Auftragsverarbeitungsvertrag

Dieser Auftragsverarbeitungsvertrag („AVV“) ist ein wesentlicher Bestandteil des Dienstleistungsvertrages, Kaufvertrages, der Auftragsbestätigung oder eines ähnlichen Vertrages („Vertrag“), der zwischen dem Kunden (wie im Vertrag definiert oder angegeben) und dem KARL STORZ-Unternehmen (wie im Vertrag definiert oder angegeben) geschlossen wird. Durch Einverständnis mit dem Vertrag oder durch Annahme des Vertrages schließen der Kunde und das KARL STORZ-Unternehmen ebenfalls diesen AVV. Im Sinne dieses AVV ist der Kunde als „Verantwortlicher“ und KARL STORZ als „Auftragsverarbeiter“ definiert (gemeinsam „Parteien“).

PRÄAMBEL

Der Auftragsverarbeiter bietet Dienstleistungen für Medizinprodukte, wie Kundendienst, Reparatur und Austausch an.

Im Rahmen des zwischen dem Auftragsverarbeiter und dem Verantwortlichen geschlossenen Vertrages kann der Auftragsverarbeiter dem Verantwortlichen die im Vertrag und/oder in Anhang 1 zu diesem AVV näher beschriebenen Dienstleistungen erbringen („Dienstleistungen“).

Im Zuge der Erbringung der Dienstleistungen könnte es gelegentlich vorkommen, dass dem Auftragsverarbeiter Informationen über die Patienten und Mitarbeiter des Verantwortlichen zur Verfügung gestellt werden oder er Zugang zu solchen Informationen hat, und diese Informationen könnten laut Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr („DSGVO**“**) und laut anderer geltender Datenschutzgesetze als personenbezogene Daten gelten.

Der Verantwortliche beschäftigt den Auftragsverarbeiter als einen im Auftrag des Verantwortlichen handelnden Auftragsverarbeiter laut Art. 28 DSGVO.

Dieser AVV enthält die Bedingungen, die für die Erhebung, Verarbeitung und Nutzung solcher personenbezogenen Daten durch den Auftragsverarbeiter als beauftragter Datenverarbeiter des Verantwortlichen gelten, und die gewährleisten sollen, dass die Parteien den geltenden Datenschutzgesetzen entsprechen.

IN ANBETRACHT DESSEN und damit die Parteien ihre Beziehung auf rechtmäßige Weise ausführen können, haben die Parteien diesen AVV wie folgt geschlossen:

1. Terminologie

Für die Zwecke dieses AVV gelten die in der DSGVO verwendeten Begriffsdefinitionen und Terminologie. Darüber hinaus gilt Folgendes:

„Mitgliedstaat"	ist ein zur Europäischen Union oder zum Europäischen Wirtschaftsraum gehörendes Land;
„Unterauftragsverarbeiter"	bezeichnet jeden weiteren Auftragsverarbeiter, der vom Auftragsverarbeiter als Unterauftragnehmer für die Erbringung aller oder einiger der Dienstleistungen im Auftrag des Verantwortlichen beschäftigt wird, sofern dieser Unterauftragsverarbeiter im Zuge der Erbringung der untervergebenen Dienstleistungen Zugang zu den personenbezogenen Daten des Verantwortlichen hat.

2. Einzelheiten der Verarbeitung

Die Einzelheiten der Verarbeitungstätigkeiten, die der Auftragsverarbeiter als beauftragter Datenverarbeiter für den Verantwortlichen ausführt (z. B. den Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien betroffener Personen), sind in Anhang 1 zu diesem AVV aufgeführt.

3. Verpflichtungen des Verantwortlichen

a) Der Verantwortliche muss die Einhaltung aller geltenden Verpflichtungen laut DSGVO und laut sonstigen für den Verantwortlichen geltenden Datenschutzgesetzen gewährleisten und muss diese Einhaltung wie von Art. 5 (2) DSGVO gefordert nachweisen können.

b) Der Verantwortliche muss dem Auftragsverarbeiter gemäß Art. 30 (1) DSGVO die jeweiligen Verzeichnisse von Verarbeitungstätigkeiten für die im Rahmen dieses AVV erbrachten Dienstleistungen bereitstellen, insoweit dies für den Auftragsverarbeiter zur Erfüllung der Verpflichtung nach Art. 30 (2) DSGVO erforderlich ist.

c) Soweit dies vom geltenden Datenschutzgesetz gefordert wird, benennt der Verantwortliche einen Datenschutzbeauftragten und/oder Vertreter. Der Verantwortliche muss gegebenenfalls Kontaktangaben des Datenschutzbeauftragten bzw. Vertreters an den Auftragsverarbeiter weiterleiten.

d) Vor Beginn der Verarbeitung bestätigt der Verantwortliche durch Annahme dieses AVV, dass die in Anhang 2 aufgeführten, technischen und organisatorischen Maßnahmen des Auftragsverarbeiters geeignet und ausreichend sind, um die Rechte der betroffenen Person zu schützen, und bestätigt, dass der Auftragsverarbeiter diesbezüglich hinreichende Garantien bietet.

4. Weisungen

a) Der Verantwortliche weist den Auftragsverarbeiter an, die personenbezogenen Daten ausschließlich für den Verantwortlichen zu verarbeiten. Die Weisungen des Verantwortlichen sind in diesem AVV aufgeführt. Der Verantwortliche muss sicherstellen, dass alle dem Auftragsverarbeiter erteilten Weisungen dem geltenden Datenschutzgesetz entsprechen. Der Auftragsverarbeiter hat sich bei der Verarbeitung der personenbezogenen Daten ausschließlich an die Weisungen des

Verantwortlichen zu halten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten anderweitig verpflichtet ist (im letzteren Fall gilt Abs. 5. (d) (iii)).

b) Alle weiteren Weisungen, die über die in diesem AVV enthaltenen Weisungen hinausgehen, müssen im Rahmen des Gegenstands dieses AVV und des Vertrages liegen. Bringt die Ausführung einer weiteren Weisung Kosten für den Auftragsverarbeiter mit sich, hat dieser den Verantwortlichen vor Ausführung der Weisung diesbezüglich zu informieren und diese Kosten zu erläutern. Erst nachdem der Verantwortliche bestätigt hat, dass er die betreffenden Kosten für die Ausführung der Weisung übernimmt, ist der Auftragsverarbeiter verpflichtet, die weitere Weisung umzusetzen. Der Verantwortliche erteilt weitere Weisungen im Allgemeinen in Schriftform, es sei denn, die Dringlichkeit oder sonstige spezifische Umstände erfordern eine andere (z. B. mündliche oder elektronische) Form. In anderer als in schriftlicher Form erteilte Weisungen sind vom Verantwortlichen unverzüglich schriftlich zu bestätigen.

c) Sofern der Verantwortliche die Berichtigung, Löschung und/oder Einschränkung von personenbezogenen Daten nicht selber ausführen kann, können sich Weisungen auch wie in Abs. 6 beschrieben auf die Berichtigung, Löschung und/oder Einschränkung von personenbezogenen Daten beziehen.

d) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu benachrichtigen, wenn eine Weisung seiner Meinung nach gegen die DSGVO oder andere Datenschutzbestimmungen der Europäischen Union oder eines Mitgliedstaates verstößt („angefochtene Weisung“). Ist der Auftragsverarbeiter der Meinung, eine Weisung verstoße gegen die DSGVO oder andere Datenschutzbestimmungen der Europäischen Union oder eines Mitgliedstaates, ist er nicht verpflichtet, der angefochtenen Weisung nachzukommen. Wenn der Verantwortliche die angefochtene Weisung bei Benachrichtigung durch den Auftragsverarbeiter bestätigt und seine Haftung für die angefochtene Weisung anerkennt, hat der Auftragsverarbeiter die angefochtene Weisung auszuführen, sofern diese sich nicht auf (i) die Umsetzung von organisatorischen und technischen Maßnahmen, (ii) die Rechte der betroffenen Personen, oder (iii) die Beschäftigung von Unterauftragsverarbeitern bezieht. Im Falle von (i) bis (iii) kann der Auftragsverarbeiter sich zwecks einer rechtlichen Bewertung der angefochtenen Weisung an eine zuständige Aufsichtsbehörde wenden. Erklärt die Aufsichtsbehörde die angefochtene Weisung für rechtmäßig, hat der Auftragsverarbeiter dieser Weisung nachzukommen. Abs. 4 (b) gilt weiterhin.

