

Anlage 5.1: Vertrag zur Auftragsverarbeitung (AVV)

zwischen

dem **Universitätsklinikum Heidelberg**

Anstalt des öffentlichen Rechts

Im Neuenheimer Feld 672

69120 Heidelberg

vertreten durch den Vorstand

– nachfolgend „**Auftraggeber**“ (**AG**) genannt –

und

dem Gewinner der Ausschreibung

– nachfolgend „**Auftragnehmer**“ (**AN**) genannt –

§ 1 Gegenstand, Dauer und Zweck der Verarbeitung

(1) Der Auftragnehmer wird für den Auftraggeber als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 i.V.m. Art. 28 DSGVO tätig. Gegenstand und Zweck der Verarbeitung ist die Durchführung von Abrechnungsdienstleistungen für den Auftraggeber gemäß den Bestimmungen des Hauptvertrages.

(2) Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages.

§ 2 Kategorien von Daten und Kreis betroffener Personen

(1) Im Rahmen des Auftrags werden folgende Arten personenbezogener Daten verarbeitet:

- Patientenstammdaten (z.B. Name, Geburtsdatum, Anschrift, Versichertennummer etc.)
- Abrechnungs- und Finanzdaten (z.B. Rechnungsbeträge, Bankverbindungen etc.)
- Besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO (z.B. Medizinische Behandlungsdaten, Diagnosen, Prozeduren, Medikation und sonstige sensible Gesundheitsdaten)

(2) Der Kreis der von der Verarbeitung betroffenen Personen umfasst Patientinnen und Patienten des Auftraggebers sowie deren gesetzliche Vertreter.

§ 3 Verantwortlichkeiten

(1) Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Ziff. 7 DSGVO und für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten und die Beauftragung des Auftragsverarbeiters verantwortlich.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers zur Erbringung der im Hauptvertrag geschuldeten Leistungen.

(3) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie nach der DSGVO geltenden Bestimmungen sowie der jeweiligen nationalen datenschutzrechtlichen Bestimmungen verantwortlich.

§ 4 Weisungsbefugnis des Auftraggebers

(1) Die Verarbeitung der Daten, insbesondere Art, Umfang und Verfahren der Datenverarbeitung, erfolgt ausschließlich nach Weisung des Auftraggebers im Rahmen der im Hauptvertrag und seinen Anlagen getroffenen Vereinbarungen oder nach jederzeit möglicher in Text- oder Schriftform dokumentierter Einzelanweisung des Auftraggebers.

(2) Mündliche Weisungen wird der Auftraggeber unverzüglich in Textform oder Schriftform bestätigen. Der Auftragnehmer notiert bei mündlichen Weisungen, Datum, Uhrzeit und die weisungserteilende Person sowie den Grund für die mündliche Weisung.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, alle im Rahmen der Auftragsverarbeitung erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Dies gilt unbeschadet einer im Hauptvertrag geltenden Vereinbarung zur Verschwiegenheit. Die Verpflichtung nach diesen Bestimmungen besteht über die Beendigung des Hauptvertrages hinaus.

(2) Der Auftragnehmer gewährleistet, dass die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Der Auftragnehmer und ihm unterstellte Personen, die Zugang zu den Daten haben, dürfen diese nur auf Weisung des Verantwortlichen verarbeiten. Dies ist durch eine schriftliche Verpflichtung und geeignete Überwachungsmaßnahmen sicherzustellen.

(4) Der Auftragnehmer hat darüber hinaus sicherzustellen, dass die von ihm zur Auftragserfüllung eingesetzten Beschäftigten vor Beginn der Verarbeitung und dann regelmäßig über ihre Datenschutzpflichten belehrt werden. Der Auftraggeber kann die Vorlage der entsprechenden Schulungsnachweise verlangen.

(5) Der Auftragnehmer hat das von ihm zu führende Verzeichnis von Verarbeitungstätigkeiten auf Verlangen dem Auftraggeber vorzulegen, soweit der Auftrag davon betroffen ist.

(6) Wendet sich eine Person zur Wahrnehmung ihrer Rechte nach Kapitel III der DSGVO an den Auftragnehmer, verweist dieser die Person unverzüglich an den Auftraggeber, sofern eine Zuordnung zum Auftraggeber möglich ist. Der Auftragnehmer wird gegenüber der Person keine Auskunft zum Inhalt der Anfrage geben.

(7) Der Auftragnehmer unterstützt den Auftraggeber auf Nachfrage bei all dessen sich aus der DSGVO und dem für ihn geltenden nationalen Recht ergebenden Pflichten mit Informationen, Dokumenten und erforderlichen Handlungen. Dies betrifft insbesondere die dem Auftraggeber obliegenden Verpflichtungen nach Kapitel III der DSGVO sowie die Einhaltung seiner Pflichten nach Art. 33 bis 36 DSGVO.

