Datenschutzrechtliche Vereinbarung zur Auftragsverarbeitung (AV)

i.S.d. Art. 28 Abs. 3 EU-Datenschutz-Grundverordnung (DSGVO)

Zwischen

.....

.....

.....

.....

- Verantwortlicher, nachfolgend „**AUFTRAGGEBER**“ genannt -

und

Carl Zeiss Meditec Vertriebsgesellschaft mbH

Rudolf-Eber-Straße 11

73447 Oberkochen, Deutschland

- Auftragsverarbeiter, nachfolgend „**AUFTRAGNEHMER**“ genannt

AUFTRAGGEBER und AUFTRAGNEHMER werden nachfolgend „VERTRAGSPARTEI“ oder gemeinsam „VERTRAGSPARTEIEN“ genannt.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand
Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag mit

der Bezeichnung: ..... **und Nr.:** .....

Falls kein Hauptvertrag besteht beziehungsweise ergänzend falls im Hauptvertrag eine der unten aufgeführten Aufgaben nicht aufgeführt ist, ist der Gegenstand des Auftrags zum Datenumgang die Durchführung folgender Aufgaben durch den AUFTRAGNEHMER.

Intraokularlinsen

1. Bestellungen von Intraokularlinsen und von Verbrauchsmaterial beliefern
2. Implantationsmeldungen bearbeiten
3. Linsenberechnungen supporten
4. Konsignationslager betreuen

Serviceleistungen an den von dem AUFTRAGNEHMER vertriebenen Produkten und Systemen

1. Installationen und Einweisungen durchführen
2. Fernwartung / Remote Support durchführen
3. ZEISS Smart Services durchführen
4. Vorortinstandsetzungen (Reparatur oder Wartung) durchführen
5. Werksinstandsetzungen (Reparatur oder Wartung) durchführen
6. Demontage und Entsorgung

Zusätzlich können die oben aufgeführten Aufgaben auch an den Produkten und Systemen durch den AUFTRAGNEHMER durchgeführt werden, die nicht in dem Hauptvertrag aufgeführt sind.

(2) Dauer
Die Laufzeit der AV entspricht der Laufzeit des Hauptvertrages. Liegt kein Hauptvertrag vor, dann ist die Laufzeit unbefristet und kann mit einer Frist von einem Monat zum Monatsende gekündigt werden.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Art und Zweck der Verarbeitung personenbezogener Daten durch den AUFTRAGNEHMER für den AUFTRAGGEBER sind konkret beschrieben im Hauptvertrag beziehungsweise in Art. 1.
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 Artt. 44 ff. DSGVO erfüllt sind.
Wenn der Auftragsverarbeiter seinen Sitz in einem Drittland hat, schließen der Auftragsverarbeiter und der Auftraggeber im eigenen Namen mit Abschluss der vorliegenden Vereinbarung zugleich die Standarddatenschutzklauseln gem. Art. 46 Abs. 2 litt. c und d DS-GVO ab. Der Auftraggeber tritt in die Standarddatenschutzklauseln als Datenexporteur ein, der Auftragsverarbeiter als Datenimporteur. Für Anhang 2 der Standarddatenschutzklauseln gelten die Inhalte der Anlage 1 (TOM). Diese Regel zum Abschluss der Standarddatenschutzklauseln gilt nicht, wenn die EU Kommission entschieden hat, dass das Land, in dem der Auftragsverarbeiter seinen Sitz hat und die betreffende Datenverarbeitung erbringt, ein angemessenes Datenschutzniveau bietet.

(2) Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind die in der Anlage 1 beschriebenen Datenarten/-kategorien.

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Anlage 1 beschrieben.

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 zu dokumentieren und dem AUFTRAGGEBER zur Prüfung zu übergeben. Bei Akzeptanz durch den AUFTRAGGEBER werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des AUFTRAGGEBERS einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der AUFTRAGNEHMER hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen [Einzelheiten in Anlage 1].