5. Verpflichtungen des Auftragsverarbeiters

a) Der Auftragsverarbeiter muss sicherstellen, dass die Personen, die von ihm zur Verarbeitung der personenbezogenen Daten für den Verantwortlichen befugt wurden, insbesondere die Mitarbeiter der Auftragsverarbeiter sowie Mitarbeiter etwaiger Unterauftragnehmer, sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, und dass alle Personen, die Zugang zu den personenbezogenen Daten haben, diese Daten gemäß den Weisungen der Verantwortlichen verarbeiten.

b) Vor der Verarbeitung der personenbezogenen Daten im Auftrag des Verantwortlichen muss der Auftragsverarbeiter die in Anhang 2 aufgeführten technischen und organisatorischen Maßnahmen ergreifen. Der Auftragsverarbeiter kann die technischen und organisatorischen Maßnahmen gelegentlich ändern, sofern die geänderten technischen und organisatorischen Maßnahmen kein geringeres Schutzniveau bieten als die in Anhang 2 aufgeführten Maßnahmen.

c) Der Auftragsverarbeiter muss dem Verantwortlichen auf Aufforderung des Verantwortlichen Informationen zur Verfügung stellen, aus denen die Einhaltung der in Art. 28 DSGVO festgelegten Verpflichtungen des Auftragsverarbeiters hervorgeht. Auf Aufforderung des Verantwortlichen liefert der Auftragsverarbeiter einen jährlichen Auditbericht auf Grundlage von ISO 27001 oder ISAE3402 oder SSAE16-SOC 1 Typ 2 oder ISAE3000 oder SSAE16-SOC 2 Typ 2 oder ähnlich, oder von einem Dritten erstellte, ähnliche Auditberichte („Auditbericht"). Falls weitere Audittätigkeiten gesetzlich vorgeschrieben sind, kann der Verantwortliche Prüfungen fordern, die von ihm selbst oder einem anderen, von ihm beauftragten Prüfer durchgeführt werden („Vor-Ort-Audit"). Ein derartiges Vor-Ort-Audit unterliegt folgenden Bedingungen: (i) Vor-Ort-Audits beschränken sich auf diejenigen Verarbeitungsanlagen und Mitarbeiter des Auftragsverarbeiters, die mit den von diesem AVV betroffenen Verarbeitungstätigkeiten zu tun haben; und (ii) Vor-Ort-Audits erfolgen höchstens einmal jährlich bzw. so häufig, wie von geltenden Datenschutzgesetzen oder einer zuständigen Aufsichtsbehörde vorgeschrieben, oder unmittelbar nach einer wesentlichen Verletzung des Schutzes personenbezogener Daten in Zusammenhang mit den vom Auftragsverarbeiter im Rahmen dieses AVV verarbeiteten personenbezogenen Daten; und (iii) Vor-Ort-Audits können während normaler Werkszeiten mit nur unwesentlicher Störung der Geschäftstätigkeiten des Auftragsverarbeiters gemäß dessen Sicherheitsrichtlinien und nach angemessener vorheriger Benachrichtigung durchgeführt werden; und (iv) der Verantwortliche übernimmt alle Kosten in Zusammenhang mit dem Vor-Ort-Audit beim Verantwortlichen und Auftragsverarbeiter. Der Verantwortliche muss einen Auditbericht mit einer Zusammenfassung der Ergebnisse und Beobachtungen des Vor-Ort-Audits erstellen („Vor-Ort-Auditbericht"). Vor-Ort-Auditberichte sowie Auditberichte sind vertrauliche Informationen des Auftragsverarbeiters und dürfen nur dann an Dritte offengelegt werden, wenn dies durch geltende Datenschutzgesetze vorgeschrieben ist, oder wenn der Auftragsverarbeiter seine diesbezügliche Genehmigung erteilt hat.

d) Der Auftragsverarbeiter muss den Verantwortlichen unverzüglich über Folgendes benachrichtigen:
   (I) über eine rechtsverbindliche Aufforderung zur Offenlegung der personenbezogenen Daten durch eine Strafverfolgungsbehörde, sofern eine solche Benachrichtigung nicht verboten ist, zum Beispiel im Rahmen eines strafrechtlichen Verbots zur Wahrung der Vertraulichkeit eines strafrechtlichen Ermittlungsverfahrens;
   (II) über direkt von einer betroffenen Person eingehende Beschwerden und Anfragen (z. B. in Sachen Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch gegen die Verarbeitung, automatisierte Entscheidungsfällung), ohne die betreffende Anfrage zu beantworten, es sei denn, der Auftragsverarbeiter wurde anderweitig hierzu befugt;
   (III) wenn der Auftragsverarbeiter oder Unterauftragsverarbeiter durch das für den Auftragsverarbeiter oder Unterauftragsverarbeiter geltende Recht der Union oder eines Mitgliedstaats verpflichtet ist, die personenbezogenen Daten auf eine über die Weisungen des Verantwortlichen hinausgehende Weise zu verarbeiten, muss er den Verantwortlichen vor Durchführung dieser über die Weisung hinausgehenden Verarbeitung benachrichtigen, es sei denn, das Recht der Union oder des Mitgliedstaats verbietet eine solche Benachrichtigung aus Gründen des öffentlichen Interesses, wobei in diesem Fall die Mitteilung an den Verantwortlichen die betreffende rechtliche Auflage nach Recht der Union oder eines Mitgliedstaats anzuführen hat; und/oder

(IV) über eine die personenbezogenen, Gegenstand dieses AVV bildenden, Daten des Verantwortlichen betreffende Verletzung des Schutzes personenbezogener Daten beim Auftragsverarbeiter oder dessen Unterauftragnehmern, von der der Auftragsverarbeiter Kenntnis erlangt; in diesem Falle unterstützt er den Verantwortlichen bei der Erfüllung der im Rahmen geltender Datenschutzgesetze für den Verantwortlichen geltenden Pflicht, die betroffenen Personen bzw. die Aufsichtsbehörden unter Angabe aller dem Auftragsverarbeiter zur Verfügung stehenden Informationen gemäß Art. 33 (3) DSGVO zu benachrichtigen.

e) Der Auftragsverarbeiter muss den Verantwortlichen bei der Erfüllung dessen Pflicht unterstützen, eine gegebenenfalls laut Art. 35 DSGVO vorgeschriebene Datenschutz-Folgenabschätzung und eine gegebenenfalls laut Art. 36 DSGVO vorgeschriebene vorherige Konsultation durchzuführen, die sich auf die vom Auftragsverarbeiter im Rahmen dieses AVV für den Verantwortlichen erbrachten Dienstleistungen bezieht, indem er dem Verantwortlichen alle notwendigen und verfügbaren Informationen zur Verfügung stellt. Der Auftragsverarbeiter ist nur insofern verpflichtet, solche Unterstützung zu leisten, wie diese Pflicht des Verantwortlichen nicht auf andere Weise vom Verantwortlichen erfüllt werden kann. Der Auftragsverarbeiter informiert den Verantwortlichen über die Kosten dieser Unterstützungsleistungen. Nachdem der Verantwortliche die Übernahme dieser Kosten bestätigt hat, erbringt der Auftragsverarbeiter die betreffenden Unterstützungsleistungen.

f) Der Verantwortliche entscheidet hiermit und weist den Auftragsverarbeiter an, alle im Rahmen dieses AVV vom Auftragsverarbeiter für den Verantwortlichen verarbeiteten personenbezogenen Daten und alle etwaig vorhandenen Kopien nach Ende der Erbringung der Dienstleistungen sicher zu löschen, sofern der Auftragsverarbeiter nicht durch das Recht der Union oder der Mitgliedstaaten zur Aufbewahrung dieser personenbezogenen Daten verpflichtet ist. Personenbezogene Daten werden nur auf ausdrückliche Vereinbarung der Parteien an den Verantwortlichen zurückgegeben.

6. Rechte der betroffenen Personen

a) Der Verantwortliche ist primär für die Abwicklung und Beantwortung von Anfragen von betroffenen Personen verantwortlich.

b) Der Auftragsverarbeiter muss den Verantwortlichen mit den folgenden angemessenen und möglichen technischen und organisatorischen Maßnahmen unterstützen, um auf Anfragen zur Ausübung der in Kapitel 3 der DSGVO niedergelegten Rechte der betroffenen Personen einzugehen:

(I) Hinsichtlich von Anträgen in Zusammenhang mit der Informationspflicht hat der Auftragsverarbeiter dem Verantwortlichen die laut Art. 13 und 14 DSGVO vorgeschriebenen und beim Auftragsverarbeiter verfügbaren Informationen nur dann bereitzustellen, wenn der Verantwortliche diese Informationen nicht selber abrufen kann.

(II) Hinsichtlich von Anträgen auf die Erteilung einer Auskunft über personenbezogene Daten (Art. 15 DSGVO) hat der Auftragsverarbeiter dem Verantwortlichen diejenigen Informationen bereitzustellen, die einer betroffenen Person in Zusammenhang mit einem solchen Antrag erstellt werden müssen und die beim Auftragsverarbeiter verfügbar sind; dies gilt jedoch nur dann, wenn der Verantwortliche diese Informationen nicht selber abrufen kann.

(III) Hinsichtlich von Berichtigungsanträgen, (Art. 16 DSGVO), Löschungsanträgen (Art. 17 DSGVO), Anträgen auf Einschränkung der Verarbeitung (Art. 18 DSGVO) und Datenübertragbarkeitsanträgen (Art. 20 DSGVO) hat der Auftragsverarbeiter dem Verantwortlichen nur dann, wenn dieser die personenbezogenen Daten nicht selber berichtigen bzw. löschen, einschränken oder an einen Dritten übertragen kann, entweder die Fähigkeit zu verleihen, die betroffenen personenbezogenen Daten zu berichtigen bzw. zu löschen, einzuschränken oder an einen anderen Dritten zu übertragen, oder, wenn diese Fähigkeit nicht verliehen werden kann, hat der Auftragsverarbeiter die erforderliche Unterstützung bereitzustellen, um die betroffenen personenbezogenen Daten zu berichtigen bzw. zu löschen, einzuschränken oder an einen anderen Dritten zu übertragen.

(IV) Hinsichtlich einer Mitteilung in Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Art. 19 DSGVO) hat der Auftragsverarbeiter, wenn er vom Verantwortlichen hierzu aufgefordert wird, an der Benachrichtigung von Empfängern der personenbezogenen Daten mitzuwirken, die von ihm als Unterauftragsverarbeiter beschäftigt werden. Der Verantwortliche benachrichtigt in jedem Fall alle sonstigen Empfänger.

