Auftragsverarbeitungs-Vereinbarung – Sunrise Medical als Auftragnehmer

zwischen

- nachfolgend "Verantwortlicher" genannt -	und	**Sunrise Medical GmbH** **Kahlbachring 2-4** **D-69254 Malsch / Heidelberg** - nachfolgend "Auftragsverarbeiter" genannt -

Präambel

Im Rahmen des zwischen den Parteien geschlossenen Vertrags zur Lieferung und Anpassung von Rollstühlen ("Leistungsbeschreibung") inkl. Nebenleistungen wie Schulung, Beratung und Reklamationsmanagement sowie Qualitätssicherung wird der Auftragsverarbeiter Einblick in personenbezogene Daten des Verantwortlichen haben bzw. diese verarbeiten. Die Regelungen dieser Vereinbarung finden auch Anwendung auf zukünftige gleichartige Leistungsbeschreibungen. Aus datenschutzrechtlicher Sicht handelt es sich um Auftragsverarbeitung (im Folgenden „AV“) gem. Art. 28 Datenschutzgrundverordnung (im Folgenden „DSGVO“). Bei der AV bleibt der Verantwortliche datenschutzrechtlich verantwortlich dafür, dass die personenbezogenen Daten entsprechend geschützt sind. Nach Art. 82 Abs.4 DSGVO wird der Auftragsverarbeiter im Außenverhältnis gesamtschuldnerisch Mithaftender. Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

1. Gegenstand und Dauer der Vereinbarung

Der Umfang der Verarbeitung (Gegenstand / Art / Zweck der Datenerhebung, -verarbeitung oder –nutzung, die Art der Daten sowie der Kreis der Betroffenen) wird in Anlage 1 geregelt.

Die Vereinbarung gilt für alle Geschäftsvorfälle gem. Anlage 1 zwischen den Vertragsparteien. Die Dauer der Verarbeitung richtet sich nach den jeweiligen Aufbewahrungsfristen.

2. Pflichten des Verantwortlichen

2.1. Für die Beurteilung der Zulässigkeit der Datenverarbeitung/-erhebung/-nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Verantwortliche verantwortlich. Der Auftragsverarbeiter unterstützt den Verantwortlichen darin und leitet etwaige an ihn gerichtete Anfragen von Betroffenen unverzüglich weiter.

2.2. Der Verantwortliche ist nach Art. 28 Abs. 1 DSGVO verpflichtet, die Zuverlässigkeit des Auftragsverarbeiters vor Beginn der Verarbeitung und sodann regelmäßig zu überprüfen. Der Auftragsverarbeiter wird ihn dabei unterstützen.

2.3. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und entsprechend in Anlage 1 dieser Vereinbarung festzulegen oder in gesonderter, schriftlicher Leistungsbeschreibung bzw. Vertragsänderung.

2.4. Der Verantwortliche behält sich das Recht vor, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragsverarbeiter zu erteilen.
Alle Ergänzungen werden dokumentiert und mündliche Weisungen werden unverzüglich schriftlich oder per E-Mail durch den Verantwortlichen dokumentiert

2.5. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen entstehen, bleiben unberührt. Der Verantwortliche muss erwartete Mehraufwände vor Realisierung freigeben.

2.6. Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse oder einen begründeten Verdacht feststellt.

2.7. Der Verantwortliche ist verpflichtet, alle erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiter vertraulich zu behandeln.

3. Pflichten des Auftragsverarbeiters

3.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen. Er hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Verantwortliche dies in getroffener Vereinbarung oder einer Weisung verlangt.

3.2. Der Auftragsverarbeiter verarbeitet die Daten ausschließlich in Mitgliedsstaaten der EU oder des EWR. Ausnahmen sind mit schriftlicher Zustimmung des Verantwortlichen und Nachweis eines angemessenen Datenschutzniveaus im Verarbeitungsstaat nach Art. 44ff. DSGVO möglich.

3.3. Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen Daten - ohne Wissen des Verantwortlichen – für keine anderen als die im dieser Vereinbarung bestimmten Zwecke. Davon nicht erfasst sind Daten, die im Rahmen von Sicherungsmaßnahmen hinsichtlich der Verfügbarkeit erstellt werden (Backups).