(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 darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des AUFTRAGGEBERS berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich oder in Ausübung anderweitiger Rechte (insbesondere Kapitel 3 der DSGVO) unmittelbar an den AUFTRAGNEHMER wendet, wird der AUFTRAGNEHMER dieses Ersuchen unverzüglich an den AUFTRAGGEBER weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des AUFTRAGGEBERS unmittelbar durch den AUFTRAGNEHMER sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des AUFTRAGNEHMERs

Der AUFTRAGNEHMER hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten gemäß Anlage 1, der seine Tätigkeit gemäß Artt. 38 und 39 DSGVO ausübt. Ein Wechsel des Datenschutzbeauftragten wird dem AUFTRAGGEBER unverzüglich mitgeteilt.

b) Soweit der AUFTRAGNEHMER seinen Sitz außerhalb der Union hat, ist der in Anlage 1 bezeichnete Vertreter nach Art. 27 Abs. 1 DSGVO in der Union bestimmt. Ein Wechsel wird dem AUFTRAGGEBER unverzüglich mitgeteilt.

c) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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 durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, gesetzlich zur Verarbeitung verpflichtet sind. Der Auftragnehmer teilt dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DSGVO, insbesondere der in Anlage 1 festgelegten Maßnahmen.
e) Der AUFTRAGGEBER und der AUFTRAGNEHMER arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
f) 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.
g) 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 (insbesondere der Erfüllung seiner Pflichten nach Kapitel 3 der DSGVO), hat ihn der AUFTRAGNEHMER angemessen sowie mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen.
h) Der AUFTRAGNEHMER kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
i) 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 in Anspruch nimmt, wie z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. 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 erhält die grundsätzliche Genehmigung UNTERAUFTRAGNEHMER (weitere Auftragsverarbeiter)) zu beauftragen. Dabei sind die in Anlage 2 vereinbarten Bestimmungen zu beachten.

(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) Erbringt der UNTERAUFTRAGNEHMER die vereinbarte Leistung außerhalb der EU/des EWR stellt der AUFTRAGNEHMER die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Im Falle einer weiteren Auslagerung durch den AUFTRAGNEHMER sind sämtliche vertraglichen Regelungen in der Vertragskette auch dem weiteren UNTERAUFTRAGNEHMER aufzuerlegen.
(6) Soweit (i) nicht gemäß Ziffer 2 mit Abschluss der vorliegenden Vereinbarung zugleich die Standarddatenschutzklauseln abgeschlossen wurden, und (ii) der Auftraggeber der Einschaltung von Unterauftragnehmern im Drittland zugestimmt hat, schließt der Auftragsverarbeiter im Namen und in Vertretung dieser Unterauftragnehmer die Standarddatenschutzklauseln für den bzw. mit dem Auftraggeber (Ermächtigung). Die Unterauftragnehmer schließen die Standarddatenschutzklauseln als Datenimporteure ab, der Auftraggeber als Datenexporteur. Für Anhang 2 der Standarddatenschutzklauseln gelten die Inhalte der Anlage 1 (TOM). Diese Regel zum Abschluss der Standarddatenschutzklauseln gilt nicht, wenn die EU

Kommission entschieden hat, dass das Land, in dem der Auftragsverarbeiter seinen Sitz hat und die betreffende Datenverarbeitung erbringt, ein angemessenes Datenschutzniveau bietet.

7. Kontrollrechte des AUFTRAGGEBERS

(1) Der AUFTRAGGEBER hat das Recht, im Benehmen 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 den üblichen Geschäftszeiten (maximal 1 Mal jährlich) zu überzeugen.

(2) Der AUFTRAGNEHMER stellt sicher, dass sich der AUFTRAGGEBER von der Einhaltung der Pflichten des AUFTRAGNEHMERs nach Art. 28 DSGVO überzeugen kann. Der AUFTRAGNEHMER verpflichtet sich, dem AUFTRAGGEBER auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz oder ISO 27001).
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

(4) Jede VERTRAGSPARTEI hat die hieraus entstehenden Kosten selbst zu tragen.