(V) Hinsichtlich eines von einer betroffenen Person ausgeübten Widerspruchsrechts (Art. 21 und 22 DSGVO) bestimmt der Verantwortliche, ob der Widerspruch legitim ist und wie auf ihn eingegangen werden soll. Falls der Verantwortliche die Unterstützung des Auftragsverarbeiters benötigt, um auf den Widerspruch einzugehen, erteilt der Verantwortliche eine weitere Weisung gemäß Abs. 4 (b).

c) Der Verantwortliche muss feststellen, ob eine betroffene Person das Recht hat, die in diesem Abs. 6 aufgeführten Rechte betroffener Personen auszuüben oder nicht, und muss den Auftragsverarbeiter anweisen, in welchem Umfang die in Abs. 6 (b) beschriebene Unterstützung erforderlich ist.

d) Falls der Verantwortliche zum Eingehen auf Anfragen in Zusammenhang mit Rechten betroffener Personen zusätzliche oder abgeänderte technische und organisatorische Maßnahmen benötigt, die über die vom Auftragsverarbeiter gemäß Abs. 6 (b) gewährte Unterstützung hinausgehen, informiert der Auftragsverarbeiter den Verantwortlichen über die mit der Ausführung solcher zusätzlichen oder abgeänderten technischen und organisatorischen Maßnahmen verbundenen Kosten. Nachdem der Verantwortliche die Übernahme dieser Kosten bestätigt hat, führt der Auftragsverarbeiter diese zusätzlichen oder abgeänderten technischen und organisatorischen Maßnahmen aus, um den Verantwortlichen beim Eingehen auf die Anfragen betroffener Personen zu unterstützen.

e) Ohne Einschränkung von Abs. 6 (d) ist der Verantwortliche verpflichtet, dem Auftragsverarbeiter angemessene Auslagen zurückzuerstatten, die diesem in Zusammenhang mit Anfragen betroffener Personen entstanden sind.

7. Unterauftragsverhältnisse

a) Der Verantwortliche genehmigt die Inanspruchnahme von Unterauftragsverarbeitern, die vom Auftragsverarbeiter zur Erbringung der Dienstleistungen im Rahmen dieses AVV beschäftigt werden. Der Auftragsverarbeiter muss Unterauftragsverarbeiter sorgfältig auswählen. Der Auftragsverarbeiter haftet für die Handlungen oder Unterlassungen seiner Unterauftragsverarbeiter auf dieselbe Weise wie für seine

eigenen Handlungen oder Unterlassungen im Rahmen dieses Vertrages. Der Verantwortliche genehmigt die Unterauftragsverarbeiter wie in Anhang 1 beschrieben.

b) Der Auftragsverarbeiter hat seine Verpflichtungen als Auftragsverarbeiter im Rahmen dieses AVV in dem für die untervergebenen Dienstleistungen geltenden Maße an die Unterauftragsverarbeiter weiterzuleiten.

c) Gemäß dem vorliegenden Abschnitt 7 (c) kann der Auftragsverarbeiter nach eigenem Ermessen Unterauftragsverarbeiter entfernen, austauschen oder weitere geeignete und zuverlässige Unterauftragsverarbeiter ernennen:
   (I) Der Auftragsverarbeiter informiert den Verantwortlichen im Voraus über Änderungen der in Abschnitt 7 (a) aufgeführten Liste der Unterauftragsverarbeiter. Wenn der Verantwortliche nicht binnen dreißig Tagen nach Eingang der Mitteilung des Auftragsverarbeiters Einspruch gemäß Abschnitt 7(c) (ii) erhebt, gilt der weitere bzw. gelten die weiteren Unterauftragsverarbeiter als angenommen.
   (II) Wenn der Verantwortliche einen legitimen Grund hat, Einspruch gegen einen weiteren Unterauftragsverarbeiter zu erheben, teilt er dem Auftragsverarbeiter dies binnen dreißig Tagen nach Eingang der diesbezüglichen Mitteilung des Auftragsverarbeiters mit. Wenn der Verantwortliche Einspruch gegen die Inanspruchnahme des weiteren Unterauftragsverarbeiters erhebt, hat der Auftragsverarbeiter das Recht, dem Einspruch durch eine der folgenden Optionen abzuhelfen (wobei die Auswahl der Option dem alleinigen Ermessen des Auftragsverarbeiters unterliegt): (a) Der Auftragsverarbeiter sieht davon ab, den weiteren Unterauftragsverarbeiter für die personenbezogenen Daten der Verantwortlichen in Anspruch zu nehmen; oder (b) der Auftragsverarbeiter ergreift die vom Verantwortlichen im Zuge seines Einspruchs geforderten Abhilfemaßnahmen (zur Aufhebung des Einspruchs der Verantwortlichen), woraufhin er den weiteren Unterauftragsverarbeiter für die personenbezogenen Daten der Verantwortlichen in Anspruch nimmt; oder (c) der Auftragsverarbeiter kann die Erbringung desjenigen Aspektes der Dienstleistungen, der die Inanspruchnahme eines solchen weiteren Unterauftragsverarbeiters für die personenbezogenen Daten des Verantwortlichen mit sich bringen würde, einstellen, oder die Verantwortlichen können sich bereit erklären, diesen Aspekt (vorübergehend oder dauerhaft) nicht in Anspruch zu nehmen. Wenn keine der obigen Optionen zur Verfügung steht und dem Einspruch nicht binnen dreißig Tagen nach Eingang des Einspruchs der Verantwortlichen beim Auftragsverarbeiter abgeholfen wurde, kann jede der Parteien die betroffene Dienstleistung nach angemessener Kündigungsfrist beenden.

d) Befindet sich der Sitz eines Unterauftragsverarbeiters in einem Land außerhalb der EU/des EWR, das kein angemessenes Datenschutzniveau bietet, hat der Auftragsverarbeiter Maßnahmen zu ergreifen, um die Notwendigkeit eines der Sache nach gleichwertiges Datenschutzniveaus beim Unterauftragsverarbeiter zu adressieren (diese Maßnahmen können insbesondere die Vereinbarung von auf EU-Standardvertragsklauseln basierenden Datenverarbeitungsverträgen sein).

8. Haftung und Haftungsbeschränkung

a) Jede Partei haftet für ihre in diesem AVV und in geltenden Datenschutzgesetzen aufgeführten Verpflichtungen.

b) Sofern der Vertrag oder dieser AVV keine anderen Vereinbarungen enthält, gilt Folgendes hinsichtlich von Haftungsansprüchen, die durch oder in Zusammenhang mit Verletzungen der Verpflichtungen dieses AVV oder geltender Datenschutzgesetze erwachsen:

(I) Die vertragliche und gesetzliche Haftung des Auftragsverarbeiters für leicht fahrlässig verursachte Schäden, gleich aus welchem Rechtsgrund, ist wie folgt beschränkt:

Der Auftragsverarbeiter haftet bis zur Höhe des vertragstypischen, voraussehbaren Schadens, der durch eine Verletzung wesentlicher vertraglicher Verpflichtungen entsteht;

Der Auftragsverarbeiter haftet weder für Verletzungen von nicht-wesentlichen vertraglichen Verpflichtungen noch für die leicht fahrlässige Verletzung einer sonstigen anwendbaren Sorgfaltspflicht.

(II) Die oben genannten Haftungsbeschränkungen gelten nicht für zwingende gesetzliche Haftung, insbesondere für Haftung nach dem deutschen Produkthaftungsgesetz und für Haftung für schuldhaft verursachte Personenschäden. Ferner gelten diese Haftungsbeschränkungen nicht, wenn und insofern der Auftragsverarbeiter eine entsprechende Garantie übernommen hat.

(III) Abs. 8 (b) (i) und (ii) gelten analog für die Haftung des Auftragsverarbeiters für Vertrauensschaden (ein Schaden, der dadurch entsteht, dass eine Geschäftspartei auf die Gültigkeit des Rechtsgeschäfts vertraut hat).

(IV) Der Verantwortliche ist verpflichtet, angemessene Maßnahmen zur Schadensabwehr und -minderung zu treffen.

9. Ersatzleistungen

Sofern der Vertrag oder dieser AVV keine anderen Vereinbarungen enthält, wird der Verantwortliche den Auftragsverarbeiter und dessen Führungskräfte, Direktoren, Angestellten, Rechtsnachfolger und Vertreter von allen Forderungen, Schadenersatz- oder Haftungsansprüchen, Veranlagungen, Verlusten, Kosten, Bußgeldern und sonstigen Auslagen (einschließlich unter anderem von angemessenen Anwalts- und Rechtskosten) freistellen und schadlos halten, die aus Forderungen, Behauptungen, Ansprüchen, Klagen, Prozessen, Verfügungen oder sonstigen Verfahren Dritter (einschließlich Aufsichtsbehörden) in Zusammenhang mit einer schuldhaften Verletzung der Verpflichtungen des Verantwortlichen im Rahmen dieses AVV und geltender Datenschutzgesetze erwachsen.

10. Laufzeit und Kündigung

(a) Ist im Vertrag eine Laufzeit des betreffenden Vertrages vorgegeben, gilt Folgendes: Die Laufzeit dieses AVV entspricht der Laufzeit des betreffenden Vertrages. Vorbehaltlich anderslautender Angaben im vorliegenden Vertrag gelten dieselben Kündigungsrechte und -bedingungen wie im betreffenden Vertrag, sofern zutreffend.

(b) Wird im Vertrag keine Laufzeit vorgegeben, gilt Folgendes: Der AVV gilt für einen unbefristeten Zeitraum. Jede Partei kann diesen AVV schriftlich unter Einhaltung einer dreimonatigen Frist zum Ende des Kalendermonats kündigen (E-Mail ist ausreichend).

