



DATENSCHUTZ-RAHMENVERTRAG

Zwischen

Firmenname:

ggfl. Abteilung:

Straße, Nr:

PLZ, Ort:

(**"Auftraggeber"**)

und

Carl Zeiss Meditec Vertriebsgesellschaft mbH,

Rudolf-Eber-Straße 11, 73447 Oberkochen

sowie

Carl Zeiss Meditec AG,

Göschwitzer Str. 51-52, 07745 Jena

(jeweils als **"Auftragnehmer"**)



INHALTSVERZEICHNIS

Präambel	3
Teil A Auftragsverarbeitungsvertrag	4
1. Anwendungsbereich dieses Teil A.....	4
2. Details der Verarbeitung.....	4
3. Pflichten und Rechte des Verantwortlichen.....	4
4. Pflichten des Auftragsverarbeiters.....	6
5. Übermittlung personenbezogener Daten in Drittländer.....	11
6. Berufsgeheimnis.....	12
Teil B Vertrag zur gemeinsamen Verantwortlichkeit	13
7. Anwendungsbereich dieses Teil B.....	13
8. Details der GV-Leistungen.....	13
9. Zuständigkeiten und Verpflichtungen der Parteien.....	13
10. Übermittlung personenbezogener Daten in Drittländer.....	15
Teil C Allgemeine Bestimmungen	16
11. Anwendungsbereich dieses Teil C.....	16
12. Begriffsbestimmungen.....	16
13. Haftung.....	17
14. Inkrafttreten, Laufzeit und Beendigung.....	17
15. Anwendbares Recht und Gerichtsstand.....	17
16. Schlussbestimmungen.....	17
Anhang 1	21
Anhang 2	23
Anhang 3	25



Präambel

- (A) Die Parteien beabsichtigen eine geschäftliche Zusammenarbeit unter einem oder mehreren Verträgen, nach denen der jeweilige Auftragnehmer Leistungen für den Auftraggeber und/oder gemeinsam mit dem Auftraggeber erbringt. Bei der Leistungserbringung unter dem jeweiligen Vertrag verarbeitet der jeweilige Auftragnehmer möglicherweise personenbezogene Daten (Art. 4 Nr. 1 DSGVO) als Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) im Auftrag des Auftraggebers als Verantwortlichem (Art. 4 Nr. 7 DSGVO) und/oder als mit dem Auftraggeber gemeinsam für die Verarbeitung Verantwortlicher (Art. 26 DSGVO).
- (B) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, muss die Verarbeitung durch den Auftragsverarbeiter gemäß Art. 28 (3) DSGVO auf der Grundlage eines Vertrags erfolgen, der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betreffender Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.
- (C) Erfolgt eine Verarbeitung in gemeinsamer Verantwortlichkeit, müssen die gemeinsam Verantwortlichen gemäß Art. 26 (1) DSGVO in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Art. 13 und 14 DSGVO nachkommt. Diese Vereinbarung muss auch die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das Wesentliche der Vereinbarung ist den betroffenen Personen zur Verfügung zu stellen.
- (D) Gemäß Kapitel V DSGVO ist eine Übermittlung und/oder Verarbeitung personenbezogener Daten an/in Länder(n) außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (Drittländer) nur zulässig, wenn bestimmte Bedingungen eingehalten werden. In Fällen, in denen die Europäische Kommission nicht beschlossen hat, dass ein Drittland ein angemessenes Schutzniveau bietet, darf die Übermittlung personenbezogener Daten an dieses Drittland und/oder die Verarbeitung in diesem Drittland nur erfolgen, wenn geeignete Garantien vorgesehen sind oder wenn Ausnahmen für bestimmte Fälle zutreffen. Geeignete Garantien können unter anderem darin bestehen, Standardvertragsklauseln zu implementieren, die die Europäische Kommission erlassen hat.
- (E) Informationen aus der Sphäre des Auftraggebers, die dem jeweiligen Auftragnehmer bei der Leistungserbringung zur Kenntnis gelangen, können einem Berufsgeheimnis unterliegen, ungeachtet, ob es sich dabei um personenbezogene Daten handelt oder nicht. Gemäß berufs- und strafrechtlichen Regelungen bedarf die Offenbarung solcher Informationen besonderer Verpflichtungen zur Wahrung des Berufsgeheimnisses.
- (F) Mit diesem Datenschutz-Rahmenvertrag und den für jede relevante Leistung gesondert abzuschließenden Einzelaufträgen zu diesem Datenschutz-Rahmenvertrag beabsichtigen die Parteien, die nötige vertragliche Grundlage für die Erfüllung der vorgenannten datenschutz- und berufsrechtlichen Verpflichtungen zu schaffen. Solche Einzelaufträge sollen jeweils zwischen dem Auftraggeber und dem jeweils zuständigen Auftragnehmer abgeschlossen werden.



DIES VORAUSGESCHICKT, vereinbaren die Parteien Folgendes:

Teil A Auftragsverarbeitungsvertrag

1. Anwendungsbereich dieses Teil A

1.1 Anwendungsbereich

Dieser Teil A (Auftragsverarbeitungsvertrag) findet Anwendung zwischen dem Auftraggeber und dem jeweiligen Auftragnehmer, soweit diese Parteien für eine Verarbeitung personenbezogener Daten durch den jeweiligen Auftragnehmer als Auftragsverarbeiter in einem Einzelauftrag festgelegt haben, dass der jeweilige Auftragnehmer Auftragsverarbeitungs-Leistungen erbringt.

Klarstellend halten die Parteien fest, dass dieser Teil A für sich, also ohne einen solchen Einzelauftrag, noch keine Rechte und Pflichten der Parteien begründet und dass dieser Teil A und der jeweilige Einzelauftrag jeweils nur zwischen dem Auftraggeber und dem jeweiligen Auftragnehmer Anwendung findet, also insoweit keine Rechtswirkung gegenüber dem anderen Auftragnehmer entfaltet, der nicht Vertragspartei des jeweiligen Einzelauftrags ist.

1.2 Parteien und ihre jeweiligen Rollen

Im Rahmen der Erbringung von Auftragsverarbeitungs-Leistungen ist der Auftraggeber der Verantwortliche und der Auftragnehmer der Auftragsverarbeiter. Das heißt die Pflichten und Rechte des Verantwortlichen (insbesondere Abschnitt 3) gelten für den Auftraggeber und die Pflichten des Auftragsverarbeiters (insbesondere Abschnitt 4) für den Auftragnehmer.

1.3 Anwendung auf Informationen, die dem Berufsgeheimnis unterliegen

Dieser Teil A findet außerdem Anwendung auf den Umgang mit Informationen aus der Sphäre des Auftraggebers, die einem Berufsgeheimnis unterliegen, ungeachtet, ob es sich hierbei um personenbezogene Daten handelt oder nicht. Soweit es sich bei diesen Informationen nicht um personenbezogene Daten handelt, finden die Regelungen zur Verarbeitung personenbezogener Daten dieses Teil A entsprechende Anwendung.

2. Details der Verarbeitung

Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien betroffener Personen sowie der Ort der Verarbeitung im Zusammenhang mit einem Einzelauftrag werden im jeweiligen Einzelauftrag festgelegt.

3. Pflichten und Rechte des Verantwortlichen

3.1 Verantwortlichkeiten des Verantwortlichen

Der Verantwortliche ist für die Einhaltung der nach der DSGVO auf einen Verantwortlichen anwendbaren Verpflichtungen verantwortlich, insbesondere für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten gemäß Kapitel II DSGVO und die Einhaltung der Rechte der Betroffenen gemäß Kapitel III DSGVO.

