Vereinbarung zur Datenverarbeitung im Auftrag gemäß Art. 28 DS-GVO - Auftragsbedingungen -		
Gegenstand	Verarbeitung pseudonymisierter Telekonsildaten zur Erkenntnisgewinnung und Evaluation der fachlichen und technischen Ausgestaltung des dermatologischen Konsils im Rahmen des Projekts Telederm Interim	
Auftraggeber und Weisungsberechtigter	**Beauftragender Hausarzt** im Rahmen des HZV Vertrags mit der AOK BW im Projekt Telederm Interim	
Auftragnehmer	**Hochschule Reutlingen** Alteburgstraße 150, 72762 Reutlingen	
Auftragsansprechpartner/ Weisungsempfänger beim Auftragnehmer	Projektleitung: Prof. Dr. Christian Thies Alteburgstraße 150, 72762 Reutlingen Mail: Christian.thies@reutlingen-university.de Tel. +49 (0)7121 – 271 4076	Systembetreuung: Sven Dörflinger Alteburgstraße 150, 72762 Reutlingen Mail: Sven.Doerflinger@reutlingen-university.de Tel. +49 (0)7121 – 271 4024

Präambel

1. Der **Auftraggeber** erteilt im Rahmen seiner Teilnahmeerklärung am Projekt den Auftrag an den Auftragnehmer unter Bezug auf diese Auftragsbedingungen.
2. Der **Auftragnehmer** hat sich im Rahmen des Vertrages zwischen den Projektbeteiligten AOK BW und ihm selbst dazu verpflichtet, diese Auftragsbedingungen einzuhalten.

1. Rechtsgrundlage, Anwendungsbereich

1.1 Der Auftragnehmer verarbeitet im Rahmen des Projekts pseudonymisierte, für ihn faktisch anonymisierte Telekonsil-Gesundheitsdaten für den Auftraggeber. Insoweit handelt es sich um eine Auftragsverarbeitung gemäß Art. 28 EU-Datenschutzgrundverordnung (DS-GVO). Die Verarbeitung erfolgt auf Basis einer aufgeklärten Einwilligung der Betroffenen (Art. 9 Abs. 2 lit. a DS-GVO).

1.2 Der Auftraggeber bleibt im Rahmen des Auftrags für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

1.3 Der Auftragnehmer sichert für sich und seine Beschäftigten die Umsetzung/Einhaltung der nachstehenden Punkte im Rahmen der Auftragserledigung verbindlich zu.

1.4 Der Auftragnehmer sichert gemäß Art. 28 Abs. 3 lit. e DS-GVO zu, die in Kapitel 3 DS-GVO genannten Rechte der betroffenen Personen zu beachten und umzusetzen. Er wird im Falle von Anfragen den Auftraggeber bei der Erfüllung seiner Pflichten soweit für den Auftragnehmer zumutbar unterstützen.

1.5 Der Auftragnehmer unterstützt gemäß Art. 28 Abs. 3 lit. f DS-GVO den Auftraggeber bei dessen Pflichten nach Art. 32 bis 36 DSGVO in für ihn zumutbarer Weise.

2. Gegenstand und Umfang der Datenverarbeitung

2.1. Für die Durchführung des dermatologischen Telekonsils werden folgende Daten vom Auftraggeber an den Auftragnehmer übermittelt:

- Pseudonym, Alter und Geschlecht
- Information zur Hautbefund-relevanten Vorgeschichte, sowie Angaben zur aktuellen Problematik
- Falls für die Behandlung relevant, Informationen zum Behandlungsverlauf inkl. Angabe der Medikamente und Überlassung von Untersuchungsergebnissen
- Bildmaterial zum Befund

2.2. Der Auftragnehmer führt für den Auftraggeber folgende Aktivitäten mit den unter 2.1. genannten Daten der Probanden durch. Die Aktivitäten zur Durchführung von Telekonsilen sind im Datenschutzkonzept TeleDerm Interim der HSRT (DS-Konzept TeleDerm Interim) spezifiziert und umfassen unter anderem:

a. Speicherung der Daten für den gesetzlich vorgeschriebenen Zeitraum.
b. Bereitstellung der Daten für registrierte und authentifizierte Dermatologen, die im Rahmen des Projektes die Befundung der Daten übernehmen.
c. Berichterstattung (PDF-Export) nach erfolgter Befundung an den Hausarzt.
d. Übermittlung an die AOK BW wie viele Konsile im Rahmen des o.g. Projektes durchgeführt wurden.
e. Löschung der Daten basierend auf den im Datenschutzkonzept vereinbarten Löschfristen.