11. Sonstiges

a) Bei Unstimmigkeiten zwischen den Bestimmungen dieses AVV und irgendwelchen anderen Vereinbarungen zwischen den Parteien sind die Bestimmungen dieses AVV für die Datenschutzpflichten der Parteien in Zusammenhang mit den Dienstleistungen maßgebend. Bestehen Zweifel, ob Klauseln in anderen Vereinbarungen sich auf Datenschutzpflichten der Parteien beziehen, ist dieser AVV maßgebend.

b) Ist eine Bestimmung dieses AVV ungültig oder nicht durchsetzbar, bleiben die restlichen Bestimmungen dieses AVV gültig und in Kraft. Die ungültige oder nicht durchsetzbare Bestimmung ist entweder (i) so abzuändern, dass ihre Gültigkeit und Durchsetzbarkeit unter möglichst genauer Wahrung der Absichten der Parteien gewährleistet wird, oder, falls dies nicht möglich ist, (ii) so auszulegen, als wäre der ungültige oder nicht durchsetzbare Teil nie in diesem Vertrag enthalten gewesen. Das Voranstehende gilt auch, wenn dieser AVV Auslassungen enthält.

c) Dieser AVV unterliegt demselben Gesetz wie der Vertrag, außer insofern zwingend vorgeschriebene Datenschutzgesetze Anwendung finden.

d) Der Gerichtsstand für alle Streitigkeiten in Zusammenhang mit diesem AVV ist der Hauptgeschäftssitz des Auftragsverarbeiters, außer insofern zwingend vorgeschriebene Datenschutzgesetze Anwendung finden.

e) Vor dem Inkrafttreten der DSGVO am 25. Mai 2018 ist jede Bezugnahme auf die DSGVO als Bezugnahme auf die entsprechende Bestimmung in der EU-Datenschutzrichtlinie und/oder in anderen anwendbaren Datenschutzgesetzen zu verstehen. Ab Inkrafttreten der DSGVO am 25. Mai 2018 beinhaltet jede Bezugnahme auf die DSGVO die Bezugnahme auf die entsprechende Bestimmung in anderen anwendbaren Datenschutzgesetzen, insbesondere in Datenschutzgesetzen der Mitgliedstaaten.

f) Die Parteien haben das Recht, um Änderungen dieses AVV anzusuchen, insofern dies notwendig ist, um Auslegungen, Weisungen oder Anordnungen nachzukommen, die von zuständigen EU- oder Mitgliedstaatsbehörden, durch nationale Ausführungsbestimmungen oder sonstige rechtliche Entwicklungen entstehen, die die Anforderungen der DSGVO zur Beauftragung von Datenverarbeitern betreffen.

g) Gegebenenfalls werden die Parteien Anhang 2 rechtzeitig vor dem Datum des Inkrafttretens der DSGVO abändern, um die Anforderungen der technischen und organisatorischen Sicherheitsmaßnahmen laut Art. 32 DSGVO zu erfüllen.

Anhang 1 zum AVV – Beschreibung der Datenverarbeitungsaktivitäten

1. Kategorien betroffener Personen

Die verarbeiteten personenbezogenen Daten beziehen sich auf die folgenden Kategorien betroffener Personen:

- Patienten des Verantwortlichen;
- Mitarbeiter des Verantwortlichen.

2. Gegenstand der Datenverarbeitung

Der Auftragsverarbeiter hat Zugriff auf die personenbezogenen Daten, die auf den Medizinprodukten oder in Zusammenhang mit den Medizinprodukten gespeichert sind, für die der Auftragsverarbeiter Reparatur- und Austauschdienste erbringen könnte.

3. Art und Zweck der Datenverarbeitung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten der betroffenen Personen für den Verantwortlichen in Zusammenhang mit der Ausführung von Reparatur- und Austauschdiensten.

- Reparaturdienste beim Auftragsverarbeiter:

  Die Medizinprodukte werden beim Auftragsverarbeiter geprüft und (wenn möglich) repariert. Je nach Reparaturtätigkeit könnte ein Zugriff auf die im Medizinprodukt gespeicherten personenbezogenen Daten möglich sein. Der Auftragsverarbeiter weist den Verantwortlichen ausdrücklich an, alle Daten auf dem Medizinprodukt zu löschen.

  Der Verantwortliche erstellt ein Back-up aller Daten und löscht anschließend alle Daten, bevor das Medizinprodukt an den Auftragsverarbeiter gesendet wird. Der Auftragsverarbeiter übernimmt keine Verantwortung für Datenverluste oder -schäden.

- Außendienstreparaturdienste / Fernservice:

  Bei technischen Problemen mit dem Vertragsprodukt besuchen Außendiensttechniker des Auftragsverarbeiters den Verantwortlichen oder stellen eine Fernverbindung zum Gerät her.

  Die Medizinprodukte werden beim Verantwortlichen geprüft und (wenn möglich) gewartet/repariert. Je nach Wartungs-/Reparaturtätigkeit könnte ein Zugriff auf die im Medizinprodukt gespeicherten personenbezogenen Daten möglich sein. Personenbezogene Daten werden normalerweise nicht vom Auftragsverarbeiter gelöscht, sofern keine anderslautende Weisung des Verantwortlichen vorliegt.

  Der Verantwortliche erstellt einen Back-up aller Daten und löscht anschließend alle Daten, bevor das Medizinprodukt vom Auftragsverarbeiter geprüft wird. Der Auftragsverarbeiter übernimmt keine Verantwortung für Datenverluste oder -schäden.

  Nur wenn vom Verantwortlichen im Zuge des Außendienstreparaturdienstes gefordert: Wenn während der Reparatur Speichermedien ausgetauscht werden, werden Daten auf ein neues Speichermedium des Medizinprodukts kopiert.

Der Auftragsverarbeiter kann als Unterauftragsverarbeiter folgende Dienstleister beschäftigen:

Art	Nutzungszweck
Reparaturwerkstätten	Zertifizierte Reparaturwerkstätten könnten zum Ausführen von Reparaturdiensten beschäftigt werden.
Hosting-Provider	Hosting-Service-Provider werden in Zusammenhang mit Ferndiensten und Fernzugriff beschäftigt.
IT-Supportdienstleister	IT-Supportdienstleister werden in Zusammenhang mit Reparatur- und Ferndiensten beschäftigt.
Entsorgungsdienstleister	Entsorgungsunternehmen werden in Zusammenhang mit der sicheren Entsorgung von Speichermedien beschäftigt.

Eine Liste der Unterauftragsverarbeiter wird vom Auftragsverarbeiter auf Anfrage des Verantwortlichen zur Verfügung gestellt.

4. Art der personenbezogenen Daten

Die vom Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten betreffen die folgenden Kategorien personenbezogener Daten:

- Allgemeine Daten, wie: Name, Alter, Kennnummer;
- Bilder und Videos, die z. B. während der Verwendung der vertraglichen Geräte angefertigt wurden;
- Zusätzliche Informationen über die Operation, Behandlung, usw. (leeres Textfeld)

5. Spezielle Datenkategorien (falls angemessen)

Die verarbeiteten personenbezogenen Daten betreffen die folgenden speziellen Datenkategorien:

Die personenbezogenen Daten unter Punkt 4. könnten ebenfalls als

- personenbezogene Gesundheitsdaten;
- Daten über das Sexualleben oder die sexuelle Orientierung einer Person

betrachtet werden.

Anhang 2 zum AVV - Technische und Organisatorische Maßnahmen

Die nachfolgende Darstellung orientiert sich hierbei an den in der Art. 32 Datenschutz-Grundverordnung geforderten Maßnahmen, die 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 des Risikos für die Rechte und Freiheiten natürlicher Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen unter anderem Folgendes ein:

A.) Pseudonymisierung personenbezogener Daten

B.) Verschlüsselung personenbezogener Daten

C.) Gewährleistung der Vertraulichkeit der Systeme und Dienste

D.) Gewährleistung der Integrität der Systeme und Dienste

E.) Gewährleistung der Verfügbarkeit der Systeme und Dienste

F.) Gewährleistung der Belastbarkeit der Systeme und Dienste

G.) Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall

H.) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

A. Pseudonymisierung personenbezogener Daten

Maßnahmen zur Pseudonymisierung personenbezogener Daten soweit möglich und sinnvoll:

- Trennung von Kundenstammdaten und Kundenumsatzdaten
- Trennung von Patienten-Kontaktdaten und Behandlungsdaten/Befunden etc.
- Verwendung von Personal-, Kunden-, Patienten-Kennziffern statt Namen für bestimmte Abteilungen.

B. Verschlüsselung personenbezogener Daten

Maßnahmen zur Verschlüsselung soweit möglich und sinnvoll, beispielsweise in stationären und mobilen Speicher-/Verarbeitungsmedien, beim elektronischen Transport:

- symmetrische Verschlüsselung
- asymmetrische Verschlüsselung

C. Gewährleistung der Vertraulichkeit der Systeme und Dienste

Maßnahmen zur Gewährleistung der Vertraulichkeit der Systeme und Dienste, die einen unautorisierten Zugang oder Zugriff auf personenbezogene Daten verhindern sollen, beim Verantwortlichen selbst oder auf dem Transportweg zu Auftragsverarbeitern oder Dritten:

a) Zutrittskontrolle

b) Zugangskontrolle

c) Zugriffskontrolle

d) Weitergabekontrolle

e) Trennungskontrolle

a) Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
Im Rechenzentrum DKS 11 sowie in IT Räumen:

