Auftragsverarbeitungsbedingungen für Serviceleistungen

Stand: 30. April 2025, version 1.0

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Auftragsverarbeitungsbedingungen (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG sichergestellt werden.

b) Olympus Austria Gesellschaft m.b.H, Shuttleworthstraße 25, 1210 Wien, Österreich (nachfolgend „Auftragsverarbeiter“) und der Kunde („nachfolgend“ Verantwortlicher) haben diesen Klauseln durch die Beauftragung der Serviceleistung zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Beschreibung der Datenverarbeitung in Anhang I.

d) Die Anhänge I bis III sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2

Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 3

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang I aufgeführt.

Klausel 4

Pflichten der Parteien

4.1 Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

4.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang I genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

4.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang I angegebene Dauer verarbeitet.

4.4 Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

4.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische

Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

4.6 Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

4.7 Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in Anhang III aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens vier Wochen im Voraus ausdrücklich über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden

Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

4.8 Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 4.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679

beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 5

Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 5 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang II die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 6

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

6.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

6.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang II alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 7

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 4.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Anhang I

BESCHREIBUNG DER VERARBEITUNG

Verarbeitungsmaßnahme: Service, Support, Consulting, Administration, Fernwartung

- Die Verarbeitung der Daten beginnt mit Beginn des Serviceauftrags bzw. Servicevertrages.
- Die Datenverarbeitung endet mit Beendigung des Serviceauftrags bzw. Servicevertrages.

Kategorien betroffener Personen, Art/Zweck der Verarbeitung, Datenkategorien und Besondere Kategorien personenbezogener Daten richten Sie nach der Art der Serviceleistung, den Geräten, auf die sich die Serviceleistungen beziehen sowie nach den beim Kunden gespeicherten personenbezogenen Daten, auf die Olympus im Rahmen der Serviceleistung Zugriff hat.

Der Kontext und Zwecke der Datenverarbeitung und die Verpflichtungen der Vertragsparteien im Rahmen des Geschäftsverhältnisses ergeben sich aus dem Serviceauftrag bzw. Servicevertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter.

Kategorien betroffener Personen	**Art/Zweck der Verarbeitung**	**Datenkategorien**	**Besondere Kategorien personenbezogener Daten – falls zutreffend**
☒ Patienten ☒ Kontaktpersonen ☒ Mitarbeiter ☒ Kunden ☒ Lieferanten und deren Mitarbeiter	☒ IT-Support ☒ Betrieb und Instandhaltung von IT-Systemen und Infrastruktur, z. B, Analysesysteme ☒ Wartung und Fernwartung von medizinischen Geräten (z. B. Lichtsteuerung)	☒ Kontendaten ☒ Unternehmen ☒ Geburtsdatum ☒ Gerätefreigabe und -berechtigung ☒ Geräte-ID	☒ Gesundheitsdaten (z. B. Daten über Krankschreibungen/ krankheitsbedingte Abwesenheit, medizinische Informationen)

☒ Ehemalige Mitarbeiter	☒ Technischer Support einschließlich Aufschaltung auf die Systeme, sofern technisch möglich ☒ Consulting zur Produktnutzung ☒ System-Administration ☒ Reparatur/Tests/Wartung vor Ort oder in einem Olympus Reparaturzentrum ☒ Hardware-Ferndiagnose für Hardware-Produkt(e) ☒ Software-Ferntests/Wartung für Softwareprodukte ☒ Bereitstellung von Leihgeräten	☒ Geräte-Zugangsdaten ☒ Gerätename ☒ E-Mail-Adresse ☒ Geschlecht ☒ ID (Analytics, Vertrag, Gerät) ☒ Sprache ☒ Standort ☒ Logs ☒ Name ☒ Benutzername ☒ Nutzungsdaten (IP-Adresse, Protokollierung, Telefonverbindungen) ☒ Geräte-Nutzungsdaten ☒ System-Nutzungsdaten ☒ Mitarbeiterdaten (Name, E-Mail)	

		☒ Patientendaten/Benutzer-stammdaten (Patienten-ID, anderen von den Olympus-Geräten verarbeitete Daten) ☒ Bild- und Videodaten (falls auf den Olympus-Geräten gespeichert)	

Die Arbeiten an dem Gerät können es erforderlich machen, das Logfile des Gerätes zu kopieren und zu analysieren. Das Logfile kann dabei auch den Namen des Patienten enthalten. Der First- und Second-Level-Support wird innerhalb der EU erbracht. Der Third-Level-Support wird durch ein amerikanisches OLYMPUS Unternehmen („Olympus Surgical Technologies America“) erbracht. Sollte also für die Problemlösung der Third-Level-Support erforderlich sein, müssen die Daten möglicherweise in die USA übertragen werden. Um ein angemessenen Schutzniveau zu gewährleisten, hat OLYMPUS mit seinen amerikanischen, verbundenen Unternehmen entsprechend interne AVVs abgeschlossen. Weiter erfolgt ein Zugriff auf die verschlüsselten Daten ausschließlich durch autorisierte Olympus Mitarbeiter. Für die Logfiles ist ein strikten Löschkonzept festgelegt, das regelmäßig geprüft wird.