3.4. Soweit vom Leistungsumfang umfasst, ist das Recht auf Löschung, Berichtigung von Daten, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen. Etwaiger Mehraufwand ist vom Auftragsverarbeiter anzumelden.

3.5. An den Auftragsverarbeiter gerichtete Anfragen Betroffener leitet dieser unverzüglich an den Verantwortlichen weiter. Er unterstützt den Verantwortlichen bei der fristgerechten Beantwortung und stellt proaktiv die notwendigen Informationen zur Information Betroffener nach Art. 12 ff. DSGVO zur Verfügung.

3.6. Dem Auftragsverarbeiter ist bekannt, dass nach. Art. 33 f. DSGVO strafbewehrte Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können.

Deshalb sind Vorfälle in jeglicher Art und Weise von unrechtmäßiger Übermittlung oder Kenntniserlangung unverzüglich dem Verantwortlichen mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei gegen den Auftragsverarbeiter eingeleiteten Ermittlungen von Straf- oder Aufsichtsbehörden. Der Auftragsverarbeiter hat unverzüglich angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

3.7. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Sofern der vermutete Verstoß

schriftlich zur Kenntnis gebracht wurde, ist der Auftragsverarbeiter berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Verantwortlicher bestätigt oder geändert wird. Dies gilt auch für etwaige Subunternehmer.

3.8. Der Auftragsverarbeiter wird den Verantwortlichen oder einen vom Verantwortlicher bestellten Dritten jederzeit im Rahmen des Zumutbaren bei der Durchführung von Kontrollen bezüglich der Einhaltung der Vorschriften über den Datenschutz und die vertraglichen Vereinbarungen unterstützen, z.B. durch Bereitstellung geeigneter Dokumentation, Gewährung von Zutritt zur Inaugenscheinnahme oder Nachweis der Einhaltung geeigneter Verhaltensregeln nach Art. 40 DSGVO, einschlägiger Zertifizierungen nach Art. 42 DSGVO oder anderer Prüfberichte. Der Verantwortliche hat das Recht, die vertragsgemäße Datenverarbeitung beim Auftragsverarbeiter zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragsverarbeiters erfolgen. Die Vor-Ort-Kontrolle ist mit angemessener Frist durch den Verantwortlichen anzukündigen.

3.9. Nach Abschluss der vertraglichen Arbeiten archiviert der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen und Dokumentationen mindestens für die Dauer der Garantie bzw. der handels- und steuerrechtlichen Aufbewahrungsfristen.

4. Subunternehmer

4.1. Die Beauftragung von Subunternehmern ist zugelassen, sofern der Auftragsverarbeiter dem Subunternehmer dieselben Datenschutzpflichten auferlegt, wie sie zwischen dem Verantwortlichen dem Auftragsverarbeiter vereinbart wurden und der Auftragsverarbeiter deren Einhaltung regelmäßig kontrolliert und das Ergebnis der Kontrollen dokumentiert.

4.2. Es dürfen nur Subunternehmer innerhalb der EU / des EWR beschäftigt werden. Nicht als Subunternehmer gem. dieser Vereinbarung sind Dienstleister von Unterstützungsleistungen wie Logistik- oder Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungs- und Bewachungspersonal, Entsorger von Datenträgern sowie solche ohne Zugriff auf die personenbezogenen Daten des Auftraggebers.

4.3. Der Auftragsverarbeiter hält eine Liste der an der Auftragsverarbeitung für den Verantwortlicher beteiligten bzw. auf dessen Daten zugriffsberechtigten Subunternehmer zum Abruf durch den Verantwortlichen bereit. Die bei Abschluss der Vereinbarung beschäftigten Subunternehmer gelten als genehmigt. Über neue Subunternehmer, die Zugriff auf Datenbestände des Verantwortlichen erhalten, informiert der Auftragsverarbeiter den Verantwortlichen mit einer Vorlaufzeit, die es diesem ermöglicht, dagegen Widerspruch einzulegen. Der Auftraggeber darf nur bei berechtigten, nachweisbaren und konkreten Zweifeln an dessen Zuverlässigkeit widersprechen. Im Falle eines Widerspruchs, hat der Auftragsverarbeiter die Möglichkeit, das Vertragsverhältnis zum nächstmöglichen Termin einvernehmlich zu beenden.