3.2 Weisungsrecht

- 3.2.1 Der Verantwortliche hat das Recht, Weisungen an den Auftragsverarbeiter bezüglich der Verarbeitung personenbezogener Daten unter diesem Teil A zu erteilen.
- 3.2.2 Die Regelungen dieses Teil A, insbesondere die Bestimmung der Details der Verarbeitung gemäß Abschnitt 2, dienen für den jeweiligen Einzelauftrag als allgemeine Weisungen, personenbezogene Daten so zu verarbeiten, wie es für die Erbringung der AV-Leistungen vernünftigerweise erforderlich ist und mit diesem Teil A, dem jeweiligen Hauptvertrag und dem jeweiligen Einzelauftrag vereinbar ist.
- 3.2.3 Der Verantwortliche ist befugt, Einzelweisungen mindestens in Textform zu erteilen.
- 3.2.4 Personen, die autorisiert sind, im Namen des Verantwortlichen Einzelweisungen an den Auftragsverarbeiter zu erteilen und Weisungen vom Verantwortlichen im Namen des Auftragsverarbeiters zu empfangen, werden in Anhang 1 benannt. Regelungen hierzu im jeweiligen Einzelauftrag gehen für den jeweiligen Einzelauftrag den Angaben in Anhang 1 vor.
- Die Parteien benachrichtigen einander unverzüglich in Textform über etwaige Änderungen der autorisierten Personen. Bis zum Zugang einer solchen Benachrichtigung bei der anderen Partei gelten die in Anhang 1 bzw. im jeweiligen Einzelauftrag genannten Personen weiterhin als autorisiert, Weisungen zu erteilen und zu empfangen.
- 3.2.5 Der Verantwortliche dokumentiert die an den Auftragsverarbeiter erteilten Einzelweisungen.
- 3.2.6 Einzelweisungen, die von den Regelungen des jeweiligen Hauptvertrags, des jeweiligen Einzelauftrags oder dieses Teil A abweichen oder darüber hinausgehen, gelten als Änderungsverlangen im Sinne der Regelungen des jeweiligen Hauptvertrags bzw. erfolgen auf Grundlage der dort oder im jeweiligen Einzelauftrag ggf. geregelten Stunden-/Tagessätze oder der dort ggf. geregelten Vergütung für über den jeweiligen Hauptvertrag bzw. Einzelauftrag hinausgehende Zusatzleistungen.

3.3 Informationsrecht und Recht auf Durchführung von Überprüfungen, einschließlich Inspektionen

- 3.3.1 Der Verantwortliche hat das Recht vom Auftragsverarbeiter alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zu verlangen und Überprüfungen – einschließlich Inspektionen – beim Auftragsverarbeiter entweder selbst oder durch einen von ihm beauftragten Prüfer durchzuführen.
- 3.3.2 Das Recht des Verantwortlichen auf Informationen und auf Durchführung von Überprüfungen, einschließlich Inspektionen, gemäß Abschnitt 3.3 besteht auch nach Beendigung des jeweiligen Einzelauftrags hinsichtlich der Einhaltung der Pflichten des Auftragsverarbeiters zur Löschung oder Rückgabe der personenbezogenen Daten an den Verantwortlichen nach Abschluss der Erbringung der Verarbeitungsleistungen nach Abschnitt 4.6 für eine Dauer von 30 Tagen ab Abschluss der Erbringung der Verarbeitungsleistungen unter dem jeweiligen Einzelauftrag.
- 3.3.3 Vor der Durchführung von Überprüfungen – einschließlich Inspektionen – prüft der Verantwortliche die vom Auftragsverarbeiter bereitgestellten Informationen ordnungsgemäß dahingehend, ob diese zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten des Auftragsverarbeiters genügen.



- 3.3.4 Der Verantwortliche informiert den Auftragsverarbeiter rechtzeitig, im Regelfall mindestens zwei (2) Wochen im Voraus, über die Durchführung einer Überprüfung, einschließlich einer Inspektion. In dringenden, vom Verantwortlichen nachzuweisenden und zu begründenden Ausnahmefällen ist der Verantwortliche berechtigt, eine Überprüfung, einschließlich einer Inspektion, mit einer kürzeren, für den jeweiligen Fall angemessenen Vorankündigungsfrist durchzuführen. Ein solcher Ausnahmefall kann zum Beispiel vorliegen, wenn eine zuständige Aufsichtsbehörde rechtmäßig verlangt, dass der Verantwortliche unverzüglich eine solche Überprüfung durchführt.
- 3.3.5 Der Verantwortliche führt Inspektionen während der normalen Geschäftszeiten des Auftragsverarbeiters durch.
- 3.3.6 Das Betreten der Räumlichkeiten des Auftragsverarbeiters darf nur in ständiger Anwesenheit eines Vertreters des Auftragsverarbeiters erfolgen. Dieser Vertreter ist befugt, Entscheidungen über den Verlauf der Inspektion zu treffen, soweit dies erforderlich ist, um Störungen des Geschäftsbetriebs des Auftragsverarbeiters zu vermeiden und dessen Geheimhaltungspflichten gegenüber Dritten zu wahren.
- 3.3.7 Der Verantwortliche darf regelmäßige Überprüfungen – einschließlich Inspektionen – höchstens einmal pro Kalenderjahr durchführen. Der Verantwortliche darf zusätzliche Überprüfungen – einschließlich Inspektionen – nur aus einem von ihm nachzuweisenden wichtigen Grund durchführen.
- 3.3.8 Der Verantwortliche hat die Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters, die dem Verantwortlichen während einer Überprüfung – einschließlich Inspektionen – bekannt werden, streng vertraulich zu behandeln. Der Verantwortliche erstellt keine Aufzeichnungen über diese Informationen, es sei denn, dies ist für die Ausübung seines Prüfungsrechts unbedingt erforderlich.

4. Pflichten des Auftragsverarbeiters

4.1 Verarbeitung auf dokumentierte Weisung des Verantwortlichen

- 4.1.1 Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten, die Gegenstand dieses Teil A sind, nur auf dokumentierte Weisung des Verantwortlichen - auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation - sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- 4.1.2 Der Auftragsverarbeiter stellt sicher, dass jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, die Gegenstand dieses Teil A sind, die Daten ausschließlich auf Weisung des Verantwortlichen verarbeitet, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet ist. Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home-Office, mobiles Arbeiten) ist zulässig, sofern der Auftragsverarbeiter die Einhaltung der hierfür angemessenen Sicherheitsmaßnahmen im Sinne des Art. 32 DSGVO sicherstellt.



- 4.1.3 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

Der Auftragsverarbeiter ist befugt, die Ausführung der jeweiligen Weisung auszusetzen, bis sie vom Verantwortlichen bestätigt oder geändert wurde.

- 4.1.4 Der Auftragsverarbeiter ist berechtigt, Einzelweisungen zurückzuweisen und diese nicht auszuführen, soweit sie vom jeweiligen Hauptvertrag oder dem jeweiligen Einzelauftrag abweichen oder darüber hinausgehen und soweit die Durchführung der jeweiligen Weisung nicht im Rahmen der in Abschnitt 4.5 dieses Teil A geregelten Unterstützungspflichten erforderlich ist.