8. Mitteilung bei Verstößen des AUFTRAGNEHMERs

(1) Der AUFTRAGNEHMER unterstützt den AUFTRAGGEBER bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO 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 nicht auf ein Fehlverhalten des AUFTRAGNEHMERs zurückzuführen sind, kann der AUFTRAGNEHMER eine Vergütung beanspruchen.

(3) Der AUFTRAGGEBER informiert den AUFTRAGNEHMER unverzüglich, wenn er Fehler oder sonstige Unregelmäßigkeiten bei den Verarbeitungsergebnissen feststellt, insbesondere wenn er Grund zu der Annahme hat, dass die Art und Weise der Datenverarbeitung durch den AUFTRAGNEHMER gegen datenschutzrechtliche Anforderungen verstößt.

9. Weisungsbefugnis des AUFTRAGGEBERS

(1) Mündliche Weisungen bestätigt der AUFTRAGGEBER unverzüglich (mind. Textform). Weisungen sind vom AUFTRAGGEBER für ihre Gültigkeitsdauer und anschließend noch für drei Jahre aufzubewahren.

(2) Der AUFTRAGNEHMER hat den AUFTRAGGEBER unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der AUFTRAGNEHMER ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den AUFTRAGGEBER bestätigt oder geändert wird.

(3) Der AUFTRAGGEBER erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Der AUFTRAGNEHMER verarbeitet Kundenanfragen, in welchen Bezüge zu Patientendaten enthalten sind nur dann, wenn die datenschutzrechtlichen Anforderungen beachtet werden. Diese sind insbesondere:

a) Die Übermittlung erfolgt mittels eines elektronischen Verschlüsselungsverfahren, welches dem aktuellen Stand der Technik entspricht.
b) Die Patientendaten werden mindestens in pseudonymisierter Form übermittelt.

Sollte für die Verarbeitung von Patientendaten eine Einwilligungserklärung erforderlich sein, ist der AUFTRAGGEBER dafür verantwortlich, dass diese zweckbezogene Einwilligungserklärung vom Patienten zur Verarbeitung seiner personenbezogenen Daten unterschrieben vorliegt und archiviert wird.

10. 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 des 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. 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.

11. Haftung

Die VERTRAGSPARTEIEN haften im Rahmen ihrer jeweiligen Verantwortlichkeiten gemäß den gesetzlichen Bestimmungen des Art. 82 DSGVO gegenüber Dritten für Schäden, die durch eine nicht der DSGVO entsprechenden Datenverarbeitung entstanden sind.

12. Schlussbestimmungen

(1) Diese datenschutzrechtliche Vereinbarung ersetzt alle bisherigen Vereinbarungen zur Auftragsdatenverarbeitung zwischen den VERTRAGSPARTEIEN.

(2) Diese Vereinbarung sowie alle Änderungen und Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform. Gescannte Kopien der im Original unterzeichneten Dokumente, wie zum Beispiel PDF-Kopien, sowie elektronisch unterzeichnete Dokumente genügen der Schriftform und gelten als Originale. Das Schriftformerfordernis gilt nicht für die Aktualisierung der Anlagen, hier ist die Textform z.B. per E-Mail ausreichend. Sofern in den Anlagen hinsichtlich Änderungen keine andere Regelung festgelegt ist, benötigt jede Änderung der Anlagen für ihre Wirksamkeit die Bestätigung durch die jeweils andere VERTRAGSPARTEI schriftlich oder in einem dokumentierten elektronischen Format. Die VERTRAGSPARTEIEN hinterlegen in

Anlage 1 eine Liste der jeweils autorisierten Personen, die eine Änderung der Anlagen initiieren oder bestätigen dürfen.

(3) Wenn und soweit Vorgaben der Aufsichtsbehörden und/oder zusätzliche gesetzliche Vorgaben die Änderung von Bestimmungen der datenschutzrechtlichen Vereinbarung und/oder der zugehörigen Anlagen erforderlich machen, sind die VERTRAGSPARTEIEN verpflichtet, an der Umsetzung der Anforderungen und der Aufnahme in die datenschutzrechtliche Vereinbarung mitzuwirken. Vorgaben der für die vom Auftrag umfasste Datenverarbeitung zuständigen Aufsichtsbehörde oder einer sonstigen zuständigen offiziellen Stelle sind dabei als verbindlich zu betrachten.