2.3. Der Auftragnehmer übernimmt hierbei nur die technischen Verarbeitungsvorgänge, die Bereitstellung von Speicherkapazität, Rechenleistung, die hierfür erforderliche Infrastruktur und die Systembetreuung. Eingesetzte Programme sind vom Auftragnehmer erstellt oder konfiguriert, Verarbeitungsvorgänge werden von Beschäftigten des Auftraggebers angestoßen bzw. durchgeführt.

2.4. Der Auftraggeber beauftragt den Auftragnehmer und dessen hierzu Beschäftigte die faktisch anonymisierten Gesundheitsdaten zu verarbeiten, solange/soweit dies für die obigen Aufgaben erforderlich ist. Es gelten die Vorbehalte/Rahmenbedingungen dieser Vereinbarung.

2.5. Im Rahmen der Auftragserledigung wird die Einhaltung der nachfolgenden technischen und organisatorischen Maßnahmen verbindlich vereinbart.

2.6. Diese Vereinbarung beginnt und endet automatisch mit dem Start und Ende des Projektes „TeleDerm Interim“, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Pflichten oder Kündigungsrechte ergeben.

3. Weisungsrechte des Auftraggebers

3.1 Der Auftragnehmer verpflichtet sich, die Verarbeitung der pseudonymisierten Daten ausschließlich im Rahmen dieses Auftrags oder nach Weisungen des Auftraggebers durchzuführen.

3.2 Der Auftraggeber kann dem Auftragnehmer jederzeit weitere Weisungen hinsichtlich der Verarbeitung seiner personenbeziehbaren Daten erteilen.

4. Technische und organisatorische Maßnahmen (Art.32 DS-GVO)

4.1 Allgemein

a. Der Auftragnehmer (HSRT) hat ein dokumentiertes und implementiertes IT-Sicherheitskonzept.
b. Hierin ist dem koordinierenden Weisungsberechtigungen des Auftraggebers, sowie dem Datenschutzbeauftragten des Auftraggebers, oder einer durch den Auftraggeber genannten dritten juristischen Person zu üblichen Arbeitszeiten Einsicht zu gewähren.
c. Die den Auftragnehmer betreffenden Maßnahmen sind im DS-Konzept TeleDerm Interim abgebildet.
d. Daneben sind die nachstehenden Maßnahmen vom Auftragnehmer zu gewährleisten.

4.2 Personal:

a. Der Auftragnehmer hat dieses Personal ausdrücklich schriftlich auf die Einhaltung der nachfolgenden Maßnahmen zu verpflichten. Er hat sein Personal dabei auf die besondere Sensibilität der Daten des Auftraggebers hinzuweisen. Der Auftraggeber hat jederzeit das Recht Kopien der Verpflichtungen dieser Beschäftigten zu verlangen.
b. Der Einsatz von Subauftragnehmern ist auftragsbezogen nur in dem Rahmen zulässig, der im DS-Konzept TeleDerm Interim definiert ist. Das Datenverarbeitungskonzept ist dem Auftraggeber auf Wunsch vorzulegen.

4.3 Datennutzung, Datenweitergabe:

a. Im Rahmen der Auftragserledigung ist nur die Kenntnisnahme pseudonymisierter Daten des Auftraggebers zulässig. Jede Nutzung oder Verarbeitung von Daten darüber hinaus hat ausschließlich anonymisiert zu erfolgen. Der Auftragsnehmer hat insbesondere dafür Sorge zu tragen, dass keine personenbezogenen Daten außer die in 2.1. definierten Daten gespeichert werden.
b. Der Auftragnehmer gibt keine auftragsbezogenen Daten an Dritte weiter, soweit dies nicht auftragsgemäß oder auf Einzelweisung des Auftraggebers geschieht.