4.2 Vertraulichkeit der Personen, die zur Verarbeitung der personenbezogenen Daten berechtigt sind

Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten, die Gegenstand dieses Teil A sind, befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

4.3 Sicherheit der Verarbeitung

- 4.3.1 Der Auftragsverarbeiter ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen.
- 4.3.2 Die konkreten vom Auftragsverarbeiter zu ergreifenden Maßnahmen sind in Anhang 2 dieses Datenschutz-Rahmenvertrages festgelegt. Regelungen hierzu im jeweiligen Einzelauftrag gehen für den jeweiligen Einzelauftrag den Angaben in Anhang 2 vor.
- 4.3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragsverarbeiter ist daher befugt und ggf. gemäß Art. 32 DSGVO verpflichtet, zusätzliche oder alternative Maßnahmen zu den in Anhang 2 dieses Datenschutz-Rahmenvertrags bzw. im jeweiligen Einzelauftrag aufgeführten Maßnahmen zu ergreifen. Etwaige zusätzliche oder alternative Maßnahmen dürfen das Sicherheitsniveau der in Anhang 2 bzw. im jeweiligen Einzelauftrag festgelegten Maßnahmen nicht absenken.
- 4.3.4 Bei der Ergreifung der nach Art. 32 DSGVO erforderlichen Maßnahmen berücksichtigt der Auftragsverarbeiter die mit der Verarbeitung einhergehenden Risiken für die Rechte und Freiheiten der betroffenen Personen. Bei der Risikobewertung berücksichtigt der Auftragsverarbeiter insbesondere die im jeweiligen Einzelauftrag beschriebenen Einzelheiten der Verarbeitung.
- 4.3.5 Der Auftragsverarbeiter dokumentiert alle Änderungen der Maßnahmen und legt sie dem Verantwortlichen auf Anfrage vor.
- 4.3.6 Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten, die Gegenstand dieses Teil A sind, bekannt wird, meldet er diese dem Verantwortlichen unverzüglich. Diese Meldung enthält zumindest die gesetzlich erforderlichen Informationen.

4.4 Beauftragung weiterer Auftragsverarbeiter (Unterauftragsverarbeiter)

- 4.4.1 Der Auftragsverarbeiter hält die in Art. 28 (2) und (4) DSGVO genannten Bedingungen für die Beauftragung eines weiteren Auftragsverarbeiters ein, wonach insbesondere Folgendes gilt:
- a) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.
 - b) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auferlegt, wie sie in diesem Teil A und im jeweiligen Einzelauftrag festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.
- 4.4.2 Der Auftragnehmer handelt als einziger Ansprechpartner für jedwede Kommunikation zwischen dem Auftraggeber und jedem Unterauftragsverarbeiter bezüglich der Ausübung der Rechte des Verantwortlichen und der Durchsetzung der Verpflichtungen des Auftragsverarbeiters im Namen des jeweiligen Verantwortlichen und gemäß den Weisungen des jeweiligen Verantwortlichen. Der Auftragnehmer verpflichtet sich als einziger Ansprechpartner, jede Mitteilung, die vom Auftraggeber an einen Unterauftragsverarbeiter gerichtet ist, unverzüglich an den jeweiligen Unterauftragsverarbeiter weiterzuleiten. Der Auftragnehmer verpflichtet sich als einziger Ansprechpartner, jede Mitteilung, die von einem Unterauftragsverarbeiter an den Auftraggeber gerichtet ist, unverzüglich an den Auftraggeber weiterzuleiten.
- 4.4.3 Der Auftraggeber erteilt hiermit die gesonderte Genehmigung, verbundene Unternehmen des Auftragnehmers unter den in Abschnitt 4.4.1 genannten Bedingungen als Unterauftragsverarbeiter für die Verarbeitung personenbezogener Daten unter allen Einzelaufträgen zu beauftragen.
- 4.4.4 Mit Abschluss des jeweiligen Einzelauftrags erteilt der Auftraggeber die gesonderte Genehmigung, die Unterauftragsverarbeiter, die im jeweiligen Einzelauftrag festgelegt sind, unter den in Abschnitt 4.4.1 genannten Bedingungen für die Verarbeitung personenbezogener Daten unter dem jeweiligen Einzelauftrag zu beauftragen.

Der Auftraggeber erteilt hiermit außerdem die allgemeine Genehmigung, unter allen Einzelaufträgen Unterauftragsverarbeiter unter den in Abschnitt 4.4.1 genannten Bedingungen zu beauftragen. Für jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragsverarbeitern gilt Folgendes:

- a) Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder der Ersetzung von Unterauftragsverarbeitern ohne schuldhaftes Zögern über einen geeigneten Kommunikationskanal.

- b) Der Auftragnehmer behält sich vor, diese Information in Form einer E-Mail-Benachrichtigung dem Auftraggeber zukommen zu lassen. Hierzu verwendet der Auftragnehmer die in Anhang 1 angegebene Adresse des Auftraggeber-Datenschutzbeauftragten. Alternativ gibt der Auftraggeber folgende E-Mail-Adresse an: _____ . Der Auftraggeber hat die Pflicht, den Auftragnehmer über Änderungen an dieser E-Mail-Adresse zu informieren. Sollte die E-Mail-Adresse ersichtlich nicht mehr gültig sein, ist es dem Auftragnehmer gestattet, auf eine E-Mail-Adresse aus dem jüngsten Einzelauftrag zurückzugreifen.
- c) Ein Einspruch des Verantwortlichen gegen eine beabsichtigte Änderung hinsichtlich der Hinzuziehung oder der Ersetzung von Unterauftragsverarbeitern ist nur zulässig, wenn dem Auftragnehmer ein wichtiger Grund nachgewiesen wird. Ein wichtiger Grund liegt nur vor, wenn die Änderung für den Verantwortlichen unter Berücksichtigung alle Umstände und unter Abwägung der Interessen beider Seiten nicht zumutbar ist.

Der Verantwortliche kann nur innerhalb einer angemessenen Frist (normalerweise zwei (2) Wochen), nachdem er vom Auftragsverarbeiter über die Änderung informiert wurde, Einspruch einlegen. Im Falle eines zulässigen Einspruchs liegt es im Ermessen des Auftragsverarbeiters die Verarbeitung ohne die geplante Änderung selbst oder über einen vom Auftragsverarbeiter mit der Genehmigung des Verantwortlichen beauftragen anderen Unterauftragsverarbeiter weiterzuführen oder alle Maßnahmen zu ergreifen, um den vom Verantwortlichen geltend gemachten Einspruchsgrund zu beseitigen, den Verantwortlichen darüber zu informieren und erneut ein entsprechendes Einspruchsrecht einzuräumen sowie die Verarbeitung mit der geplanten Änderung fortzusetzen, wenn entweder (i) die neue Einspruchsfrist ohne einen erneuten Einspruch des Verantwortlichen abgelaufen ist oder (ii) der Auftragsverarbeiter lediglich die vom Verantwortlichen vorgeschlagenen Maßnahmen umgesetzt hat.

- 4.4.5 Nimmt der Auftragsverarbeiter Nebenleistungen von Dritten in Anspruch, die keine (Unter-) Auftragsverarbeitung sind (z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen oder Reinigungsleistungen), ist der Auftragsverarbeiter verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der personenbezogenen Daten, die Gegenstand dieses Teil A sind, angemessene vertragliche Geheimhaltungsverpflichtungen mit dem jeweiligen Leistungsbringer zu vereinbaren, die insbesondere auch vorsehen, dass der jeweilige Leistungserbringer sämtliche mit der Erbringung der Leistungen betraute Personen ebenso zur Geheimhaltung verpflichtet. Die Pflicht, solche Geheimhaltungsverpflichtungen zu vereinbaren, besteht nicht, soweit spezialgesetzliche, strafbewehrte Geheimhaltungsverpflichtungen sämtlicher mit der Erbringung der Nebenleistungen betrauter Personen bestehen (z.B. nach § 203 StGB).