5. Datenschutz und Sicherheit der Verarbeitung

5.1. Der Auftragsverarbeiter hält die gesetzlichen Regelungen nach Art. 28-33 DSGVO ein und unterstützt den Verantwortlichen bei der Einhaltung der Art. 32-36 DSGVO soweit zumutbar. Sofern er nach Art. 38 DSGVO dazu verpflichtet ist, einen Datenschutzbeauftragten zu benennen, teilt er die Kontaktdaten – insbes. auch im Fall eines Wechsels – dem Verantwortlichen mit.

5.2. Der Auftragsverarbeiter darf nur solche Beschäftigten den Zugang zu personenbezogenen Daten des Verantwortlichen gewähren, die eine Vertraulichkeitsvereinbarung hinsichtlich personenbezogener Daten unterzeichnet haben, sowie hinsichtlich der Bestimmungen des Datenschutzes geschult wurden. Diese Vertraulichkeitsvereinbarung der Beschäftigten mit Zugang zu personenbezogenen Daten ist auf Anfrage dem Verantwortlichen nachzuweisen.

5.3. Auskünfte darf der Auftragsverarbeiter nur nach vorheriger, mindestens in Textform vorliegender Zustimmung durch den Verantwortlichen erteilen.

6. Datensicherheitsmaßnahmen Art. 28 Abs. 3 c), Art. 32 DSGVO

(s. auch Anlage 2)

6.1. Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet und dokumentiert die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen und stellt diese Dokumentation dem Verantwortlichen auf Anforderung und in dem Umfang, wie sie zur Erbringung der Leistung relevant sind, zur Verfügung, um den Anforderungen des Art. 5 DSGVO gerecht zu werden.

6.2. Die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt. Sie sollen den Schutzzielen der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Systeme angemessen im Hinblick auf Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen Rechnung tragen. Die beschriebenen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden.

6.3. Soweit die beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht oder nicht mehr genügen, benachrichtigt der Verantwortliche den Auftragsverarbeiter. Eine einvernehmliche Regelung über etwaige Mehraufwände zur Erfüllung der Anforderungen bleibt unberührt.

7. Laufzeit

7.1. Diese Vereinbarung wird auf unbestimmte Zeit geschlossen und kann von jeder Partei mit Frist von einem Monat gekündigt werden.

7.2. Die Datenschutzpflichten des Auftragsverarbeiters einschließlich der sicherheitsrelevanten Maßnahmen gelten nach Beendigung des Auftragsverhältnisses fort, sofern noch personenbezogene Daten verarbeitet werden, z.B. noch Daten des Verantwortlichen gespeichert werden.

7.3. Der Verantwortliche kann die zugrundeliegende Leistungsbeschreibung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen die Bestimmungen dieser Vereinbarung vorliegt.

8. Haftung

8.1. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Auftragsverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Verantwortliche gegenüber den Betroffenen verantwortlich. Ihm bleibt der Rückgriff auf den Auftragsverarbeiter bei Verstoß gegen diese Vereinbarung vorbehalten.

8.2. Aufgrund der gesamtschuldnerischen Haftung auch des Auftragsverarbeiters nach Art. 82 DSGVO bei rechtswidriger Datenverarbeitung sichert der Verantwortliche zu, den Auftragsverarbeiter hinsichtlich dieser Haftung sowie in Bezug auf die Verteidigung gegen solche Ansprüche schadlos zu stellen, sofern nicht ein Verstoß dessen gegen diese Vereinbarung vorliegt, unabhängig davon, ob die Verarbeitung tatsächlich rechtswidrig ist.

9. Sonstiges

Für Nebenabreden ist die Schriftform erforderlich, das gilt auch für die Streichung der Schriftformklausel.