Bitte schicken Sie uns ein unterschriebenes Exemplar an folgende E-Mail: qm.mvg.meditec.de@zeiss.com

Unterschrift(en) AUFTRAGGEBER

.....
Ort, Datum

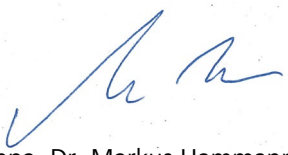
.....	.....
Unterschrift	Unterschrift
.....	.....
Name, Vorname	Name, Vorname
.....	.....
Funktion	Funktion

Unterschriften AUFTRAGNEHMER

Oberkochen, 01. April 2021

Christian Steinmetz

Geschäftsführer



ppa. Dr. Markus Hammann

Leiter Services

Anlage 1 – Datenschutzseitige Zuverlässigkeit und technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung personenbezogener Daten

1. Allgemeine Angaben

1.1. Datenarten und Datenkategorien

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

- Gesundheitsdaten oder genetische Daten
- Authentifizierungsdaten
- Identifikationsdaten (Name, UID, etc.)
- Demographische Daten
- Biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
- Finanzdaten
- Kommunikationsdaten
- Kontakt- und Adressdaten

1.2 Kategorien betroffener Personen

Von der Verarbeitung sind folgende Kategorien betroffener Personen umfasst:

- Kunden
- Interessenten
- Patienten
- Lieferanten
- Abonnenten
- Probanden

1.3 Datenschutzbeauftragte/r des AUFTRAGNEHMERs

Beim AUFTRAGNEHMER ist als Beauftragte(r) für den Datenschutz bestellt:

Andreas Karl
Corporate Data Protection Officer
Corporate Legal and Patents
Carl Zeiss AG
Carl-Zeiss-Straße 22
73447 Oberkochen, Germany

Phone: +49 7364 20 3841
Mobile: +49 175 6280206
Fax: +49 7364 20 3911
dataprivacy@zeiss.com

1.4 Besteht eine Vertraulichkeitsverpflichtung mit allen Mitarbeitern, die mit der Verarbeitung personenbezogener Daten beauftragt sind?

☒ Ja ☐ Nein

1.5 In welcher Weise wurden/werden Mitarbeiter, die mit der Verarbeitung personenbezogener Daten beauftragt sind, im Datenschutz geschult oder eingewiesen?

Mitarbeiter, welche mit personenbezogenen Daten in Berührung kommen können, werden regelmäßig auf die Einhaltung der konzernweit gültigen und der speziell im Anwendungsbereich gültigen Datenschutzregeln geschult. Diese Schulungen werden regelmäßig wiederholt und aktualisiert.

1.6 Der AUFTRAGNEHMER hat die im 2. Abschnitt dieser Anlage dokumentierten technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 DSGVO implementiert.

☒ Ja ☐ Nein

1.7 Für den AUFTRAGNEHMER ist folgende Aufsichtsbehörde zuständig:

Für die Carl ZEISS AG, als übergeordnete Instanz der ZEISS-Gruppe:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI)
Königstraße 10 a, 70173 Stuttgart

Tel.: +49 (0)711 6155410

1.8 Bitte bezeichnen Sie die Orte (inkl. Land) der Datenverarbeitung:

Bundesrepublik Deutschland

1.9 Erfolgt eine Datenübermittlung in sog. Drittländer (außerhalb der EU bzw. des EWR) oder an internationale Organisationen?

☒ Ja ☐ Nein

Wenn ja, bitte geben Sie die Maßnahmen zur Herstellung eines angemessenen Schutzniveaus an:

☐ Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DSGVO);

☒ Verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DSGVO);

☐ Feststellung durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO);

☐ Genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e i.V.m. 40 DSGVO);

☐ Genehmigter Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DSGVO).