Klarstellend halten die Parteien fest, dass die Inanspruchnahme von Nebenleistungen zur Prüfung oder Wartung (z. B. Fernwartung, externer Support) automatisierter Verfahren oder von Datenverarbeitungsanlagen ein Fall der Unterauftragsverarbeitung ist, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten, die Gegenstand dieses Teil A sind, nicht ausgeschlossen werden kann.

4.5 Unterstützungspflichten

- 4.5.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Personen nachzukommen.
- 4.5.2 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich nachdem er Kenntnis von einem Antrag einer betroffenen Person auf Wahrnehmung ihrer Rechte bezüglich personenbezogener Daten erhalten hat, die Gegenstand dieses Teil A sind.
- 4.5.3 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten bezüglich personenbezogener Daten, die Gegenstand dieses Teil A sind.
- 4.5.4 Der Auftraggeber trägt seine eigenen Kosten für die Einhaltung der Verpflichtung des Verantwortlichen. Soweit im jeweiligen Hauptvertrag oder im jeweiligen Einzelauftrag nichts Abweichendes vereinbart ist, trägt der Auftragsverarbeiter seine eigenen Kosten und Aufwendungen für die Unterstützung des Verantwortlichen.

4.6 Löschung oder Rückgabe der personenbezogenen Daten an den Verantwortlichen nach Abschluss der Erbringung der Verarbeitungsleistungen

- 4.6.1 Nach Abschluss der Erbringung der Verarbeitungsleistungen unter dem jeweiligen Einzelauftrag löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen entweder alle personenbezogenen Daten, die Gegenstand des jeweiligen Einzelauftrags und dieses Teil A sind, oder gibt diese an den Verantwortlichen zurück und löscht die vorhandenen Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
- 4.6.2 Klarstellend halten die Parteien fest, dass der Auftragsverarbeiter personenbezogene Daten, die Gegenstand dieses Teil A sind, auch jederzeit vor Abschluss der Erbringung der Verarbeitungsleistungen auf Einzelweisung des Verantwortlichen löscht.
- 4.6.3 Klarstellend halten die Parteien fest, dass personenbezogene Daten, die Gegenstand dieses Teil A sind, gegebenenfalls auch in Sicherungskopien enthalten sein können, die zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind. Eine individuelle Löschung aus solchen Sicherungskopien ist technisch gegebenenfalls nicht möglich, sodass solche Daten in Sicherungskopien auch nach einem Löschverlangen des Verantwortlichen noch für einen gewissen Zeitraum enthalten sein können. Nach Maßgabe des Abschnitts 14.1.3 gilt dieser Datenschutz-Rahmenvertrag insoweit auch nach einer Beendigung des jeweiligen Hauptvertrages fort.

4.7 Bereitstellung von Informationen und Ermöglichung von und Unterstützung bei Überprüfungen, einschließlich Inspektionen

- 4.7.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht und trägt zu Überprüfungen – einschließlich Inspektionen – bei, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden.

- 4.7.2 Die Regelungen in Abschnitt 3.3 zum Recht des Verantwortlichen auf Informationen und auf Durchführung von Überprüfungen, einschließlich Inspektionen finden entsprechende Anwendung auf die Pflicht des Auftragsverarbeiter gemäß diesem Abschnitt 4.7.
- 4.7.3 Zum Nachweis der Einhaltung seiner Pflichten kann der Auftragsverarbeiter aktuelle Bescheinigungen, Berichte oder Auszüge aus Berichten von unabhängigen Stellen (z.B. Wirtschaftsprüfer, interne Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzprüfer, Qualitätsprüfer) oder eine entsprechende Zertifizierung durch eine IT-Sicherheits- oder Datenschutzüberprüfung (z.B. gemäß dem BSI Grundschutz) vorlegen.

5. Übermittlung personenbezogener Daten in Drittländer

5.1 Bedingungen für Übermittlung personenbezogener Daten in Drittländer

Der Auftragnehmer und etwaige vom Auftragnehmer beauftragte Unterauftragsverarbeiter übermitteln und/oder verarbeiten keine personenbezogenen Daten, die Gegenstand dieses Teil A sind, an/in Drittländer(n), die keine sicheren Drittländer sind, es sei denn der Auftraggeber hat dies vorher ausdrücklich für bestimmte Drittländer genehmigt und die in Kapitel V der DSGVO festgelegten Anforderungen sind erfüllt.

5.2 Standardvertragsklauseln und verbindliche interne Datenschutzvorschriften

- 5.2.1 Unbeschadet der Bedingungen für die Beauftragung eines Unterauftragsverarbeiters (Abschnitt 4.4) erteilt der Auftraggeber dem Auftragnehmer mit Abschluss des jeweiligen Einzelauftrags die Genehmigung, personenbezogene Daten, die Gegenstand des jeweiligen Einzelauftrags und dieses Teil A sind, auf der Grundlage von SVK an Unterauftragsverarbeiter in die im jeweiligen Einzelauftrag bestimmten Drittländer zu übermitteln, die dann solche personenbezogenen Daten auf Grundlage der SVK verarbeiten dürfen.

Zu diesem Zweck schließt der Auftragnehmer (als „Datenexporteur“) mit jedem Unterauftragsverarbeiter in einem Drittland, das kein sicheres Drittland ist, (als „Datenimporteur“) die SVK unter Verwendung des Modul 3 („Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter“) der SVK ab.

- 5.2.2 In Anhang 3 sind gegebenenfalls ergänzende Maßnahmen festgelegt, die der jeweilige Datenimporteur zusätzlich zu den Garantien der SVK treffen muss, um die in Kapitel V der DSGVO festgelegten Anforderungen zu erfüllen.
- 5.2.3 Sobald für den Auftragnehmer genehmigte verbindliche interne Datenschutzvorschriften im Sinne der Art. 46 (2) (b), 47 DSGVO vorliegen, erfolgt die Übermittlung personenbezogener Daten, die Gegenstand dieses Teil A sind, an Drittländer bzw. deren Verarbeitung in Drittländern ausschließlich unter den verbindlichen internen Datenschutzvorschriften, soweit die verbindlichen internen Datenschutzvorschriften die jeweilige Übermittlung bzw. Verarbeitung abdecken. Hierzu erteilt der Auftraggeber dem Auftragnehmer die Genehmigung (vgl. Abschnitt 5.2.1). SVK sind insoweit ab dem Zeitpunkt der Information an den Auftraggeber nicht mehr anzuwenden und nicht mehr nach den oben genannten Regelungen abzuschließen.

5.3 Übermittlungen an vom Verantwortlichen individuell bestimmte Empfänger, die nicht Unterauftragsverarbeiter des Auftragnehmers sind

Auf Einzelweisung des Verantwortlichen übermittelt der Auftragsverarbeiter Daten, die Gegenstand dieses Teil A sind, gemäß der jeweiligen Weisung an vom Verantwortlichen bestimmte Empfänger, die keine Unterauftragsverarbeiter des Auftragnehmers sind. Dabei kann es sich auch um Empfänger in Drittländern handeln.

Der Auftragsverarbeiter wird solche Übermittlungen weisungsgemäß ausführen. Klarstellend halten die Parteien fest, dass die Verantwortung für die Einhaltung der in Kapitel V der DSGVO festgelegten Anforderungen insoweit nicht beim Auftragsverarbeiter, sondern allein bei dem Verantwortlichen liegt.

