraggeber" genannt –

Inhaltsverzeichnis

1. Gegenstand und Dauer des Auftrags 3
(1) Gegenstand 3
(2) Dauer 3
2. Konkretisierung des Auftragsinhalts 3
(1) Art und Zweck der vorgesehenen Verarbeitung von Daten 3
(2) Art der Daten 3
(3) Kategorien betroffener Personen 3
3. Technisch-organisatorische Maßnahmen 3
4. Berichtigung, Einschränkung und Löschung von Daten 4
5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers 4
6. Unterauftragsverhältnisse 5
7. Kontrollrechte des Auftraggebers 5
8. Dienstleistungen über Fernzugriffe 6
9. Mitteilung bei Verstößen des Auftragnehmers 6
10. Weisungsbefugnis des Auftraggebers 7
11. Löschung und Rückgabe von personenbezogenen Daten 7
12. Gültigkeitserweiterung 7
Anlage 1 9
Anlage 2 - Technisch-organisatorische Maßnahmen 9
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) 9
2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO) 10
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO) 10
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO) 10

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: elektronische Übermittlung digitaler Dokumente mit medizinischem Inhalt

(2) Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 6 Monaten beiderseitig gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftraggeber nutzt Systemkomponenten des Auftragnehmers zwecks Zustellung end-to-end-verschlüsselter, personenbezogener Daten zum Nachrichtenempfänger.

Der Auftragnehmer hat keinerlei Möglichkeiten der Entschlüsselung und Einsicht in die Daten.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in *Deutschland entspricht dem EU-DSGVO.*

(2) Art der Daten

Die Art der verwendeten personenbezogenen Daten ist in der **Anlage 1** aufgelistet.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der **Anlage 1** aufgelistet.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung dokumentiert und stehen dem Auftraggeber in **Anlage 2** zur Prüfung zu Verfügung. Die dokumentierten Maßnahmen werden Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der

Vertraulichkeit, der 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 unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in **Anlage 2**].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer hat keinerlei Einfluss und Einsicht in die vom Auftraggeber veranlassten Vorgänge.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Datenschutzbeauftragten beim Auftragnehmer ist Frau Christine Seebach, 06301.3890015 bestellt.

2. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

3. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in **Anlage 2**].

4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits-oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

6. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

7. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard-und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach Vorliegen einer entsprechenden Vereinbarung zur Auftragsdatenverarbeitung beauftragen.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht vorgesehen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Einvernehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

(4) Für die Ermöglichung von Kontrollen und Nachweis solcher Maßnahmen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Alle durch dritte anfallenden Kosten sind in jedem Fall vom Auftraggeber zu begleichen.

8. Dienstleistungen über Fernzugriffe

Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen sind nur Personen autorisiert, die eine im Arbeitsvertrag verankerte Datenschutzerklärung zur Geheimhaltungsverpflichtung unterzeichnet haben.

In jedem Fall verpflichtet sich der Auftragnehmer im Zusammenhang mit dem Kontakt zu entsprechenden Daten des Auftraggebers, seine Mitarbeiter auf diejenige Verschwiegenheit zu verpflichten, welche den Ärzten gegenüber deren Patienten selbst obliegt, unter Beachtung insbesondere der Regelung des § 203 StGB (Ärztliche Verschwiegenheit).

Auf Grundlage dieser weitreichenden Verschwiegenheitspflicht des Auftragsnehmers und seiner Mitarbeiter erklärt der Auftragsgeber hiermit die Einwilligung in den bedarfsbezogenen Zugriff des Auftragnehmers auf die beim Auftraggeber installierten Systemkomponenten des Auftragnehmers und Netzwerke zum Zwecke der Fernwartung. Eine Dokumentation des Zugriffs ist nicht erforderlich, sofern kein Zugriff und/oder Veränderung personenbezogener Daten erforderlich ist.

Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

9. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

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 Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

10. Weisungsbefugnis des Auftraggebers

(1) Weisungen durch den Auftraggeber sind in schriftlicher Form zulässig, sofern sie nicht den vertragsbedingten Ablauf der Datenverarbeitung behindern und gegen Datenschutzvorschriften verstoßen. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber dahingehend geändert wird.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12. Gültigkeitserweiterung

Vorstehende Vereinbarung gilt zusätzlich zu unter 'Auftraggeber' genanntem Standort für folgende weitere Standorte, für die der Auftraggeber zeichnungsberechtigt ist:

Anschrift Standort _____

Anschrift Standort _____

Anschrift Standort _____

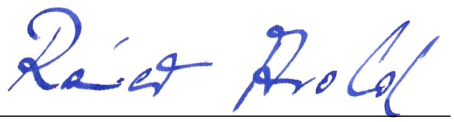
Anschrift Standort _____

Anschrift Standort _____

Anschrift Standort _____

Ort, Datum

Unterschrift des Auftraggebers



Offenburg, den 07.02.2019

Anlage 1

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☒ Patientendaten – Gesundheitsdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☒ Benutzerdaten

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Patienten
- ☒ Einweiser / Überweiser
- ☒ Ansprechpartner

Anlage 2 - Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- ✓ Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen durch elektronische Schlüssel, Alarmanlagen, Videoanlagen;

- ✓ Zugangskontrolle
  Keine unbefugte Systembenutzung, durch sichere Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

- ✓ Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

  Die Systemkomponenten des Auftragnehmers werden dem Auftraggeber in einer virtuellen Maschine (Linux-VM) zum Herunterladen von der hompage des Auftragnehmers angeboten und sind mittels eines individuellen Initialisierungs-Codes aktivierbar. Der direkte Zugriff auf die virtuelle Maschine des Auftragnehmers ist vor Fremdeinwirkung geschützt und nur dem Auftragnehmer vorbehalten.

- ✓ Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit

  Empfängerspezifische RSA-end-to-end - Verschlüsselung
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- ✓ Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

- ✓ Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in interne Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden durch Protokollierung, Dokumentenmanagement; externe Feststellung ist nicht erforderlich, da nur automatisierte und keine manuellen Prozesse die Eingabe steuern und im Verantwortungsbereich des Auftraggebers liegen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- ✓ Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

- ✓ Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
  redundante Virtualisierung, Ersatzteil Vorhaltung

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- ✓ Datenschutz-Management
  Zutrittsperre für Unbefugte, Schutz vor unbefugter Einsicht, Vergitterter Serverraum mit elektronischem Zutrittschutz, Alarmanlage mit Bewegungsmelder, Fenster- und Türkontakten

- ✓ Incident-Response-Management
  standortübergreifende, redundante, multi-OS-verteilte Virtualisierung

- ✓ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
  Ende-Zu-Ende Verschlüsselung erfolgt bereits vor dem Versand, d.h. Einblick in personenbezogene Daten durch On-Lab Personal erfolgt nur nach fallbezogener Aufforderung des Auftraggebers