Anhang II

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen, trifft der Verantwortliche folgende technische und organisatorische Maßnahmen:

MASSNAHME	**BESCHREIBUNG**
1. Vertraulichkeit	
a) Zutrittskontrolle	Die Gebäude von Olympus sind rundherum verschlossen und bewacht. Mitarbeiter können die Gebäude nur mit Hilfe der persönlichen Identifikationskarte betreten. Besucher können nur über den Empfang und in Begleitung von Mitarbeitern in die Gebäude gelangen. Unbefugten ist der Zutritt zu den Gebäuden verwehrt. Folgende Sicherheitsmaßnahmen sind implementiert: - Mitarbeiter- / Besucherausweise - Zutrittskontrollsystem, Ausweisleser, Transponder, Magnet- oder Chipkarten - Empfang / Rezeption / Pförtner

	- (Kontrollierte) Schlüssel / Schlüsselvergabe - Türsicherung (elektrische Türöffner, Türen mit Knauf Außenseite usw.) - Werkschutz, Pförtner - Überwachungseinrichtung Alarmanlage, Video- / Fernsehmonitor
b) Zugangskontrolle	Alle Systeme sind in besonders gesicherten Rechenzentren installiert und durch persönliche ID-Karten in Kombination mit PIN geschützt. Folgende Sicherheitsmaßnahmen sind implementiert: - Sicheres Kennwortverfahren (u. a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts) - Automatische Sperrmechanismen (z. B. Kennwort oder Pausenschaltung, automatische Desktopsperre) - Anleitung manuelle Desktopsperre - Einrichtung und Verwaltung eines Benutzerprofils und –stammsatzes - Firewall, Anti-Virus-Software für Server und Clients - Einsatz von VPN bei Remote-Zugriffen - Mobile Device Policy

c) Zugriffskontrolle; Lese,- Bearbeitungsbefugnis, Rechteverwaltung	Es gibt eine systematische Rechteverwaltung für die Nutzung der IT-Systeme. Zugriff auf Systeme ist nur mit Nutzernamen und Passwörtern möglich. Es werden die Befugnisse nach Lese- und Schreibrechten unterschieden. Folgende Sicherheitsmaßnahmen sind implementiert: - Differenziertes Berechtigungskonzept und bedarfsgerechte Zugriffsrechte (Profile, Rollen, Transaktionen und Objekte)
d) Trennungskontrolle	Fernwartungen werden für jeden Kunden separat durchgeführt. Folgende Sicherheitsmaßnahmen sind implementiert: - Mandantenfähigkeit relevanter Anwendungen - Zweckbindung - Funktionstrennung von Produktiv- und Testumgebung - Physikalische Trennung von Systemen, Datenbanken und Datenträgern - Festlegung von Datenbankrechten
e) Verschlüsselung	Eine Verschlüsselung der Kommunikation wird bevorzugt. Das Verschlüsselungsverfahren entspricht dem Stand der Technik.
2. Integrität	
a) Weitergabekontrolle	Folgende Sicherheitsmaßnahmen sind implementiert: - E-Mail-Verschlüsselung im Netzwerk möglich - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

	- Einsatz von VPN, sowie Bereitstellung über verschlüsselte Verbindungen wie sftp, https
b) Eingabekontrolle	Änderungen in den Systemen werden protokolliert. Folgende Sicherheitsmaßnahmen sind implementiert: - Protokollierung von Zugriffen - Protokollauswertungssysteme und Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen - Vergabe von Rechten über personalisierte Benutzerkonten - Dokumentenmanagement
3. Verfügbarkeit und Belastbarkeit	
a) Verfügbarkeitskontrolle; Datensicherungsmaßnahmen	Personenbezogene Daten werden gesichert. Der Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust wird ebenso Sorge getragen, wie der Kontrolle der Verfügbarkeit der Daten. Folgende Sicherheitsmaßnahmen sind implementiert: - Backup-Verfahren: Beschreibung von Rhythmus und Medium der Datensicherung, dazu Aufbewahrungszeit und Aufbewahrungsort für Backup (online/offline; on-site/off-site) - Spiegeln von Festplatten, z. B. RAID-Verfahren - Unterbrechungsfreie Stromversorgung (USV) - Getrennte Aufbewahrung bzw. Partition für Betriebssysteme und Daten - Virenschutz und Firewall