6. Berufsgeheimnis

Informationen, die Gegenstand dieses Teil A sind, können einem Berufsgeheimnis unterliegen, ungeachtet, ob es sich dabei um personenbezogene Daten handelt oder nicht.

Neben den sonstigen Regelungen dieses Teil A (vgl. Abschnitt 1.3) gilt für die Verarbeitung von Informationen, die einem Berufsgeheimnis unterliegen, Folgendes:

- Die beim Auftraggeber insbesondere als Ärzte tätigen Personen sowie deren berufsmäßig tätigen Gehilfen unterliegen der strafrechtlichen Verschwiegenheitspflicht, insbesondere nach § 203 (1) Nr. 1 StGB. Der Auftraggeber und der Auftragnehmer sind sich darüber einig, dass der Auftragnehmer (einschließlich aller sonstiger mitwirkender Personen) denselben strafrechtlichen Pflichten unterliegt, wie der Berufsgeheimnisträger, soweit er mit Informationen des Auftraggebers in Berührung kommt, die einem Berufsgeheimnis unterliegen.
- Der Auftraggeber weist den Auftragnehmer darauf hin, dass er und sämtliche bei ihm tätige Personen, die mit solchen Informationen in Berührung kommen, sich strafbar machen, wenn sie diese unbefugt Dritten gegenüber offenbaren. Ein Verstoß gegen § 203 (4) Satz 1 StGB kann mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft werden.
- Der Auftragnehmer verpflichtet sich deshalb, (1) sich zu solchen Informationen nur Kenntnis zu verschaffen, soweit dies für die Erfüllung der Auftragsverarbeitungs-Leistungen erforderlich ist, (2) solche Informationen geheim zu halten und (3) dafür Sorge zu tragen, dass diese Dritten gegenüber nicht bekannt werden. Das gilt auch bei Vernehmungen oder Befragungen durch Gerichte, Staatsanwaltschaften, Polizeidienststellen oder sonstige Behörden, sofern der Auftraggeber nicht von der Pflicht zur Verschwiegenheit entbunden ist.
- Der Auftragnehmer ist verpflichtet seine Mitarbeiter sowie die von ihm eingesetzten Unterauftragsverarbeiter, die mit solchen Informationen in Berührung kommen, schriftlich zur Vertraulichkeit zu verpflichten und über die mögliche Strafbarkeit nach § 203 (4) Satz 1 StGB zu belehren sowie sicherzustellen, dass die von ihm eingesetzten Unterauftragsverarbeiter diese Verpflichtung und Belehrung an die jeweils von ihnen eingesetzten Personen weitergeben, die mit solchen Informationen in Berührung kommen können.

Teil B

Vertrag zur gemeinsamen Verantwortlichkeit

7. Anwendungsbereich dieses Teil B

7.1 Anwendungsbereich

Dieser Teil B (Vertrag zur gemeinsamen Verantwortlichkeit) findet Anwendung zwischen dem Auftraggeber und dem jeweiligen Auftragnehmer, soweit diese Parteien für eine Verarbeitung personenbezogener Daten durch den Auftraggeber und den jeweiligen Auftragnehmer als im Sinne des Art. 26 DSGVO gemeinsam für die Verarbeitung Verantwortliche in einem Einzelauftrag festgelegt haben, dass Gemeinsame-Verantwortlichkeits-Leistungen (GV-Leistungen) erbracht werden.

Klarstellend halten die Parteien fest, dass dieser Teil B für sich, also ohne einen solchen Einzelauftrag, noch keine Rechte und Pflichten der Parteien begründet und dass dieser Teil B und der jeweilige Einzelauftrag jeweils nur zwischen dem Auftraggeber und dem jeweiligen Auftragnehmer Anwendung findet, also insoweit keine Rechtswirkung gegenüber dem anderen Auftragnehmer entfaltet, der nicht Vertragspartei des jeweiligen Einzelauftrags ist.

7.2 Parteien und ihre jeweiligen Rollen

Im Rahmen der Erbringung von GV-Leistungen sind der Auftraggeber und der Auftragnehmer gemeinsam für die Verarbeitung Verantwortliche im Sinne des Art. 26 DSGVO.

8. Details der GV-Leistungen

Die GV-Leistungen, deren Zwecke, Mittel und Rechtsgrundlagen, die von diesen Vorgängen betroffenen Kategorien von personenbezogenen Daten und Personen sowie die Funktionen und Beziehungen der Parteien zu den betroffenen Personen im Zusammenhang mit dem jeweiligen Einzelauftrag werden im jeweiligen Einzelauftrag festgelegt.

9. Zuständigkeiten und Verpflichtungen der Parteien

9.1 Erfüllung der Anforderungen der DSGVO

9.1.1 Soweit hierzu im jeweiligen Einzelauftrag oder Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Parteien unterliegen, nichts Abweichendes festgelegt ist, erfüllt jede Partei, die einem Verantwortlichen durch die DSGVO auferlegten Verpflichtungen selbst, um sicherzustellen, dass die gesamte Verarbeitung personenbezogener Daten in gemeinsamer Verantwortlichkeit unter diesem Teil B vollständig den Anforderungen der DSGVO entspricht.

9.1.2 Insbesondere

- gewährleistet jede Partei die Einhaltung der Datenschutzgrundsätze nach Art. 5 DSGVO, insbesondere die Rechtmäßigkeit der von ihr im Rahmen der GV-Leistungen durchgeführten Verarbeitung personenbezogener Daten,
- kommt jede Partei für die in ihrer eigenen Sphäre vorgenommenen GV-Leistungen ihren Informationspflichten gegenüber den betroffenen Personen nach Art. 13 und



14 DSGVO nach und stellt diesen nach Art. 26 (2) Satz 2 DSGVO den wesentlichen Inhalt dieses Teil B und des jeweiligen Einzelauftrags zur Verfügung,

- trifft jede Partei für die in ihrer Sphäre erfolgenden, von diesem Teil B erfassten Verarbeitungsvorgänge in eigener Verantwortung die Maßnahmen, um die mit den Rechten betroffener Personen korrespondierenden Verpflichtungen zu erfüllen,
- dokumentiert jede Partei die Verarbeitungstätigkeiten im Rahmen der von diesem Teil B erfassten Verarbeitungsvorgänge in ihrem Verarbeitungsverzeichnis nach Art. 30 (1) DSGVO, sofern nicht eine Ausnahme von der Verpflichtung nach Art. 30 (5) DSGVO vorliegt,
- kommt jede Partei bei einem Einsatz von Auftragsverarbeitern durch sie für Verarbeitungstätigkeiten im Rahmen der von diesem Teil B erfassten Verarbeitungsvorgänge den Anforderungen des Art. 28 DSGVO nach,
- ergreift jede Partei für Verarbeitungstätigkeiten im Rahmen der von diesem Teil B erfassten Verarbeitungsvorgänge in ihrer eigenen Sphäre die gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen, und
- benennt jede Partei einen eigenen Datenschutzbeauftragten, wenn die Voraussetzungen des Art. 37 DSGVO vorliegen.