(8) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich schriftlich oder in Textform:

- a. über Verstöße gegen datenschutzrechtliche Bestimmungen oder vertragliche Regelungen bei der Auftragsausführung oder entsprechenden Verstößen bei von ihm in Anspruch genommenen weiteren Auftragsverarbeitern. Er trifft unverzüglich erforderliche Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen

- b. über jegliche Maßnahmen staatlicher Stellen, insbesondere Kontrollen, Ermittlungs-, Strafverfolgungsverfahren, oder Ermittlungen der Finanzbehörden, die die im Auftrag zu verarbeitenden Daten betreffen oder betreffen könnten. Ebenso über jegliche Gefährdung der Daten des Auftraggebers oder der Auftragsverarbeitung durch Rechtsverfahren, Ereignisse oder Maßnahmen Dritter. Der Auftragnehmer informiert in beiden Fällen die in diesem Zusammenhang Verantwortlichen über die Hoheits- und Eigentumsverhältnisse an den Daten im Rahmen der Auftragsverarbeitung. Er stellt dem Auftraggeber die Information an die Verantwortlichen unaufgefordert unverzüglich schriftlich zur Verfügung.
 - c. falls er der Meinung ist, dass eine Weisung des Auftraggebers gegen die DSGVO oder andere Datenschutzbestimmungen, die für diese Auftragsverarbeitung anwendbar sind verstößt
 - d. über Anfragen Betroffener zur Ausübung ihrer Rechte, die bei ihm eingegangen sind. Der Auftragnehmer übersendet die Anfrage des Betroffenen, soweit diese nicht mündlich erfolgte.
- (9) Jede Verarbeitung des Auftragnehmers in einem Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
- (10) Wird der Auftraggeber nach Art. 82 DSGVO in Haftung genommen, wird ihn der Auftragnehmer bei der Abwehr des Anspruchs unterstützen, soweit er sich dadurch nicht selber einer Haftung aussetzt.

§ 6 Geheimnisschutz nach § 203 StGB (Patientengeheimnis)

- (1) Der Auftragnehmer ist sich bewusst, dass die im Rahmen dieses Vertrages zugänglich gemachten Daten dem Patientengeheimnis unterliegen.
- (2) Der Auftragnehmer verpflichtet sich und alle im Rahmen dieses Auftrags eingesetzten Personen (einschließlich der Mitarbeiter von zugelassenen Subunternehmern) schriftlich auf die Wahrung der Berufsgeheimnisse gemäß § 203 StGB zu verpflichten. Die standardmäßigen Verpflichtungserklärungen wurden dem Auftraggeber mit dem Angebot vorgelegt.

§ 7 Technisch-organisatorische Maßnahmen (TOMs)

- (1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Anforderungen nach Art. 32 DSGVO einzuhalten und die Sicherheit der Verarbeitung durch geeignete technische und organisatorische Maßnahmen fortlaufend zu gewährleisten.
- (2) Die Parteien vereinbaren, dass die vom Auftragnehmer im Rahmen des Vergabeverfahrens mit dem Angebot eingereichten Nachweise und Sicherheitskonzepte (insbesondere die ausgefüllte und bestätigte **Anlage 2** „Eigenerklärung zu den Datenschutz- und Sicherheitsanforderungen“ fester Bestandteil dieses AVV werden, ebenfalls die als **Anlage 4** beigefügten TOMs.
- (3) Die dort definierten Standards (u.a. ISO 27001/IT-Grundschutz oder gleichwertiges Framework, mindestens TLS 1.2 mit PFS oder höher /AES-256, Multi-Faktor-Authentisierung, 24/7 SOC/SIEM sowie das Ransomware-resistente Backup-Konzept usw.) stellen die vertraglich geschuldete Mindestqualität der TOMs dar und dürfen während der Vertragslaufzeit nicht unterschritten werden. Sie müssen an das dem technischen Fortschritt entsprechende Sicherheitsniveau angepasst werden.

§ 8 Unterauftragsverhältnisse (Subunternehmer)

- (1) Der Auftragnehmer darf Unterauftragsverarbeiter nur mit vorheriger Genehmigung des Auftraggebers in Text- oder Schriftform einsetzen.
- (2) Die Parteien vereinbaren, dass die mit dem Angebot eingereichte **Anlage 3** (Verzeichnis der eingesetzten Unterauftragsverarbeiter) mit Zuschlagserteilung als genehmigt gilt.
- (3) Jede beabsichtigte Änderung oder Neueinsetzung von Subunternehmern ist dem Auftraggeber mindestens vier Wochen im Voraus schriftlich anzuzeigen. Der Auftraggeber kann der Änderung oder Neueinsetzung aus wichtigem Grund (insbesondere bei datenschutzrechtlichen Bedenken) widersprechen und die Genehmigung verweigern.
- (4) Der Auftragnehmer muss die weiteren Auftragsverarbeiter (Subunternehmer) unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen und der Anforderungen der DSGVO im Rahmen der Auftragsverarbeitung gewissenhaft auswählen.
- (5) Der Auftragnehmer ist verpflichtet, mit jedem weiteren Auftragsverarbeiter (Subunternehmer) eine schriftliche Vereinbarung zu treffen, die diesem dieselben strengen Datenschutz- und IT-Sicherheitspflichten auferlegt, die zwischen dem Auftraggeber und dem Auftragnehmer in diesem Vertrag vereinbart sind (Kette von Auftragsverarbeitungsverträgen gemäß Art. 28 Abs. 4 DSGVO). Dies gilt insbesondere für die Einhaltung der vereinbarten technischen Mindeststandards.
- (6) Kommt ein von ihm beauftragter weiterer Auftragnehmer (Subunternehmer) seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten dieses weiteren Auftragsverarbeiters.