- Regelungen und Anweisungen für die Maßnahmen der Zutrittskontrolle
- Festlegung von Sicherungsbereichen
- Sicherung durch Alarmanlagen, Einbruchsmelder und Polizeinotruf
- Verschließen der Räume nach Dienstende und bei längerer Abwesenheit
- Sicherheitsschlösser mit Schlüsselverwaltung und Schließplan
- Revisionssichere Festlegung von Zutrittsberechtigungen
- Zutrittsregelungen für Personal
- Zutrittsregelungen für Dritte (Reinigungs-, Wartungspersonal, Handwerker, Besucher, ...)
- Legitimation der Zutrittsberechtigten
- Kontrolle des Zutritts
- Revisionsfähigkeit der Vergabe und des Entzugs der Zutrittsberechtigungen
- Berechtigungsausweise / Codekarten
- Gesicherter Eingang für An- und Ablieferung

b) Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Regelungen und Anweisungen für die Maßnahmen der Zugangskontrolle
- Identifikation und Authentisierung der Zugangsberechtigten
- Zugang nur mit Benutzerkennung und Passwort
- Begrenzung der Fehlversuche bei der Anmeldung
- Kontrolle der Benutzung der Datenverarbeitungssysteme
- Protokollierung der Nutzung von Zugangsberechtigungen und deren regelmäßige Auswertung
- Absicherung der DV-Systeme entsprechend den Anforderungen
- Einhaltung der Funktionstrennung bei Vergabe von Zugangsberechtigungen
- Abschließbarkeit von Terminals und dezentralen DV-Systemen
- Identifizierung des Terminals und/oder Terminalbenutzers gegenüber dem DV-System (z.B. Login mit Account und Passwort)
- Automatische Bildschirmsperre bei längerem Inaktivsein

- Funktionelle und/oder zeitlich beschränkte Nutzung von Terminals
- Abschottung interner Netzwerke gegen ungewollte Zugriffe von draußen (Firewall)
- Absicherung der Übertragungsleitungen

c) Zugriffskontrolle

Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

1) Zugriffskontrolle Datenverarbeitungssysteme

Maßnahmen, um Unbefugten den Zugriff zu den Daten und / oder Programmen des Datenverarbeitungssystem zu verwehren, mit welchen personenbezogene Daten verarbeitet oder genutzt werden:

- Regelungen und Anweisungen für die Maßnahmen der Zugriffskontrolle
- Richtlinien für die Dateiorganisation
- Berechtigungs- und Rollenkonzept
- Festlegung der Befugnisse für Dateneingabe sowie Kenntnisnahme, Veränderung und Löschung gespeicherter Daten
- Geregeltes Verfahren über Vergabe, Änderung und Entzug von Zugriffsberechtigungen
- Differenzierte Zugriffsregelungen für Prozeduren
- Benutzerbezogener Zugriffsschutz
- Teilzugriffsmöglichkeit auf Datenbestände und Funktionen
- Funktionelle und/oder zeitlich beschränkte Nutzung von Terminals
- Einsatz von Benutzercodes (Passwörtern) für Dateien, System-, Anwendungs- und Dienstprogramme
- Passwortregeln bei Konfiguration der IT-Systeme umgesetzt
- Identifikation und Authentifizierung der Benutzer
- Maschinelle Überprüfung der Berechtigungen
- Protokollierung der Zugriffe auf bestimmte Dateien (z.B. Konsolprotokoll, Logbuch)
- Kontrolle der Aktivitäten des Systemadministrators
- Absicherung des über selbsttätige Einrichtungen erfolgenden Zugriffs
- Beschränkung des Einsatzes freier Abfragemöglichkeiten (SQL-Query) von Datenbanken
- Anweisungen für Restart-Verfahren
- Automatische Bildschirmsperre bei längerem Inaktivsein
- Einsatz von Verschlüsselungsverfahren

2) Zugriffskontrolle Datenträger

Maßnahmen, um Unbefugten den Zugriff zu den Daten und / oder Programmen zu verwehren, welche sich auf Speichermedien außerhalb des Datenverarbeitungssystems befinden:

- Richtlinien für die Dateiorganisation
- Festlegung der Bereiche, in denen sich Datenträger (z.B. Platten, Bänder, Kassetten, Disketten, Karteien, Mikrofilme) befinden dürfen oder befinden müssen
- Legitimation der Befugten
- Datenschutzgerechte Vernichtung nicht mehr benötigter Datenträger mit Protokollierung
- Verwendung des Schreibschutzes bei Datenträgern
- Kennzeichnungspflicht für Datenträger mit Klassifizierung
- Kontrollierte Lagerung von aktuellen und ausgelagerten Datenträger in einem Sicherheitsbereich (Archiv, Sicherheitsschränke)
- Regelung für die Anfertigung von Kopien
- Verwendung des Schreibschutzes bei Datenträgern

d) Weitergabekontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Maßnahmen zur Sicherstellung, dass bei automatisierten Abrufverfahren durch geeignete Protokollierungsverfahren auch im Nachhinein feststellbar ist, wer welche Daten abgerufen hat
- Regelungen und Anweisungen zu Datenträgertransport und Weitergabekontrolle
- Festlegung und Dokumentation des Übermittlungsverfahrens, der Übermittlungswege und der Datenempfänger
- Festlegung der zur Übermittlung bzw. zum Transport Befugten
- Dokumentation der Abruf- und Übermittlungsprogramme
- Protokollierung der Datenübermittlung und der Empfänger
- Gesicherte Datenleitungen
- Beauftragung zuverlässiger Transportunternehmen
- Verschließbare Transportbehälter
- Einsatz kryptographischer Verfahren soweit anwendbar und gefordert
- Elektronische Signatur soweit anwendbar und gefordert
- Plausibilitätsprüfungen

e) Trennungskontrolle

Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Klare Vorgaben für die Datenerhebung, -verarbeitung und -nutzung
- Dokumentation der Datenbank
- Einrichtung logischer Datenbanken
- Arbeiten mit Pseudonymen soweit möglich und sinnvoll
- Dokumentation der Verarbeitungsprogramme
- Dokumentation der Zwecke der Datenerhebung, -verarbeitung und -nutzung
- Logische Trennung der Daten
- Physische Trennung der Daten
- Erstellung von Benutzerprofilen
- Vergabe von Berechtigungen

D. Gewährleistung der Integrität der Systeme und Dienste

Maßnahmen zur Gewährleistung der Integrität der Systeme und Dienste, die gewährleisten, dass personenbezogene Daten nicht (unbemerkt) geändert werden können.

Hierzu zählen insbesondere:

a) Eingabekontrolle

b) Organisatorische und technische Absicherung

a) Eingabekontrolle

Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Nachweis der organisatorisch festgelegten Zuständigkeiten für die Eingabe
- Revisionssichere Protokollierung der Zugriffsberechtigungen
- Lückenlose Vorgangsprotokollierung für jeden Einzelfall
- Protokollierung über Systemgenerierung und Modifikation von Systemparametern
- Protokollierung der Benutzung verschiedener Administrations-Tools
- Definition von Aufbewahrungs- und Löschungsfristen für die genannten Protokolle
- Protokolldateien sind IT-gestützt auswertbar
- Elektronische Signatur (optional)

b) Organisatorische und technische Absicherung

Maßnahmen, die im Rahmen der innerbetrieblichen Organisation den besonderen Anforderungen des Datenschutzes gerecht werden, insbesondere organisatorische und

technische Absicherung von Berechtigungen, Protokollierungsmaßnahmen, Protokoll-Auswertungen/Revision etc.:

- Bestellung eines Datenschutzbeauftragten
- Organisatorische, räumliche und / oder personelle Abgrenzung der Datenverarbeitung von anderen Unternehmensbereichen und Auftraggebern
- Regelungen zur ordnungsgemäßen und sicheren Abwicklung der mit der Datenverarbeitung verbundenen Aufgaben
- Regelmäßige Schulung der Regelungen
- Überwachung der Einhaltung der Regeln
- Regelungen und Anweisungen für die Maßnahmen der Zutrittskontrolle
- Regelungen und Anweisungen für die Maßnahmen der Zugangskontrolle
- Regelungen und Anweisungen für die Maßnahmen der Zugriffskontrolle
- Regelungen und Anweisungen zu Datenträgertransport und Weitergabekontrolle
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Regelmäßige Aufklärung und Schulung der Mitarbeiter
- Dokumentation von IT-Verfahren, Software, IT-Konfiguration
- Beschreibung der Tätigkeiten in Arbeitsanweisungen
- IT-Notfallkonzept
- Löschungskonzept
- Datensicherungskonzept
- Externe Zertifizierung oder Datenschutzüberprüfungen

E. Gewährleistung der Verfügbarkeit der Systeme und Dienste

Maßnahmen zur Gewährleistung der Verfügbarkeit der Systeme und Dienste, die sicherstellen, dass personenbezogene Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn sie gebraucht werden.

a) Verfügbarkeitskontrolle

- Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:
- Festlegung und Kontrolle von Brandschutzmaßnahmen und Feuer-/ Wasser-Frühwarnsystem
- Brandschutzmaßnahmen
- Erlass von Arbeitsanweisungen und Sicherheitsrichtlinien

- Absicherung der Stromversorgung über unterbrechungsfreie Stromversorgung (USV) und Notstromaggregat
- Notfallkonzept, Notfallhandbuch und Sicherheitsinfrastruktur

- Durchführung einer Risiko- und Schwachstellenanalyse für den betroffenen DV-Bereich
- Zentrale Beschaffung von Hard- und Software
- Funktionstrennung zwischen Fachabteilung und DV-Abteilung
- Formalisierte Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen in Altverfahren
- Einsatz geprüfter und in einem formalisierten Verfahren freigegebener Fremdsoftware
- Regelmäßige Durchführung von Datensicherungen
- Lagerung der Sicherungskopien an geschützten Orten
- Datenbank-Logging
- Recovery-Verfahren
- Datenspiegelung
- Regelmäßige und gründliche Schulung aller Mitarbeiter

b) Auftragskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Schriftlicher Vertrag mit Festlegungen der Weisungen auf der Grundlage der gesetzlichen Vorgaben
- Sorgfältige Auswahl des Auftragnehmers
- Definition von Sicherheitsmaßnahmen
- Kontrolle der ordnungsgemäßen Vertragsausführung
- Kontrolle der Sicherheitseinrichtungen beim Auftragnehmer
- Zutrittsrecht beim Auftragnehmer
- Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber hinsichtlich
- Datensicherungsmaßnahmen
- Transportregelungen
- Aufbewahrungs-, Löschungsvorschriften
- Vertragsverletzungen
- Versicherung

F. Gewährleistung der Belastbarkeit der Systeme und Dienste

Maßnahmen, die sicherstellen, dass die Systeme und Dienste so ausgelegt sind, dass auch punktuell hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen leistbar bleiben.