9.2 Vertraulichkeit der Personen, die zur Verarbeitung der personenbezogenen Daten berechtigt sind

Die Parteien gewährleisten innerhalb ihrer Sphäre, dass sich die zur Verarbeitung der personenbezogenen Daten, die Gegenstand dieses Teil B sind, befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

9.3 Geltendmachung von Rechten betroffener Personen

- 9.3.1 Die Parteien können im jeweiligen Einzelauftrag eine gemeinsame Anlaufstelle für betroffene Personen festlegen, bei der betroffene Personen ihre Rechte nach der DSGVO im Zusammenhang mit dem jeweiligen Einzelauftrag geltend machen können.
- 9.3.2 Die betroffenen Personen können ihre Rechte nach der DSGVO bei und gegenüber jeder Partei geltend machen, ungeachtet dessen, ob die Parteien eine gemeinsame Anlaufstelle für solche Anfragen bestimmt haben.
- 9.3.3 Jede Partei unterrichtet die andere Partei unverzüglich darüber, wenn eine betroffene Person bei ihr Rechte nach der DSGVO geltend macht, die von diesem Teil B erfasste personenbezogene Daten betreffen.

9.4 Unterstützungs- und Kooperationspflichten

- 9.4.1 Unter Berücksichtigung der Art der Verarbeitung und der ihnen zur Verfügung stehenden Informationen unterstützt jede Partei die jeweils andere bei deren Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen sowie bei der Einhaltung ihrer in den Art. 24, 25 und 30 bis 36 DSGVO genannten Pflichten im angemessenen Umfang.

- 9.4.2 Die Parteien informieren sich gegenseitig unverzüglich und vollständig, wenn eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die von diesem Teil B erfasste personenbezogene Daten betrifft, und stimmen sich vor einer etwaigen Meldung an die Aufsichtsbehörde oder einer etwaigen Benachrichtigung betroffener Personen über deren Inhalt ab.
- 9.4.3 Die Parteien informieren sich gegenseitig unverzüglich und vollständig, wenn eine Anfrage von Aufsichtsbehörden bekannt wird, die von diesem Teil B erfasste personenbezogene Daten betrifft. Die Parteien haben sich bei der Beantwortung solcher Anfragen zu unterstützen und sich miteinander abzustimmen, soweit dies rechtlich zulässig ist.
- 9.4.4 Die Parteien bewahren Nachweise für die datenschutzkonforme Datenverarbeitung über das Vertragsende hinaus auf, solange diese zur Erfüllung der datenschutzrechtlichen Rechenschaftspflicht gemäß Art. 5 (2) DSGVO erforderlich sind. Die Parteien stellen sich solche Nachweise auf Anfrage auch über das Vertragsende hinaus gegenseitig zur Verfügung, soweit das für die jeweils andere Partei zur Erfüllung der datenschutzrechtlichen Rechenschaftspflicht gemäß Art. 5 (2) DSGVO oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

9.5 Konkretisierung der Zuständigkeiten und Verpflichtungen im jeweiligen Einzelauftrag

Der jeweilige Einzelauftrag enthält Konkretisierungen der Zuständigkeiten und Verpflichtungen der Parteien im Zusammenhang mit dem jeweiligen Einzelauftrag. Soweit im jeweiligen Einzelauftrag Abweichungen zu den in diesem Abschnitt 9 enthaltenen Regelungen enthalten sind, gehen die Regelungen im jeweiligen Einzelauftrag den Regelungen in diesem Abschnitt 9 für die Verarbeitung im Zusammenhang mit dem jeweiligen Einzelauftrag vor.

10. Übermittlung personenbezogener Daten in Drittländer

10.1 Übermittlung zwischen den Parteien

Zwischen den Parteien findet grundsätzlich keine Übermittlung personenbezogener Daten in Drittländer im Sinne der Art. 44 ff. DSGVO statt. Sollte dies in einem Einzelfall dennoch eintreten, darf eine Verlagerung in ein Drittland darf nur erfolgen, soweit die in Kapitel V der DSGVO festgelegten Anforderungen erfüllt sind.

10.2 Übermittlungen in der Sphäre einer Partei in Drittländer

Die Parteien übermitteln und/oder verarbeiten personenbezogenen Daten, die Gegenstand dieses Teil B sind, nur an/in Drittlander(n), soweit die in Kapitel V der DSGVO festgelegten Anforderungen erfüllt sind. Der jeweilige Einzelauftrag enthält ggf. Konkretisierungen der Anforderungen an Übermittlungen in Drittländer. Soweit im jeweiligen Einzelauftrag Abweichungen zu den in diesem Abschnitt 10.2 enthaltenen Regelungen enthalten sind, gehen die Regelungen im jeweiligen Einzelauftrag den Regelungen in diesem Abschnitt 10.2 für die Verarbeitung im Zusammenhang mit dem jeweiligen Einzelauftrag vor.

Teil C

Allgemeine Bestimmungen

11. Anwendungsbereich dieses Teil C

Dieser Teil C (Allgemeine Bestimmungen) dieses Datenschutz-Rahmenvertrages gilt für sämtliche Tätigkeiten, die Gegenstand dieses Datenschutz-Rahmenvertrages sind, unabhängig davon, ob diese unter Teil A oder Teil B fallen.

12. Begriffsbestimmungen

12.1 Begriffsbestimmungen der DSGVO

Für die Zwecke dieses Datenschutz-Rahmenvertrages finden die Begriffsbestimmungen des Art. 4 DSGVO Anwendung, sofern nachfolgend in Abschnitt 12.2 nichts anderes bestimmt ist.

12.2 Besondere Begriffsbestimmungen dieses Datenschutz-Rahmenvertrages

Für die Zwecke dieses Datenschutz-Rahmenvertrages, finden die folgenden abweichenden und/oder zusätzlichen Begriffsbestimmungen Anwendung:

- 12.2.1 **„Auftragsverarbeitungs-Leistungen“** oder **„AV-Leistungen“** sind die vom jeweiligen Auftragnehmer für den Auftraggeber im Rahmen eines Hauptvertrages als Auftragsverarbeiter zu erbringenden Leistungen, wie sie im jeweiligen Einzelauftrag beschrieben sind.
- 12.2.2 **„Datenschutz-Grundverordnung“** oder **„DSGVO“** ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016.
- 12.2.3 **„Einzelauftrag“** ist eine Vereinbarung zwischen dem Auftraggeber und einem der Auftragnehmer, die auf diesen Datenschutz-Rahmenvertrag Bezug nimmt und die Auftragsverarbeitungs-Leistungen und/oder GV-Leistungen nach Teil A und/oder Teil B zum Gegenstand hat.
- 12.2.4 **„Gemeinsame-Verantwortlichkeits-Leistungen“** oder **„GV-Leistungen“** sind die im Rahmen eines Hauptvertrages vom jeweiligen Auftragnehmer und dem Auftraggeber als gemeinsame Verantwortliche zu erbringenden Leistungen, wie sie im jeweiligen Einzelauftrag beschrieben sind.
- 12.2.5 **„Hauptvertrag“** ist der im jeweiligen Einzelauftrag als solcher bezeichnete Vertrag.
- 12.2.6 **„Parteien“** (oder einzeln eine „Partei“) sind der Auftraggeber und die Auftragnehmer. Soweit Teile dieses Datenschutz-Rahmenvertrages im Rahmen eines Einzelauftrags nur zwischen dem Auftraggeber und einem der Auftragnehmer Anwendung finden, bezieht sich der Begriff „Partei“/„Parteien“ insoweit nur auf den Auftraggeber und den jeweiligen Auftragnehmer.
- 12.2.7 **„Standardvertragsklauseln“** oder **„SVK“** sind die Standardvertragsklauseln, die dem Durchführungsbeschluss (EU) 2021/914 der Europäischen Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer (wie im Amtsblatt der Europäischen Union veröffentlicht OJ L 199, 7.6.2021, S. 31 - 61 (DE) (<https://eur-lex.europa.eu/eli/dec/2021/914/oj>) anhängen.