4.4 Transportkontrolle: Der Auftragnehmer stellt durch folgende Maßnahmen sicher, dass Unbefugte während des Transports/der Übermittlung keinen Zugriff auf die gespeicherten Auftraggeberdaten erhalten:

a. Datennutzung und Remote-Service finden nur über eine kryptographisch verschlüsselte Verbindung statt. Dazu genutzte Konzepte sind X.509 Zertifikate und TLS 1.3.

4.5 Organisationskontrolle: Der Auftragnehmer hat folgende organisatorischen Maßnahmen einzuhalten:

a. Das Anfertigen von Hardcopies mit personenbeziehbaren Daten ist untersagt. Die Speicherung pseudonymisierten Daten gem. 2.1 erfolgt wie im Datenschutzkonzept der HSRT erläutert. Das DS-Konzept ist dem Auftraggeber auf Wunsch vorzulegen.
b. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung könnte gegen Datenschutzvorschriften verstoßen. Auch wird der Auftragnehmer den Auftraggeber unverzüglich informieren, wenn ein Verdacht oder die Erkenntnis darüber vorliegt, dass im Rahmen der Auftragserfüllung Unbefugte Auftraggeberdaten zur Kenntnis genommen haben könnten. Ebenso, wenn die Kenntnisnahme zugangs- oder zugriffsrelevanter Informationen (z.B. Passwörter, Zertifikate) durch Unbefugte oder der Verlust von Zugangsmedien (z.B. Hardware Token, Schlüssel) vorliegt oder zu befürchten ist.
c. Genauere Informationen hinsichtlich der Organisationskontrolle ist dokumentiert in den technischen und organisatorischen Maßnahmen (TOMs) der HSRT und kann auf Anfrage eingesehen werden.

4.6 Besondere Vorgaben für Arbeiten des Auftragnehmers im Kontext der auftragsbezogenen Datenverarbeitung:

a. Arbeiten dürfen nur insoweit durchgeführt werden, als sie zur auftragsgemäßen Bereitstellung von Ressourcen erforderlich sind oder mit dem Auftraggeber bzw. dessen Weisungsberechtigten abgestimmt wurden
b. In jedem Einzelfall ist die Kenntnisnahme der pseudonymisierten/faktisch anonymisierten Probandendaten auf das absolut erforderliche Maß zu beschränken.
c. Der Auftragnehmer verpflichtet sich, in seinen Arbeitsräumen für den Bereich des Remote-Services alle nach Art. 32 DS-GVO erforderlichen Maßnahmen zu treffen. Insbesondere ist eine Kenntnisnahme von Daten oder Systeminformationen des Auftraggebers durch unbefugte Dritte auszuschließen. Die hierzu angewandten organisatorischen und technischen Maßnahmen hat der Auftragsnehmer im DV-Konzept „*Telekonsil*“ genannt. Das DV-Konzept ist dem Auftraggeber auf Wunsch vorzulegen.

5. Prüfung und Überwachung

5.1 Der Auftraggeber hat den Auftragnehmer auf Basis eines ihm vorliegenden Projekt-Prüfberichts zu Datenschutz/Datensicherheit ausgewählt.

5.2 Der Auftragnehmer überzeugt sich in geeigneter Weise von der Einhaltung dieser Bestimmungen durch seine Beschäftigten

6. Unterauftragsverhältnisse

6.1. Unterauftragsverhältnisse dürfen nur nach schriftlicher Genehmigung durch den Auftraggeber erteilt werden.

6.2. Sofern eine Einbeziehung von Unterauftragnehmern in Drittländern erfolgen soll, stellt der Auftragnehmer sicher, dass beim jeweiligen Unterauftragnehmer ein angemessenes Datenschutzniveau im Sinne der Art. 44 ff. DSGVO gewährleistet ist, zum Beispiel durch Abschluss einer Vereinbarung gemäß den von der EU-Kommission genehmigten EU-Standardvertragsklauseln.