- Sicherstellung ausreichender Speicher-, Zugriffs- und Leitungskapazitäten

- Ständige Rücksprache mit den Dienstleistern

G. Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall
Hierzu zählen insbesondere:

- Backup-Konzept
- Redundante Datenspeicherung soweit möglich und sinnvoll
- Cloud-Services
- teilweise Doppelte IT-Infrastruktur
- Schatten-Rechenzentrum

H. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen
Hierzu zählen insbesondere:

- Entwicklung eines Sicherheitskonzepts
- Prüfungen des Datenschutzbeauftragten
- Externe Prüfungen, Audits, Zertifizierungen

Data Processing Agreement

This Data Processing Agreement ("DPA") is an integral part of the service contract, support agreement, purchase contract, purchase order confirmation or similar agreement ("Agreement") concluded between Customer (as defined or specified in the Agreement) and the KARL STORZ entity (as defined or specified in the Agreement). By agreeing to or accepting the Agreement, Customer and the KARL STORZ entity also conclude this DPA. For purposes of this DPA, Customer is defined as "Controller" and KARL STORZ is defined as "Processor" (together the "Parties").

PREAMBLE

WHEREAS, Processor offers services for medical products, such as customer care, repair and replacement;

WHEREAS, under the Agreement concluded between Processor and Controller, Processor may provide Controller with the services as further specified in the Agreement and/or in Annex 1 to this DPA (the "Services");

WHEREAS, in rendering the Services, Processor may from time to time be provided with, or have access to information of Controller's patients and staff members and this information may qualify as personal data within the meaning of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR") and other applicable data protection laws;

WHEREAS, Controller engages Processor as a commissioned Processor acting on behalf of Controller as stipulated in Art. 28 GDPR;

WHEREAS, this DPA contains the terms and conditions applicable to the collection, processing and use of such personal data by Processor as a commissioned data Processor of Controller with the aim to ensure that the Parties comply with applicable data protection law.

NOW, **THEREFORE**, and in order to enable the Parties to carry out their relationship in a manner that is compliant with law, the Parties have entered into this DPA as follows:

1. Terminology

For the purposes of this DPA, the terminology and definitions as used by the GDPR shall apply. In addition to that,

"Member State"	shall mean a country belonging to the European Union or to the European Economic Area;
"Subprocessor"	shall mean any further Processor that is engaged by Processor as a sub-contractor for the performance of the Services or parts of the Services on behalf of Controller provided that such Subprocessor has access to the personal data of Controller when carrying out the subcontracted Services.

2. Details of the processing

The details of the processing operations provided by Processor to Controller as a commissioned data Processor (e.g., the subject-matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects) are specified in Annex 1 to this DPA.

3. Obligations of Controller

a) Controller is obliged to ensure compliance with any applicable obligations under the GDPR and any other applicable data protection law that applies to Controller as well as to demonstrate such compliance as required by Art. 5 (2) GDPR.

b) Controller is obliged to provide to Processor the respective records of processing activities according to Art. 30 (1) GDPR relating to the Services under this DPA, to the extent necessary for Processor to comply with the obligation under Art. 30 (2) GDPR.

c) Controller shall designate a data protection officer and/or a representative, to the extent required by applicable data protection law. Controller is obliged to provide contact details of the data protection officer and/or representative, if any, to Processor.

d) Controller confirms before processing is carried out by acceptance of this DPA that the technical and organizational measures of Processor, as set out in Annex 2, are appropriate and sufficient to protect the rights of the data subject and acknowledges that Processor provides sufficient guarantees in this respect.

4. Instructions

a) Controller instructs Processor to process the personal data only on behalf of Controller. Controller's instructions are provided in this DPA. Controller is obliged to ensure that any instruction given to Processor is in compliance with applicable data protection law. Processor is obliged to process the personal data only in accordance with the instructions given by Controller unless otherwise required by European Union or Member State law (in the latter case Sec. 5. (d) (iii) applies).

b) Any further instructions that go beyond the instructions contained in this DPA must be within the subject matter of this DPA and the Agreement. If the implementation of such further instruction results in costs for Processor, Processor shall inform Controller about such costs with an explanation of the costs before implementing the instruction. Only after Controller's confirmation to bear such costs for the

implementation of the instruction, Processor is required to implement such further instruction. Controller shall give further instructions generally in writing, unless the urgency or other specific circumstances require another (e.g., oral, electronic) form. Instructions in another form than in writing shall be confirmed by Controller in writing without delay.

c) Unless Controller cannot carry out rectification, erasure and/or restriction of personal data on its own, instructions may also relate to the rectification, erasure and/or restriction of personal data as set out in Sec. 6.

d) Processor shall immediately inform Controller if, in its opinion, an instruction infringes the GDPR or other applicable European Union or Member State data protection provisions ("Challenged Instruction"). In case Processor is of the opinion that an instruction infringes the GDPR or other applicable European Union or Member State data protection provisions, Processor is not obliged to follow the Challenged Instruction. If Controller confirms the Challenged Instruction upon Processor's information and acknowledges its liability for the Challenged Instruction, Processor will implement such Challenged Instruction, unless the Challenged Instruction relates to (i) the implementation of technical and organizational measures, (ii) the rights of the data subjects, or (iii) the engagement of Subprocessors. In case of (i) to (iii), Processor may contact a competent supervisory authority for a legal assessment of the Challenged Instruction. If the supervisory authority declares the Challenged Instruction as lawful, Processor shall follow the Challenged Instruction. Sec. 4 (b) remains applicable.

5. Obligations of Processor

g) Processor is obliged to ensure that persons authorized by Processor to process the personal data on behalf of Controller, in particular Processor's employees as well as employees of any Subprocessors, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that such persons who have access to the personal data, process such personal data in compliance with Controller's instructions.

h) Processor is obliged to implement the technical and organizational measures as specified in Annex 2 before processing the personal data on behalf of Controller. Processor may amend the technical and organizational measures from time to time provided that the amended technical and organizational measures are not less protective as those set out in Annex 2.

i) Processor is obliged to make available to Controller, upon Controller's request, information in order to demonstrate compliance with the obligations of Processor laid down in Art. 28 GDPR. Upon request by Controller Processor will provide an annual audit report based on ISO 27001 or ISAE3402 or SSAE16-SOC 1 Type 2 or ISAE3000 or SSAE16-SOC 2 Type 2 or similar or similar audit reports created by a third party ("Audit Report"). If additional audit activities are legally required, Controller may request inspections conducted by Controller or another auditor mandated by Controller ("On-Site Audit"). Such On-Site Audit is subject to the following conditions: (i) On-Site Audits are limited to processing facilities and personnel of Processor involved in the processing activities covered by this DPA; and (ii) On-Site Audits occur not more than once annually or as required by applicable data protection law or by a competent supervisory authority or immediately subsequent to a material personal data breach that affected the personal data processed by Processor under this DPA; and (iii) may be performed during regular business hours, solely insubstantially disrupting Processor's business operations and in accordance with

Processor's security policies, and after a reasonable prior notice; and (iv) Controller shall bear any costs arising out of or in connection with the On-Site Audit at Controller and Processor. Controller is obliged to create an audit report summarizing the findings and observations of the On-Site Audit ("On-Site Audit Report"). On-Site Audit Reports as well as Audit-Reports are confidential information of Processor and shall not be disclosed to third parties unless required by applicable data protection law or subject to Processor's consent.

j) Processor is obliged to notify Controller without undue delay:
   (I) about any legally binding request for disclosure of the personal data by a law enforcement authority, unless otherwise prohibited, such as by a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
   (II) about any complaints and requests received directly from a data subject (e.g., regarding access, rectification, erasure, restriction of processing, data portability, objection to processing of data, automated decision-making) without responding to that request, unless Processor has been otherwise authorized to do so;
   (III) if Processor or Subprocessor is required pursuant to European Union or Member State law to which Processor or Subprocessor is subject to process the personal data beyond the instructions of Controller, before carrying out such processing beyond the instruction, unless that European Union or Member State law prohibits such information on important grounds of public interest, in which case the notification to Controller shall specify the legal requirement under such European Union or Member State law; and/or
   (IV) after Processor becomes aware of a personal data breach at Processor or its Subprocessors that affects the personal data of Controller covered by this DPA and in this case Processor will assist Controller with Controller's obligation under applicable data protection law to inform the data subjects and the supervisory authorities, as applicable, by providing information according to Art. 33 (3) GDPR as available to Processor.

k) Processor is obliged to assist Controller with its obligation to carry out a data protection impact assessment as may be required by Art. 35 GDPR and prior consultation as may be required by Art. 36 GDPR that relates to the Services provided by Processor to Controller under this DPA by means of providing the necessary and available information to Controller. Processor shall be obliged to provide such assistance only insofar that Controller's obligation cannot be met by Controller through other means. Processor will advise Controller on the costs for such assistance. Once Controller has confirmed to bear such costs, Processor will provide such assistance.

l) The Controller hereby chooses and instructs Processor to delete by way of secure disposal all the personal data which are processed by Processor on behalf of Controller under this DPA after the end of the provision of Services, and delete any existing copies unless European Union or Member State law requires Processor to retain such personal data. Personal data will only be returned to Controller if expressively agreed by the Parties.