§ 9 Kontrollrechte des Auftraggebers (Audits)

- (1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften und der Vereinbarungen dieses Vertrages beim Auftragnehmer innerhalb der Betriebszeiten zu überprüfen.
- (2) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber oder ein von ihm Beauftragter, zur Verschwiegenheit verpflichteter externer Prüfer, Kontrollen vor Ort in den Geschäftsräumen und Rechenzentren etc. des Auftragnehmers durchführen darf.
- (3) Gemäß der im Vergabeverfahren vereinbarten Kostenregelung ist die Unterstützung des Auftragnehmers bei diesen Routine- sowie anlassbezogenen Audits mit den vertraglichen Pauschalen des Hauptvertrags abgegolten.
- (4) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

§ 10 Meldung von Sicherheitsvorfällen

Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens jedoch **innerhalb von 24 Stunden nach Bekanntwerden**, über jeden Verdacht eines Sicherheitsvorfalls, Datenverlusts oder unbefugten Zugriffs auf die Patientendaten des Auftraggebers. Die Meldung hat unter anderem zwingend über nachfolgende E-Mail-Adressen sowie über eine telefonische Meldung an den Klinikumsvorstand zu erfolgen:

- Datenschutzmeldung@med.uni-heidelberg.de
- Informationssicherheit@med.uni-heidelberg.de

§ 11 Vertragsstrafe bei schwerwiegenden Sicherheits- und Pflichtverstößen

- (1) Verstößt der Auftragnehmer gegen die 24-Stunden-Meldefrist (§ 10) beträgt die Vertragsstrafe 5.000,- EUR für jeden angefangenen Kalendertag des Verzugs.
- (2) Die Geltendmachung eines weitergehenden Schadensersatzanspruchs durch den Auftraggeber bleibt von der Zahlung der Vertragsstrafe unberührt.
- (3) Unbeschadet der Vertragsstrafe berechtigt ein wiederholter oder schwerwiegender Verstoß gegen die Sicherheitsanforderungen den Auftraggeber zur fristlosen Kündigung des Hauptvertrages aus wichtigem Grund.

§ 12 Berichtigung, Löschung und Rückgabe von Datenträgern

- (1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Soweit Daten vonseiten des Auftraggebers z.B. für Serviceanfragen, Fehlerbehebungen etc. oder Kontrollzwecke übermittelt werden, sind sie umgehend nach Zweckerfüllung rückstandslos zu löschen. Von Satz 1 ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung rechtlicher Aufbewahrungspflichten erforderlich sind.
- (2) Nach Auftragsende muss der Auftragnehmer alle Daten nach Wahl des Auftraggebers entweder löschen oder herausgeben, sofern sich aus der Ausnahme nach Art. 28 Abs. 3 lit. g DSGVO keine andere Pflicht für den Auftragnehmer ergibt. 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.
- (4) Der Auftraggeber kann jederzeit, während der Laufzeit des Vertrages, die Berichtigung, Löschung, Verarbeitungseinschränkung und Herausgabe von Daten vom Auftragnehmer verlangen.

§ 13 Haftung

- (1) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend Art. 82 DSGVO.
- (2) Weitergehende Haftungsansprüche nach allgemeinen Gesetzen bleiben unberührt.

§ 14 Schlussbestimmungen

- (1) Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern ist ausgeschlossen.
- (2) Mündliche Nebenabreden und Ergänzungen bestehen zum Zeitpunkt des Vertragsschlusses nicht. Nebenabreden, Änderungen oder Ergänzungen bedürfen zu ihrer Wirksamkeit der Schriftform.

(3) Sollten einzelne Bestimmungen dieser AV-Bedingungen nicht rechtswirksam oder undurchführbar sein, gelten die übrigen Bestimmungen weiter. Die Vertragsparteien treten ggf. umgehend in die Abstimmung und den Abschluss erforderlicher Anpassungen ein. Die Auftragsverarbeitung erfolgt bis zum Abschluss in einer Weise, die dem Sinn und Zweck von Art. 28 DS-GVO entspricht, sofern der Auftraggeber nicht eine Unterbrechung der Verarbeitung bis zur Klärung anweist.

(4) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zur Auftragsverarbeitung den Regelungen des Hauptvertrags und seiner Anlagen vor.