7. Nachweismöglichkeiten; Inspektionen

7.1. Der Auftragnehmer weist dem Auftraggeber auf dessen Anfrage die Einhaltung der in dieser Vereinbarung geregelten Pflichten mit geeigneten Mitteln auf Anfrage nach. Geeignet sind zum Beispiel:

- eine Darstellung der aktuell getroffenen technischen und organisatorischen Maßnahmen über die Punkte gemäß der Anlage zu Ziff. 2 dieser Vereinbarung,
- Selbstauskünfte oder Prozessbeschreibungen des Auftragnehmers,
- Nachweise zur Durchführung von Selbstaudits,
- unternehmensinterne Verhaltensregelungen einschließlich eines externen Nachweises über deren Einhaltung,
- Zertifikate oder Testate zum Datenschutz und/oder zur Informationssicherheit,

- genehmigte Verhaltensregelungen gemäß Art. 40 DSGVO,
- Zertifikate gemäß Art. 42 DSGVO.

7.2. Wenn im Einzelfall dennoch Inspektionen beim Auftragnehmer erforderlich sein sollten, werden diese auf Kosten des Auftraggebers durch diesen selbst oder einen unabhängigen externen Prüfer durchgeführt, den der Auftragnehmer benennt.

7.3. Der Auftragnehmer darf nur solche Prüfer benennen, die gegenüber dem Auftraggeber ihre Unabhängigkeit vom Auftragnehmer versichert und sich zur Verschwiegenheit verpflichtet haben. Den Prüfbericht des Prüfers erhalten beide Parteien.

7.4. Inspektionen (Vor-Ort-Kontrollen) beim Auftragnehmer durch den Auftraggeber oder von diesem beauftragte Prüfer finden nur statt nach vorheriger Abstimmung und Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit sowie zu den üblichen Geschäftszeiten. Der Auftraggeber muss gewährleisten, dass der Betriebsablauf des Auftragnehmers nicht gestört wird. Die Inspektionen durch vom Auftraggeber beauftragte Prüfer kann der Auftragnehmer von der Unterzeichnung einer Verschwiegenheitserklärung durch diesen abhängig machen.

7.5. Der Auftraggeber trägt neben den Kosten des Prüfers/der Prüferin die Aufwendungen des Auftragnehmers, die diesem im Rahmen der Inspektion entstehen.

7.6. Der Auftragnehmer hat in jedem Fall das Recht, die Duldung von Kontrollen und die Erteilung von Informationen zu verweigern, wenn die Kontrolle bzw. Informationserteilung ein Risiko darstellen würde für die Sicherheit der Datenverarbeitungsanlagen oder der darauf befindlichen Daten des Auftragnehmers oder Dritter (zum Beispiel anderer Auftraggeber des Auftragnehmers).

8. Schlussbestimmungen

8.1. Anpassung Anlagen: Anlagen zur Vereinbarung können durch die koordinierenden Weisungsberechtigten bei Auftraggeber und Auftragnehmer im Einvernehmen angepasst werden. Hierzu ist eine gegenseitige Bestätigung in Textform (z.B. E-Mail) erforderlich).

8.2. Beendigung des Auftrags: Dieser Auftrag endet mit Ablauf des zugrundeliegenden Vertrages bzw. der zugrundeliegenden Kooperation.

8.3. Nach Abschluss der vertraglich vereinbarten Arbeiten oder nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung eines etwaig bestehenden Hauptvertrages – 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.

Sofern bei Beendigung des Auftrages keine anderslautenden schriftlichen Vereinbarungen getroffen worden sind, gelten die gesetzlichen Bestimmungen in Bezug auf die Löschfristen.

Datum, Unterschrift

<Name Hausarzt, Adresse>

Datum, Unterschrift

Der Kanzler der
Hochschule Reutlingen
Alteburgstraße 150
72762 Reutlingen