6. Data subjects' rights

a) Controller is primarily responsible for handling and responding to requests made by data subjects.

b) Processor is obliged to assist Controller with the following appropriate and possible technical and organizational measures to respond to requests for exercising the data subjects' rights which are laid down in Chapter III of the GDPR as follows:

(I) With regard to information requests, Processor shall provide to Controller the information as required by Art. 13 and 14 GDPR and as available at Processor only if Controller cannot retrieve such information on its own.

(II) With regard to access requests (Art. 15 GDPR), Processor shall provide Controller with the information that needs to be provided to a data subject relating to such an access request and that is available at Processor only if Controller cannot retrieve such information on its own.

(III) With regard to rectification requests (Art. 16 GDPR), erasure requests (Art. 17 GDPR), restriction of processing requests (Art. 18 GDPR), and portability requests (Art. 20 GDPR), Processor shall, only if Controller cannot itself rectify or, as the case may be, erase, restrict, transmit to another third party the personal data, either provide Controller with the ability to rectify or, as the case may be, erase, restrict, transmit to another third party the affected personal data or if such ability cannot be provided Processor shall provide the necessary assistance to rectify or, as the case may be, erase, restrict, transmit to another third party the affected personal data.

(IV) With regard to notification regarding rectification or erasure or restriction of processing (Art. 19 GDPR), Processor shall assist with notifying any recipients of the personal data that are engaged by Processor as Subprocessors if requested to do so by Controller. Controller will in any event notify any other recipients.

(v) With regard to the right to object as exercised by a data subject (Art. 21 and 22 GDPR) Controller shall determine whether the objection is legitimate and how to address the objection. In case, Controller needs Processor's assistance to address the objection, Controller shall issue a further instruction subject to Sec. 4 (b).

c) Controller is obliged to determine whether or not a data subject has a right to exercise any such data subject rights as set out in this Sec. 6 and to give instructions to Processor to what extent the assistance specified in Sec. 6 (b) is required.

d) In case Controller requires additional or amended technical and organizational measures in order to respond to data subjects' rights, which go beyond the assistance provided by Processor pursuant to Sec. 6 (b), Processor will advise Controller on the costs to implement such additional or amended technical and organizational measures. Once Controller has confirmed to bear such costs, Processor will implement such additional or amended technical and organizational measures to assist Controller to respond to data subjects' requests.

e) Without limitation of Sec. 6 (d), Controller is obliged to reimburse Processor for reasonable out of pocket expenses by Processor in connection with requests made by data subjects.

7. Subprocessing

a) Controller authorizes the use of Subprocessors engaged by Processor for the provision of the Services under this DPA. Processor shall choose such Subprocessor

diligently. Processor remains responsible for any acts or omissions of its Subprocessors in the same manner as for its own acts and omissions hereunder. Controller approves the Subprocessors as described in Annex 1.

b) Processor shall pass on to Subprocessors the obligations of Processor under this DPA to the extent applicable to the subcontracted Services.

c) Processor may remove, replace or appoint suitable and reliable further Subprocessors at its own discretion in accordance with this Sec. 7 (c):
   (I) Processor will notify Controller in advance of any changes to the list of Subprocessors as set out under Sec. 7 (a). If Controller does not object in accordance with Sec. 7 (c) (ii) within thirty days after receipt of Processor's notice the further Subprocessor(s) shall be deemed accepted.
   (II) If Controller has a legitimate reason to object to a further Subprocessor, Controller shall notify Processor thereof in writing within thirty days after receipt of Processor's notice. If Controller objects to the use of the further Subprocessor, Processor shall have the right to cure the objection through one of the following options (to be selected at Processor's sole discretion): (a) Processor will cancel its plans to use the further Subprocessor with regard to Controller's personal data; or (b) Processor will take the corrective steps requested by Controller in its objection (which remove Controller's objection) and proceed to use the further Subprocessor with regard to Controller's personal data; or (c) Processor may cease to provide or Controller may agree not to use (temporarily or permanently) the particular aspect of the Service that would involve the use of such further Subprocessor with regard to Controller's personal data. If none of the above options are reasonably available and the objection has not been cured within thirty days after Processor's receipt of Controller's objection, either Party may terminate the affected Service with reasonable prior written notice.

d) In case any Subprocessor is located outside the EU/EEA in a country that is not recognized as providing an adequate level of data protection, Processor will take measures to address the requirement of an essentially equivalent level of data protection at Subprocessor (such measures may include in particular the conclusion of data processing agreements based on EU Model Clauses).

8. Liability and limitation of liability

a) Each Party is liable for its obligations set out in this DPA and in applicable data protection law.

b) Unless otherwise agreed in the Agreement or in this DPA, the following shall apply with regard to any liability arising out of or in connection with a violation of the obligations of this DPA or under applicable data protection law:

   (I) Processor's contractual and statutory liability for damages caused by slight negligence shall, irrespective of its legal ground, be limited as follows:

   Processor shall be liable up to the amount of the foreseeable damages typical for this type of contract due to a breach of material contractual obligations;

   Processor shall not be liable due to a breach of any non-material contractual obligations nor for the slightly negligent breach of any other

applicable duty of care.

(II) The aforesaid limitations of liability shall not apply to any mandatory statutory liability, in particular to liability under the German Product Liability Act (Produkthaftungsgesetz), and liability for culpably caused personal injuries. In addition, such limitations of liability shall not apply if and to the extent Processor has assumed a specific guarantee.

(III) Sec. 8 (b) (i) and (ii) shall apply analogously to Processor's liability for reliance damages (damages suffered in reliance on the validity of the contract).

(IV) Controller shall be obliged to take adequate measures to avert and reduce damages.

9. Indemnification

Unless otherwise agreed in the Agreement or in this DPA, Controller will defend, indemnify, and hold harmless Processor and the officers, directors, employees, successors, and agents of Processor from all claims, damages, liabilities, assessments, losses, costs, administrative fines and other expenses (including, without limitation, reasonable attorneys' fees and legal expenses) arising out of or resulting from any claim, allegation, demand, suit, action, order or any other proceeding by a third party (including supervisory authorities) that arises out of or relates to the culpable violation of Controller's obligations under this DPA and applicable data protection law.

10. Duration and termination

The term of this DPA is identical with the term of the obligations under the relevant Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the relevant Agreement if applicable.

11. Miscellaneous

a) In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, the provisions of this DPA shall prevail with regard to the Parties' data protection obligations related to the Services. In case of doubt as to whether clauses in such other agreements relate to the Parties' data protection obligations, this DPA shall prevail.

b) Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or – should this not be possible – (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. The foregoing shall also apply if this DPA contains any omission.

c) This DPA shall be governed by the same law as the Agreement except to the extent that mandatory applicable data protection law applies.

d) The place of jurisdiction for all disputes regarding this DPA shall be the principle place of business of Processor except to the extent that mandatory applicable data protection law applies.

e) Prior to the effective date of the GDPR on May 25, 2018, any reference to the GDPR shall be read as reference to the corresponding provision in the EU Data Protection Directive and/or any other applicable data protection law. With the effective date of the GDPR on May 25, 2018, any reference to the GDPR shall include the reference to the corresponding provision in any other applicable data protection law, in particular Member State data protection law.

f) The Parties have the right to ask for changes to this DPA to the extent required to satisfy any interpretations, guidance or orders issued by competent Union or Member State authorities, national implementation provisions, or other legal developments concerning the GDPR requirements for the commissioning of data processors.

g) The Parties will amend Annex 2, if required, in a timely manner before the date the GDPR becomes applicable in order to meet the requirements on technical and organizational security measures as per Art. 32 GDPR.

Annex 1 to the DPA – Description of the processing activities

6. Categories of data subjects

The personal data processed concern the following categories of data subjects:

- Patients of the Controller;
- Staff Members of the Controller.

7. Subject-matter of the processing

The Processor will have access to personal data stored in or in connection with the medical products for which Processor may provide repair and replacement services.

8. Nature and purpose of the processing

Processor processes the personal data of the data subjects on behalf of Controller in connection with carrying out the repair and replacement services.

- Repair services at the Processor:

  The medical products will be examined and repaired (where possible) at the Processor. Depending on the repair activity an access to personal data stored on the medical product could be possible. Processor expressively instructs Controller to delete any data on the medical product.

  The Controller shall back-up and then delete all data before the medical product will be sent to the Processor. The Processor does not accept any responsibility for data loss or damage.

- Field repair services / Remote service:

  Processor's technicians in the field will visit the Controller in case of technical problems with the contractual product or might access the device via a remote connection.

  The medical products will be examined and maintained / repaired (where possible) at the Controller. Depending on the maintenance / repair activity an access to personal data stored on the medical product could be possible. Personal data will usually not be deleted by the Processor unless instructed otherwise by Controller.

  The Controller shall back-up and then delete all data before the medical product will examined by the Processor. The Processor does not accept any responsibility for data loss or damage.

Only if requested by Controller during Field repair service: If storage mediums are replaced during repair services the data will be copied to a new storage medium of the medical device.

Processor may engage service providers acting as Subprocessors:

Type	Purpose of use
Repair shops	Certified repair shops might be engaged to carry out repair services
Hosting provider	Hosting service provider are engaged in connection with remote services and remote access
IT support service provider	IT support services providers are engaged in connection with repair and remote services
Disposal service providers	Disposal companies are engaged in connection with the secure disposal of storage media

A list of Subprocessors will be provided by Processor upon request of Controller.