13. Haftung

Die Haftung der Parteien richtet sich nach den im jeweiligen Hauptvertrag enthaltenen Haftungsregelungen und soweit dort keine Haftungsregelungen enthalten sind nach den anwendbaren gesetzlichen Regelungen.

14. Inkrafttreten, Laufzeit und Beendigung

14.1 Inkrafttreten und Laufzeit

14.1.1 Dieser Datenschutz-Rahmenvertrag tritt mit der Unterzeichnung durch beide Parteien in Kraft.

14.1.2 Dieser Datenschutz-Rahmenvertrag gilt unbefristet und ist vor Beendigung sämtlicher Hauptverträge und Einzelaufträge, die diesen Datenschutz-Rahmenvertrag in Bezug nehmen, nicht kündbar.

14.1.3 Sofern die Erbringung der Verarbeitungsleistungen, die Gegenstand dieses Datenschutz-Rahmenvertrages sind, nach Beendigung des Hauptvertrages noch nicht abgeschlossen ist, oder im Fall von Teil A der Auftragsverarbeiter sonst nach Beendigung des jeweiligen Hauptvertrages noch personenbezogene Daten verarbeitet, die Gegenstand von Teil A sind, endet die Laufzeit dieses Datenschutz-Rahmenvertrages und der betroffenen Einzelaufträge abweichend von Abschnitt 14.1.2 frühestens mit dem Abschluss der Erbringung der Verarbeitungsleistungen und im Fall von Teil A der vollständigen Löschung oder Rückgabe der personenbezogenen Daten an den Verantwortlichen nach Abschluss der Erbringung der Verarbeitungsleistungen gemäß Abschnitt 4.6.

15. Anwendbares Recht und Gerichtsstand

Dieser Datenschutz-Rahmenvertrag unterliegt dem Recht des Landes, in dem der Auftragnehmer seine Hauptniederlassung hat.

Für alle Streitigkeiten, die im Zusammenhang mit diesem Datenschutz-Rahmenvertrag stehen, ist der ausschließliche Gerichtsstand, der Gerichtsstand Stuttgart.

16. Schlussbestimmungen

16.1 Änderungen und Ergänzungen dieses Datenschutz-Rahmenvertrages

Änderungen und Ergänzungen dieses Datenschutz-Rahmenvertrages bedürfen der Schriftform. Dies gilt auch für den Verzicht auf das Schriftformerfordernis.

Gescannte Kopien der im Original unterzeichneten Dokumente sowie elektronisch unterzeichnete Dokumente, auch ohne qualifizierte elektronische Signatur, genügen der Schriftform und gelten als Originale.

16.2 Salvatorische Klausel

Sollte eine Regelung dieses Datenschutz-Rahmenvertrages ganz oder teilweise unwirksam oder nicht durchsetzbar sein oder werden, berührt dies nicht die Gültigkeit der übrigen Regelungen. Die Parteien verpflichten sich, die unwirksame oder nicht durchsetzbare Regelung gemeinsam durch eine wirksame Regelung zu ersetzen, die der unwirksamen oder nicht



durchsetzbaren Regelung, soweit dies möglich ist entspricht. Gleiches gilt für jegliche Regelungslücken dieses Datenschutz-Rahmenvertrages.

16.3 Rangfolge

Bei Widersprüchen zwischen diesem Datenschutz-Rahmenvertrag und anderen zwischen den Parteien geschlossenen Vereinbarungen, insbesondere dem jeweiligen Hauptvertrag, haben die Regelungen dieses Datenschutz-Rahmenvertrages Vorrang. Bei Widersprüchen zwischen diesem Datenschutz-Rahmenvertrag und einem Einzelauftrag, der auf diesen Datenschutz-Rahmenvertrag Bezug nimmt, haben die Regelungen des jeweiligen Einzelauftrags für Tätigkeiten unter dem jeweiligen Einzelauftrag Vorrang.



Anhänge:

Anhang 1: Einzelheiten zu den Parteien

Anhang 2: Sicherheitsmaßnahmen

Anhang 3: Ergänzende Maßnahmen zu den Standardvertragsklauseln



Auftraggeber:

Ort, Datum

Name: _____
Position: _____

Name: _____
Position: _____

Auftragnehmer:

Carl Zeiss Meditec Vertriebsgesellschaft mbH

Oberkochen, 01.07.2023

Arne Schmid

Geschäftsführer

Oberkochen, 01.07.2023

i.V.

Felix Mayer

Leiter Qualitätsmanagement

Datenschutzkoordinator CZ M VG

Carl Zeiss Meditec AG

Oberkochen, 01.07.2023

ppa.

Dr. Till Sellschopp

Head of Legal

Oberkochen, 01.07.2023

i.V.

Dietmar Mischke

Head of IT

Datenschutzkoordinator CZ M AG



Anhang 1 Einzelheiten zu den Parteien

1. Für Einzelweisungen autorisierte Personen der Parteien (für AV-Leistungen)

1.1 Auftraggeber

Name	
Adresse	
Telefon	
Telefax	
E-Mail	

1.2 Auftragnehmer

Auftragnehmer	Carl Zeiss Meditec Vertriebsgesellschaft mbH
Weisungsbefugte Funktion	Leiter/in Service
Stelleninhaber/in bei Vertragsabschluss	Dr. Markus Hammann
Adresse	Rudolf-Eber-Straße 11, 73441 Oberkochen
Telefon	+49 800 4357 633
Telefax	+49 7364 20 4939
E-Mail	service.meditec.de@zeiss.com

Auftragnehmer	Carl Zeiss Meditec AG
Weisungsbefugte Funktion	Head of IT
Stelleninhaber/in bei Vertragsabschluss	Dietmar Mischke
Adresse	Göschwitzer Str. 51-52, 07745 Jena
Telefon	+49 3641 2200
E-Mail	info.meditec.de@zeiss.com



2. Datenschutzbeauftragte der Parteien

2.1 Auftraggeber

Name	
Adresse	
Telefon	
Telefax	
E-Mail	

2.2 Auftragnehmer

Auftragnehmer	Carl Zeiss Meditec Vertriebsgesellschaft mbH
Name	Konzerndatenschutzbeauftragter der Carl Zeiss AG
Adresse	Carl-Zeiss-Straße 22, 73447 Oberkochen
Telefon	+497364200 (Stichwort „Datenschutz“)
E-Mail	dataprivacy@zeiss.com

Auftragnehmer	Carl Zeiss Meditec AG
Name	Konzerndatenschutzbeauftragter der Carl Zeiss AG
Adresse	Carl-Zeiss-Straße 22, 73447 Oberkochen
Telefon	+497364200 (Stichwort „Datenschutz“)
E-Mail	dataprivacy@zeiss.com