☐ Sonstige Maßnahmen (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DSGVO):

_____

_____

1.10.1 Weisungsbefugte Ansprechpartner und Verantwortliche des AUFTRAGGEBERS:

Name und Vorname	Funktion	Kontaktdaten

1.10.2. Weisungsbefugte Ansprechpartner und Verantwortliche des AUFTRAGNEHMERs:

Name und Vorname	Funktion	Kontaktdaten
Wolff, Bernd	Regionaler Serviceleiter (Süd / Süd-Ost)	0800-4357633 service.meditec.de@zeiss.com
Enssle, Steffen	Leiter Kundenzentrum Vertrieb	07364-206000 vertrieb.meditec.de@zeiss.com
Ott, Juergen	Regionaler Serviceleiter (Nord-West)	0800-4357633 service.meditec.de@zeiss.com
Kraft, Stefanie	Leiterin Kundenzentrum IOL und Verbrauchsmaterialien	0800-4705030 iol.meditec.de@zeiss.com
Oelze-de-Stoppany, Gerald	Regionaler Serviceleiter (Süd-West)	0800-4357633 service.meditec.de@zeiss.com
Pfalzgraf, Christian	Leiter Vertrieb und Marketing Digitalisierungslösungen	07364-206000 vertrieb.meditec.de@zeiss.com

2. Implementierte technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 EU Datenschutz-Grundverordnung (DSGVO)

	Maßnahme
1.	**Zentrale Vorgaben**
1.1.	Es existieren interne Richtlinien zu Datenschutz.
1.2.	Diese Richtlinien bzw. deren Inhalte sind den an der Verarbeitung beteiligten Mitarbeitern zugänglich.
2.	**Organisation**
2.1.	Es ist ein Sicherheitsverantwortlicher benannt.
2.2.	Es ist ein Datenschutzbeauftragter benannt.
2.3.	Es ist eine interne Revision vorhanden.
2.4.	Es finden Schulungen und Sensibilisierungsmaßnahmen zu Datenschutz, Informationssicherheit und Compliance statt.
3.	**Personalsicherheit**
3.1.	Der Eintritt, Wechsel und Austritt von Personal ist geregelt.
3.2.	Es erfolgt eine sorgfältige Auswahl von Personal mit sensiblen Zugangs- & Zutrittsrechten.
4.	**Verwaltung von Werten**
4.1.	Es sind Regelungen für die Rückgabe von Werten (u. a. Geräte, Software, Berechtigungen, Schlüssel) vorhanden.
4.2.	Es ist eine Informationsklassifizierung vorhanden.
5.	**Zugangs- und Zutrittssteuerung**
5.1.	Es sind Regelungen für den Zutritt vorhanden.
5.2.	Es sind Regelungen für den Zugriff vorhanden.
5.3.	Es sind Regelungen für sichere Kennwörter vorhanden.
5.4.	Sensible Bereiche sind gesondert gegen Unbefugte gesichert.
6.	**Kryptografie (u. a. Verschlüsselung)**
6.1.	Es werden kryptografische Verfahren für die Absicherung des Datenaustausches verwendet.
7.	**Physische und umgebungsbezogene Sicherheit**
7.1.	Schützenswerte Bereiche sind durch entsprechende Maßnahmen physisch gesichert.
7.2.	Systeme sind gegen externe Einflüsse, sowie Umwelteinflüsse gesichert.
8.	**Betriebssicherheit**
8.1.	Es sind Dokumentationen zu Betriebsabläufen vorhanden.
8.2.	Es sind Maßnahmen zum Schutz vor Schadsoftware getroffen.
8.3.	Es sind Protokollierungs- und Überwachungsmechanismen implementiert.
8.4.	Es sind Maßnahmen zum Schutz vor Datenverlust getroffen.
8.5.	Den Systemen stehen ausreichende Ressourcen zur Verfügung.
9.	**Kommunikationssicherheit**
9.1.	Es sind Netzwerksicherheitsmaßnahmen getroffen (u. a. Firewall).
9.2.	Es sind Maßnahmen für eine sichere und verfügbare Datenübertragung getroffen.
10.	**Handhabung von Sicherheits- und Datenschutzvorfällen**
10.1.	Es ist ein Vorgehen zur Behandlung von Sicherheits- und Datenschutzvorfällen vorhanden.
11.	**Compliance**
11.1.	Es ist eine interne Organisation zur Einhaltung von Vorgaben vorhanden.