9. Type of personal data

The personal data processed by Processor on behalf of Controller concern the following categories of personal data:

- General Data, such as: Name, Age, ID number;
- Pictures and videos, e.g., made during use of contractual devices;
- Additional information on the operation, treatment etc. (free text field)

10. Special categories of data (if appropriate)

The personal data processed concern the following special categories of data:
The personal data under 4. might also be considered as personal data concerning

- health;
- a natural person's sex life or sexual orientation

Appendix 2 to DPA - Technical and Organizational Measures

The discussion below is based on the measures set forth in Art. 32 Data Protection Act that are required to guarantee an adequate level of protection taking into account the state of technology, the implementation costs, and the type, scope, circumstances, and purposes of processing as well as the probabilities of occurrence and seriousness of the risks to the rights and freedoms of natural persons. For example, these measures include the following:

A.) Pseudonymizing personal data

B.) Encrypting personal data

C.) Ensuring the confidentiality of systems and services

D.) Ensuring the integrity of systems and services

E.) Ensuring the availability of systems and services

F.) Ensuring the resilience of systems and services

G.) Restoration of the availability of personal data and access to them after a physical or technical incident

H.) Processes for regularly testing, assessing, and evaluating the effectiveness of the above measures

A. Pseudonymizing personal data
Measures for the pseudonymization of personal data to the extent possible and appropriate:

- Separation of customer master data and customer sales data
- Separation of patient contact data and treatment data / findings, etc.
- Use of staff/customer/patient IDs instead of names for particular departments

B. Encrypting personal data
Measures for encryption to the extent possible and appropriate, for instance in stationary and mobile memory/processing media or in electronic transport:

- symmetric encryption
- asymmetric encryption

C. Ensuring the confidentiality of systems and services
Measures taken to ensure the confidentiality of systems and services to prevent unauthorized logical or data access to personal data, either at the responsible person's workplace or during transport to contract processors or third parties:

a) Physical access control

b) Logical access control

c) Data access control

d) Data transmission control

e) Separation control

c) Physical access control

Measures taken to prevent unauthorized persons from physically accessing the data processing systems with which personal data are processed or used
At the DKS 11 data center and in IT rooms:

- Regulations and instructions regarding physical control measures
- Specification of secure areas
- Security in the form of alarm systems, intruder alarms, and automatic calls to police
- Locking of rooms after the shift and in case of extended absence
- Security locks with key management and lock plan
- Audit-proof specification of physical access authorizations
- Rules for physical access by staff
- Rules for physical access by third parties (cleaning, maintenance staff, craftsmen, visitors, etc.)
- Authentication of holders of physical access authorizations
- Control of physical access
- Auditability of the granting and withdrawal of physical access authorizations
- Authorization ID / code cards
- Secure entrance for incoming and outgoing deliveries

d) Logical access control

Measures taken to prevent the use of data processing systems by unauthorized persons:

- Regulations and instructions regarding logical access control measures
- Identification and authentication of persons with logical access rights
- Logical access only with username and password
- Limitation of the number of failed login attempts
- Monitoring of the use of data processing systems
- Logging of the use of logical access authorizations and regular analysis thereof
- Protection of the data processing systems according to needs
- Adherence to the separation of functions when assigning logical access authorizations
- Lockability of terminals and decentralized data processing systems
- Identification of the terminal and/or terminal user to the data processing system (e.g., login with account and password)
- Automatic screen lock in case of extended inactivity
- Functionally limited and/or time limited use of terminals
- Isolation of internal networks from unwanted external access (firewall)

- Securing of transmission lines

e) Data access control

Measures taken to ensure that the persons authorized to use a data processing system can exclusively access the data they are authorized to access and that personal data cannot be read, copied, altered, or removed without authorization during processing or use or after they are saved.

3) Data access control for data processing systems

Measures taken to prevent unauthorized persons from accessing the data and/or programs of the data processing system with which personal data are processed or used:

- Regulations and instructions regarding data access control measures
- Guidelines for file organization
- Authorization and role concept
- Definition of authorizations for data entry as well as for the disclosure, altering, and deletion of stored data
- Regulated procedure for the allocation, change, and withdrawal of data access rights
- Differentiated data access rules for procedures
- User-related data access protection
- Optional partial data access to some data pools and functions
- Functionally limited and/or time limited use of terminals
- Use of user codes (passwords) for files and system, application, and service programs
- Password rules implemented in the configuration of IT systems
- User identification and authentication
- Automatic testing of authorizations
- Logging of accesses to certain files (e.g., console protocol, logbook)
- Control of system administrator activities
- Securing of access through automatic devices
- Restriction of the use of free queries (SQL query) of databases
- Instructions for restart procedures
- Automatic screen lock in case of extended inactivity
- Use of encryption procedures

4) Data access control for data storage devices

Measures taken to prevent unauthorized persons from accessing the data and/or programs on storage devices outside of the data processing system:

- Guidelines for file organization

- Definition of the areas in which data storage devices (e.g., disks, tapes, cassettes, diskettes, files, microfilms) may or must be located
- Legitimization of authorized individuals
- Destruction of data storage devices that are no longer needed in accordance with data protection requirements, with logging
- Use of write protection on data storage devices
- Mandatory labeling for data storage devices with classification
- Controlled storage of current and swapped data storage devices in a secure area (archive, safety storage cabinets)
- Rules on the creation of copies
- Use of write protection on data storage devices

f) Data transmission control

Measures taken to ensure that personal data cannot be read, copied, altered, or removed without authorization during electronic transmission or during transport or storage on data storage devices and to ensure that it is possible to examine and establish where personal data are to be transmitted by data transmission equipment:

- Measures taken to ensure that in case of automatic retrieval processes, suitable logging procedures allow determining even in retrospect who retrieved which data
- Regulations and instructions on the transport of data storage devices and data transmission control
- Determination and documentation of the transmission procedure, transmission pathways, and data recipients
- Definition of the persons authorized to transmit or transport
- Documentation of the retrieval and transmission programs
- Logging of the data transmission and recipients
- Secure data lines
- Commissioning of reliable transport companies
- Lockable transport containers
- Use of cryptographic procedures to the extent applicable and required
- Electronic signatures to the extent applicable and required
- Plausibility checks

g) Separation control

Measures taken to ensure that data collected for different purposes can be processed separately:

- Clear specifications for data collection, processing, and use

- Documentation of the database
- Setup of logical databases
- Use of pseudonyms to the extent possible and sensible
- Documentation of the processing programs
- Documentation of the purposes of data collection, processing, and use
- Logical separation of data
- Physical separation of data
- Generation of user profiles
- Assignment of authorizations

D. Ensuring the integrity of systems and services
Measures taken to ensure the integrity of the systems and services that ensure that personal data cannot be altered (unnoticed).

This particularly includes:

a) Input control

b) Organizational and technical security

h) Input control

Measures taken to ensure that it is possible to retrospectively examine and establish whether and by whom personal data have been entered, altered, or removed:

- Proof of organizationally specified responsibilities for the input
- Audit-proof logging of data access rights
- Complete process logging for each individual case
- Logging of the system generation and modification of system parameters
- Logging of the use of different administration tools
- Definition of retention and deletion periods for the listed logs
- Log files analyzable with IT support
- Electronic signatures (optional)

i) Organizational and technical protection

In-house organization measures that meet the special requirements of data privacy, particularly organizational and technical protection of authorizations, logging measures, log analysis/review, etc.:

- Appointment of a data protection officer
- Organizational, spatial, and/or staff-based separation of data processing from other areas of the company and customers
- Regulations for the proper and safe completion of tasks associated with data processing

- Periodic training on regulations
- Monitoring of compliance with rules
- Regulations and instructions regarding physical control measures
- Regulations and instructions regarding logical access control measures
- Regulations and instructions regarding data access control measures
- Regulations and instructions on data storage device transport and data transmission control
- Obligation of employees to comply with data secrecy
- Periodic employee information and training
- Documentation of IT processes, software, IT configuration
- Description of activities in work instructions
- IT emergency plan
- Deletion concept
- Data backup plan
- External certification or data privacy audits

E. Ensuring the availability of systems and services
Measures taken to ensure the availability of the systems and services that ensure that personal data are available at all times and without limitations and that in particular, they are available when they are needed.

a) Availability control

Measures taken to ensure that personal data are protected against accidental destruction or loss:

- Definition and control of fire protection measures and fire/water early warning systems
- Fire protection measures
- Issuing of work instructions and safety guidelines
- Securing of the power supply through an uninterruptible power supply (UPS) and emergency generator
- Emergency plan, emergency handbook, and safety infrastructure
- Conduct of risk and vulnerability analysis for the affected data processing area
- Central purchasing of hardware and software
- Functional separation between specialist department and data processing department
- Formalized release procedures for new data processing procedures and for important changes in existing procedures

- Use of third-party software subject to testing and release in a formalized procedure
- Regular data backup
- Storage of backup copies in protected locations
- Database logging
- Recovery procedure
- Data mirroring
- Periodic and thorough training of all employees

b) Order control

Measures taken to ensure that personal data that are processed by subcontractors can only be processed in conformance with the instructions of the ordering party

- Written contract with specification of instructions on the basis of legal requirements
- Careful selection of the subcontractor
- Definition of safety measures
- Control of proper execution of the contract
- Control of subcontractor's safety mechanisms
- Availability of physical access to the subcontractor's premises
- Definition of the competences and duties of subcontractor and ordering party as regards
    - Data protection measures
    - Transport rules
    - Retention/deletion rules
    - Contract violations
    - Insurance

F. Ensuring the resilience of systems and services

Measures taken to ensure that the systems and services are designed in such a way that they can manage high temporary processing workloads or high permanent processing workloads

- Securing of sufficient storage, access, and output capacities
- Continuous consultation with service providers

G. Restoration of the availability of personal data and access to them after physical or technical incidents

This particularly includes:

- Backup concept
- Redundant data storage to the extent possible and appropriate
- Cloud services

- In parts duplicate IT infrastructure
- Shadow data center

H. Processes for regularly testing, assessing, and evaluating the effectiveness of the above measures

This particularly includes:

- Development of a security concept
- Review by the data protection officer
- External review, audits, certifications