Anhang 2 Sicherheitsmaßnahmen

1 Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit		
1.1	T-01 Belastbarkeit und Kontinuität	Die relevanten Maßnahmen sind auftragsspezifisch und werden daher bei Bedarf im entsprechenden Einzelauftrag definiert.
1.2	T-02 Sicherung und Wiederherstellung	Die relevanten Maßnahmen sind auftragsspezifisch und werden daher bei Bedarf im entsprechenden Einzelauftrag definiert.
1.3	O-01 Vorfallsmanagement	Definierter und etablierter Plan zur Reaktion auf Vorfälle, der alle notwendigen Stakeholder einschließt.
1.4	O-02 Risikomanagement	Jede Verarbeitung personenbezogener Daten wird mittels einer Risikobewertung beurteilt, um eine Risikoklasse mit entsprechenden Maßnahmen zu bestimmen.
1.5	T-03 Trennung von Umgebungen/Tests	Die relevanten Maßnahmen sind auftragsspezifisch und werden daher bei Bedarf im entsprechenden Einzelauftrag definiert.
1.6	O-03 Schulung und Sensibilisierung	Regelmäßige verpflichtende Sensibilisierungsmaßnahmen zu Datenschutz, Informationssicherheit und Compliance für alle Mitarbeiter.
		Sämtliche an der Datenverarbeitung beteiligten Mitarbeiter sind zur Verschwiegenheit und zur Einhaltung des Datenschutzes verpflichtet und werden diesbezüglich regelmäßig geschult.
		Qualifizierungsprogramm für Security Engineers in den Bereichen Informationssicherheit, Datenschutz und FOSS-Compliance.
1.7	O-04 Physische Sicherheit	Daten werden grundsätzlich ausschließlich in einer gesicherten Umgebung verarbeitet.
		Weitere relevante Maßnahmen sind auftragsspezifisch und werden daher bei Bedarf im entsprechenden Einzelauftrag definiert.
1.8	O-05 Unterauftragsverarbeiter	ZEISS und mögliche Unterauftragsverarbeiter schließen einen Vertrag mit Verpflichtungen, die im Wesentlichen denen aus dem Vertrag zwischen dem Verantwortlichen und ZEISS ähneln und das Datenschutzniveau nicht absenken.
		Regelmäßige Durchführung risikobasierter Audits.
2 Maßnahmen zur Identifizierung und Autorisierung der Nutzer		
2.1	T-04 Zugangs- und Zugriffskontrolle	Es findet eine regelmäßige Überprüfung der Zugangsrechte statt.
		Benutzernamen und Passwörter müssen eindeutig sein.
		Es existieren Vorgaben für sichere Passwörter.

	Weitere relevante Maßnahmen sind auftragsspezifisch und werden daher bei Bedarf im entsprechenden Einzelauftrag definiert.
	Der Zugriff auf personenbezogene Daten ist auf autorisierte Personen beschränkt.
	Die Gewährung von Zugriffsrechten folgt allgemeinen Grundsätzen wie "least privilege" und "need to know".
3 Maßnahmen zum Schutz der Daten während der Übermittlung	
3.1 T-05 Verschlüsselung (Data-in-Transit)	Die relevanten Maßnahmen sind auftragsspezifisch und werden daher bei Bedarf im entsprechenden Einzelauftrag definiert.
4 Maßnahmen zum Schutz der Daten während der Speicherung	
4.1 T-06 Architektur und Datentrennung	Die relevanten Maßnahmen sind auftragsspezifisch und werden daher bei Bedarf im entsprechenden Einzelauftrag definiert.
4.2 T-07 Verschlüsselung (Data-at-Rest)	Die relevanten Maßnahmen sind auftragsspezifisch und werden daher bei Bedarf im entsprechenden Einzelauftrag definiert.
5 Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen	
5.1 T-08 Protokollierung und Überwachung	Die relevanten Maßnahmen sind auftragsspezifisch und werden daher bei Bedarf im entsprechenden Einzelauftrag definiert.
6 Maßnahmen zur Gewährleistung der Datenminimierung	
6.1 O-06 Verbindliche Datenschutzgrundsätze	Es gelten die Binding Corporate Rules* als ZEISS weiter "Verhaltenskodex" für die Verarbeitung von personenbezogenen Daten.
7 Maßnahmen zur Gewährleistung der Datenqualität	
7.1 O-07 Verbindliche Datenschutzgrundsätze	Es gelten die Binding Corporate Rules* als ZEISS weiter "Verhaltenskodex" für die Verarbeitung personenbezogener Daten mit Hinweisen zur Datenqualität.
8 Maßnahmen zur Gewährleistung einer begrenzten Datenspeicherung	
8.1 O-08 Verbindliche Datenschutzgrundsätze	Es gelten die Binding Corporate Rules* als ZEISS weiter "Verhaltenskodex" für die Verarbeitung personenbezogener Daten mit Anweisungen zur Speicherbegrenzung und zum Informationslebenszyklus.
	Die Klassifizierung von Informationen ist verpflichtend.
9 Maßnahmen zur Gewährleistung der Rechenschaftspflicht	
9.1 O-09 Verbindliche Datenschutzgrundsätze	Es gelten die Binding Corporate Rules* als ZEISS-weiter "Verhaltenskodex" für die Verarbeitung personenbezogener Daten mit Anweisungen zur Dokumentation und Rechenschaftspflicht.



	Es existiert eine konzernweit einheitliche Datenbank für die Aufzeichnung von Verarbeitungstätigkeiten.
	Laufende Überwachung der Dokumentationsqualität und Audits.
10 Maßnahmen zur Gewährleistung der Rechte der betroffenen Person	
10.1 O-10 Verbindliche Datenschutzgrundsätze	Es gelten die Binding Corporate Rules* als ZEISS-weiter "Verhaltenskodex" für die Verarbeitung personenbezogener Daten mit Hinweisen zur Wahrung der Betroffenenrechte. Weitere relevante Maßnahmen werden bei Bedarf in den Einzelaufträgen definiert
11 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen	
11.1 O-11 Sicherheitsorganisation	Implementiertes Informationssicherheits-Management-system, welches sich an ISO/IEC 27001 orientiert und alle relevanten Bereiche abdeckt.
	Durchführung interner und externer Audits.
	Implementiertes Risikomanagement für Anbieter.
	Ressourcenausstattung und Berichtswege sind angemessen.
	Regelmäßige Aktualisierung und Überprüfung der relevanten Vorgaben.
11.2 O-12 Datenschutzorganisation	Es existiert eine weltweite Datenschutzorganisation mit einem Konzerndatenschutzbeauftragten und Datenschutzkoordinatoren im gesamten Unternehmen.
	Etabliertes Datenschutzmanagementsystem, das sich an ISO/IEC 27701 orientiert.
	Durchführung interner und externer Audits.
	Ressourcenausstattung und Berichtswege sind angemessen.
	Regelmäßige Aktualisierung und Überprüfung der relevanten Vorgaben.
11.3 T-09 Penetrationstests	Die relevanten Maßnahmen sind auftragsspezifisch und werden daher bei Bedarf im entsprechenden Einzelauftrag definiert.
11.4 O-13 Zertifizierungen (Definition: Gemeint sind Zertifizierungen, die für die konkrete Datenverarbeitung gelten; bescheinigt durch eine unabhängige externe Prüfung oder Zertifizierungsstelle)	Die relevanten Maßnahmen sind auftragsspezifisch und werden daher bei Bedarf im entsprechenden Einzelauftrag definiert.
*Die Binding Corporate Rules der ZEISS Gruppe werden derzeit von der zuständigen Aufsichtsbehörde (Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg) geprüft. Sobald uns eine endgültige Entscheidung der Aufsichtsbehörde zu den BCR vorliegt, finden Sie auf unserer Website eine öffentliche Zusammenfassung mit den relevanten Aspekten. Unsere Öffentliche Datenschutzleitlinie finden Sie hier .	



Anhang 3

Ergänzende Maßnahmen zu den Standardvertragsklauseln

Beschreibung der ergänzenden Maßnahmen, die Datenimporteure zusätzlich zu den Garantien der Standardvertragsklauseln treffen:

Gegebenenfalls erforderliche ergänzende Maßnahmen, werden im entsprechenden Einzelauftrag definiert.