Anlage 2 – Genehmigte UNTERAUFTRAGNEHMER

1. Zulässigkeit der Unterbeauftragung

Die Auslagerung auf UNTERAUFTRAGNEHMER oder der Wechsel des bestehenden UNTERAUFTRAGNEHMERS sind zulässig, soweit:

- der AUFTRAGNEHMER eine solche Auslagerung auf bzw. den Wechsel auf einen anderen UNTERAUFTRAGNEHMER dem AUFTRAGGEBER eine angemessene Zeit* vorab schriftlich oder in Textform anzeigt und
- der AUFTRAGGEBER nicht innerhalb von 3 Monaten nach dem Zugang der Information gegenüber dem AUFTRAGNEHMER schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

*Für die Erfüllung des zeitlich angemessenen Informationszugangs sowohl bei der Auslagerung auf einen neuen UNTERAUFTRAGNEHMER als auch bei einem UNTERAUFTRAGNEHMER-Wechsel genügt die regelmäßige (zu Beginn eines jeden Kalenderquartals) Aktualisierung der UNTERAUFTRAGNEHMER-Liste unter www.zeiss.de/med/meinedaten.

2. Vorab genehmigte UNTERAUFTRAGNEHMER

Carl Zeiss AG			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
Retourenlager managen Wareneingang durchführen	Siehe Anlage 1.1	Siehe Anlage 1.2	73447 Oberkochen
Carl Zeiss Meditec AG			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
2nd Level Support durchführen Produktion Support bei Linsenberechnungen Werksinstandsetzung abwickeln	Siehe Anlage 1.1	Siehe Anlage 1.2	10589 Berlin 07745 Jena 81379 München 73447 Oberkochen
Carl Zeiss Meditec SAS			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
Produktion	Siehe Anlage 1.1	Siehe Anlage 1.2	17053 La Rochelle
Carl Zeiss Meditec Production, LLC			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
Produktion	Siehe Anlage 1.1	Siehe Anlage 1.2	Ontario, CA 91761, USA
Carl Zeiss Meditec, Inc.			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
3rd Level Support durchführen Produktion Werksinstandsetzung abwickeln	Siehe Anlage 1.1	Siehe Anlage 1.2	Dublin, CA 94568, USA

Carl Zeiss (Suzhou) Co., Ltd			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
3rd Level Support durchführen Produktion Werksinstandsetzung abwickeln	Siehe Anlage 1.1	Siehe Anlage 1.2	Suzhou City 215021
Briel Spedition-Logistik GmbH & Co. KG			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
Logistikdienstleistungen	Siehe Anlage 1.1	Siehe Anlage 1.2	73492 Rainau
Optica Abrechnungszentrum Dr. Güldener GmbH			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
Abrechnung mit Krankenkassen	Siehe Anlage 1.1	Siehe Anlage 1.2	70178 Stuttgart
Siemens Healthcare GmbH			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
Remote Service Leistungen	Siehe Anlage 1.1	Siehe Anlage 1.2	91052 Erlangen
Simon Hegele Gesellschaft für Logistik und Service mbH			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
Logistikdienstleistungen	Siehe Anlage 1.1	Siehe Anlage 1.2	76689 Karlsdorf
TechProtect GmbH			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
Call Center Dienstleistungen	Siehe Anlage 1.1	Siehe Anlage 1.2	71088 Holzgerlingen
Top it-services AG			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
Applikationsdienstleistungen & Vorortinstandsetzungen	Siehe Anlage 1.1	Siehe Anlage 1.2	10117 Berlin
TSI - Fiedler GmbH			
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen	Ort der Verarbeitung
Logistikdienstleistungen	Siehe Anlage 1.1	Siehe Anlage 1.2	07745 Jena