…….. Ort, Datum	…….. Ort, Datum
…….. Unterschrift Verantwortlicher	…….. Unterschrift Auftragsverarbeiter

Anlage 1 zur Vereinbarung über Auftragsverarbeitung (AV)

Gegenstand des Auftrages / Leistungsinhalte

Produktion, Anpassung, Beratung, Reparaturen und Reklamationsmanagement von Rollstühlen

Umfang, Art und Zweck der Datenverarbeitung oder -nutzung

Im Rahmen des o.g. Gegenstandes der Verarbeitung werden personenbezogene Daten der u.g. Gruppen Betroffener erhoben.
Darunter Kontaktdaten, Daten zur Lieferung, Daten zur Konfiguration des Produktes sowie Daten über bestimmte Krankheitsbilder, die die Konfiguration beeinflussen (Gesundheitsdaten).

Kontaktdaten des Datenschutzbeauftragten

Der bestellte Datenschutzbeauftragte ist erreichbar unter:

datenschutz@sunrisemedical.de oder postalisch.

Weisungsgeber/-empfänger

Weisungsberechtigt beim Verantwortlichen:	**Empfangsberechtigt beim Auftragsverarbeiter:** Director Sales Germany & Austria (Leiter Vertrieb & Marketing)

	Director Operations Germany Senior Director Commercial Services Central Europe

Kreis zugriffsberechtigter Personen beim Auftragsverarbeiter (Gruppen/Rollen)

Gruppe/Rolle: Mitarbeiter im Kundenservice, im Vertrieb / Außendienst, im Reklamationsmanagement, in der Produktion, in der Qualitätssicherung, im Reparatur Bereich

Beschreibung der Daten

Beschreibung	**Schutzwürdigkeit**		
Betroffene	Normaler Schutzbedarf, allgemein zugängliche Daten und geringfügig vertrauliche Daten, z.B. Adressen	Hoher Schutzbedarf, vertrauliche und sensible Daten und Dokumente, z.B. Gehaltslisten, Passwörter	Besondere Arten von Daten, sehr hoher Schutzbedarf, z.B. nach Art. 9, 10 DSGVO z.B. Gesundheitsdaten; Daten, die einem Berufsgeheimnis unterliegen, Sozialdaten, Bank-/ Kreditkartendaten, Partei-Gewerkschaftszugehörigkeit, Religion, etc.
Kunden des AGs (Endkunden)	X	X	X
Mitarbeiter des AGs	X	X	☐
sonstige Dritte	X	X	☐

Anlage 2 – technisch-organisatorische Maßnahmen (TOMs)

Dokumentation der technischen und organisatorischen Maßnahmen (TOMs) nach Art. 32 DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

- Geregelte Zutrittskontrolle durch ständig besetzten Empfang, Videoüberwachung, Schließregelung, kontrollierte Vergabe von Schlüsseln und Zutrittskarten

1.2 Zugangskontrolle

- Benutzerindividuelle Accounts in der Verwaltung

1.3 Zugriffskontrolle

- Vergabe von Zugriffsrechten und Berechtigungskonzept, Rollenmodell, Genehmigungsprozesse, regelmäßige Prüfung der Berechtigungen

1.4 Trennungskontrolle

- Logische Trennung von Daten verschiedener Auftraggeber durch IT-technische Verfahren bzw. Trennung der Daten für einzelne Aufträge

1.5 Pseudonymisierung

- sofern vom Auftraggeber unterstützt keine personenbezogene Daten in der Produktion aufgrund von pseudonymisierter Fertigung

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

- Übermittlung von Auftragsdaten des Auftraggebers via SSL-verschlüsselte Verbindung auf dem Webportal

2.2 Eingabekontrolle

- Protokollierung von Veränderungen an Auftragsstati, Dokumentenmanagement

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfügbarkeitskontrolle

- Regelmäßige Datensicherungen, sichere Serverumgebung, Einsatz von Virenschutz und Firewall, klare Meldewege, Notfallpläne Wiederanlaufpläne nach Art. 32.I c) DSGVO)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32.I. d) DSGVO; Art. 25.I DSGVO)

- Schulung der Mitarbeiter mit Zugang zu personenbezogenen Daten im Datenschutz
- Betrieb eines Datenschutz-Management-Systems mit regelmäßigen Jour Fixes mit dem bestellten (externen) Datenschutzbeauftragten

Liste von Subunternehmern

Sunrise Medical Limited Thorns Road Brierley Hill West Midlands DY5 2LD United Kingdom	Server-Wartung und IT-Management