	- Meldewege und Notfallpläne - Feuerlöscher und –meldeanlagen in Gebäuden, insbesondere im Serverraum, wo dazu auch Temperatur/Feuchtigkeit überwacht und Schutzsteckdosenleisten installiert sind
b) Rasche Wiederherstellbarkeit	Die Wiederherstellbarkeit seiner Daten obliegt dem Verantwortlichen.
4. Verfahren zur regelmäSSigen Überprüfung, Bewertung und Evaluierung	
a) Auftragskontrolle	Die Wirksamkeit der getroffenen Maßnahmen wird regelmäßig überprüft. Die vollständige Erledigung der Aufträge wird stichprobenartig kontrolliert. Folgende Sicherheitsmaßnahmen sind implementiert: - Eindeutige Vertragsgestaltung - Formalisierte Auftragserteilung - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (in Bezug auf Datenschutz und -sicherheit) - Abschluss der notwendigen Vereinbarung zur Auftragsvereinbarung bzw. EU Standard-Vertragsklauseln - Schriftliche Weisungen oder in Textform an den Auftragnehmer - Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis - Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen der Bestellpflicht

	- Vereinbarung wirksamer Kontrollrechte gegenüber der Auftragnehmer - Regelung zum Einsatz weiterer Subunternehmer - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrages - Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
b) Datenschutz- und Incident-Response-Management	- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/ Berechtigung - Interner Informationssicherheits- und Datenschutzbeauftragter - Regelmäßige Schulung der Mitarbeiter und Verpflichtung auf Vertraulichkeit/ Datengeheimnis - Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörden) - Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen und Datenpannen - Formalisierte Datenschutzfolgenabschätzung und Prozess zur Bearbeitung von Auskunftsfragen seitens Betroffener vorhanden

Anhang III

LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Name und Anschrift	**Name, Funktion und Kontaktdaten der Kontaktperson**	**Beschreibung der Verarbeitung**	**Ggf. Angaben zur Absicherung eines Drittstaatentransfer**
Olympus Europa SE & Co. KG Wendenstraße 20 20097 Hamburg Deutschland	Stefan Limbacher Datenschutzbeauftragter EMEA privacy@olympus.com	2nd Level Support für Reparatur, Wartung und Fernwartung von Software und medizintechnischen Geräten	n/a (Standort Deutschland)
Olympus Surgical Technologies Europe Olympus Winter & Ibe GmbH Kuehnstraße 61 22045 Hamburg Deutschland	privacy@olympus.com	3rd Level Support für Reparatur, Wartung und Fernwartung von Software und medizintechnischen Geräten ---------- Schnittstelle zwischen First- und Third-Level-Support für Logistik und Hardwareabwicklung	n/a (Standort Deutschland)

Olympus Medical Systems Corporation 2951 Ishikawa-machi, Hachioji-shi, Tokyo 192-8507 Japan	privacy@olympus.com	Beschwerdemanagement und Untersuchung von Fehlfunktionen --- Second-Level-Support bei Reparatur, Wartung und Fernwartung von Software und medizinischen Geräten	Angemessenheitsbeschluss (EU) 2019/419 der EU-Kommission
Olympus Surgical Technologies America 800 W Park Dr. Westborough, MA 01581 USA	privacy@olympus.com	Beschwerdemanagement und Untersuchung von Fehlfunktionen	Standardvertragsklauseln
Olympus Deutschland GmbH Wendenstraße 20 20097 Hamburg Deutschland	privacy@olympus.com	1st Level Support für Reparatur, Wartung und Fernwartung von Software und medizintechnischen Geräten	n/a (Standort Deutschland)
Olympus Schweiz AG Richtiring 30 8304 Wallisellen Schweiz	privacy@olympus.com	1st Level Support für Reparatur, Wartung und Fernwartung von Software und medizintechnischen Geräten	Angemessenheitsbeschluss (EG) 2000/518/EG der Kommission

Rein Medical GmbH Monforts Quartier 23 Schwalmstraße 301 41238 Mönchengladbach Deutschland	privacy@olympus.com	3rd Level Support für Reparatur, Wartung und Fernwartung von Software	n/a (Standort Deutschland)
MESO international GmbH Markt 21-23 09648 Mittweida Deutschland	privacy@olympus.com	3rd Level Support für Reparatur, Wartung und Fernwartung von Software	n/a (Standort Deutschland)
Tata Consultancy Services GmbH Friedrich-Ebert-Anlage 49 60308 Frankfurt am Main Deutschland	privacy@olympus.com	IT – Infrastruktur und Service Provider	n/a (Standort Deutschland)
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen Deutschland	privacy@teamviewer.com	Fernwartung	n/a (Standort Deutschland)

ImageStreamMedical One Monarch Drive Littleton, MA 01460 USA	privacy@cision.com	3rd Level Support für Reparatur, Wartung und Fernwartung von Software	Standardvertragsklauseln
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521 Irland	privacy@microsoft.com	Cloud-Dienste	n/a (Standort Irland/EU)
RealVNC Limited 50-60 Station Road Cambridge Cambridgeshire CB1 2JH Vereinigtes Königreich von Großbritannien und Nordirland	privacy@realvnc.com	Anbieter von Fernsteuerungssoftware für SPiN Planning Laptop Workstation - Keine Datenspeicherung, sondern lediglich eine verschlüsselte Bildschirmfreigabe	Angemessenheitsbeschluss für das Vereinigte Königreich