Henry Schein Medical Austria GmbH - Remote Service - Fernwartungsvereinbarung

1. Vereinbarungsgegenstand

(1) Gegenstand dieser Vereinbarung ist die Durchführung von Fernwartung durch die Henry Schein Medical Austria GmbH ("**HSMED**") im Rahmen des Remote-Service sowie die Regelung datenschutzrechtlicher Fragen im Sinne von Art. 28 DSGVO in diesem Zusammenhang.

Die Wartung folgender Systeme und Komponenten wird von dieser Vereinbarung umfasst:

- Cardiossoft - Ruhe-EKG, ERGO, LUFU, LZ-RR
- Cardioday - LZ-EKG
- Cardioread - LZ-EKG
- Profman - LZ-RR
- ProfilmanagerXD - LZ-RR, ABI
- EASYonCS/PC/Connect LUFU
- SonoGDT - Sono, EKG
- MESI - Ruhe-EKG
- Cardioline Connectivity - Ruhe-EKG
- Cardioline Cube/Touch ECG
- Vitalograph – LUFU
- Vitalograph Spirotrac/BT12/PDF-Report/Connect
- Mela Soft

Im Zusammenhang mit der Fernwartung kann nicht ausgeschlossen werden, dass Zugriff auf die auf Ihren Systemen befindlichen Daten erfolgt. Dies kann personenbezogene Daten, einschließlich besonderer Daten im Sinne der DSGVO, d.h. z.B. Gesundheitsdaten, betreffen.

(2) Im Rahmen des Remote-Service wird Sie HSMED bei nachfolgenden Problemstellungen/Fehlern unterstützen und die folgenden Dienstleistungen anbieten:

a. Im Rahmen der Gewährleistung kostenfrei
   - Support bei systembedingten, technischen Problemanalysen und -lösungen in der Anwendungssoftware und/oder Hardware, gegebenenfalls auch mit Unterstützung des jeweiligen Lieferantensupports.

b. Kostenpflichtig:
   - Software-, Hardware-, oder Systemanwendungstrainings oder fallbezogenes -coaching ggf. auch mit Tipps und Tricks
   - Hilfestellungen bei allen Software-Anwendungsthemen rund um medizinische und systemspezifische Anwendungen
   - Hilfestellung beim Installieren von Updates und Patches
   - Netzwerküberprüfung und –konfigurationen
   - Individuelle kundenspezifische Systemkonfigurationen sowie Wiederherstellung bei Systembedienungsfehler
   - Unterstützung beim Datentransfer

(3) Vorstehende Leistungen werden von HSMED nach Wunsch und Erforderlichkeit wie folgt erbracht:
   - Support per Telefon und/oder E-Mail (kostenfrei)
   - Fernwartung mittels Remoteverbindung und Chat (fallabhängig kostenpflichtig)

(4) Die Fernwartungsleistungen werden von Montag bis Donnerstag zwischen 8.00 Uhr und 17.00 Uhr und Freitag zwischen 8.00 Uhr und 14.30 Uhr erbracht. Außerhalb dieser Geschäftszeiten werden keine Leistungen erbracht.

(5) Sollte die Problembehebung per Fernwartung nicht möglich sein und wird ein Einsatz vor Ort erforderlich, werden Sie hierüber umgehend informiert. Die Terminvereinbarung erfolgt nach Absprache

mit der Einsatzleitung Technischen Service oder Servicetechniker.

(6) Die Laufzeit dieser Vereinbarung ist unbefristet und kann von beiden Parteien mit einer Frist von einem Monat zum Quartalsende gekündigt werden. Sie gilt jedenfalls so lange wie die Fernwartungsleistungen in Anspruch genommen werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Systemvoraussetzung für Onlinesupport

(1) Sie tragen eigenständig dafür Sorge, das folgende Systemvoraussetzungen und Rahmenbedingen dauerhaft sichergestellt sind. Dies umfasst:

- Installation von einem Remoteverbindungs-Client zur Wartung und/oder Problembehebung Ihrer Hardware und/oder Software
- Allgemeine Supportfähigkeit von Rechner, Betriebssystem und Gesamtkonfiguration (Firewall)
- Stabiler Internetzugang.

(2) Sollte eine Fernwartung aufgrund von Rahmenbedingungen, die nicht im Verantwortungsbereich von HSMED liegen, nicht möglich sein, kann HSMED nicht in Regresshaftung genommen werden, z.B. für durch einen Systemausfall entstandene Kosten.

(3) Bedienungs- oder Installationsprobleme, die aufgrund von nicht durch die HSMED beschaffter Hard- und Software auftreten, sowie Störungen bei Ferndatenverbindungen (z.B. Splashtop- oder allgemeine Internetverbindungsprobleme) oder der Internetzugänge (z.B. Router, etc.) sind nicht in diese Vereinbarung einbezogen und werden grundsätzlich nicht unterstützt.

3. Allgemeine Pflichten der HSMED

(1) HSMED verpflichtet sich, Fernwartung nur auf Ihre Weisung von hierzu autorisierten Mitarbeitern ordnungsgemäß durchführen zu lassen.

(2) HSMED ist bekannt, dass sie zur Verschwiegenheit über Betriebs- oder Geschäftsgeheimnis (§ 203 StGB), die HSMED im Rahmen der Fernwartung bekannt werden verpflichtet ist, und dass diese Verpflichtung auch nach Beendigung dieser Vereinbarung gilt. HSMED lässt Fernwartungsarbeiten nur von solchen Personen durchführen, die auf das Datengeheimnis sowie die Regelungen über zur Verschwiegenheit über Betriebs- oder Geschäftsgeheimnis (§ 203 StGB) verpflichtet sind.

4. Zweckbindung und Weitergabe an Dritte

(1) Personenbezogene Daten, die HSMED im Rahmen der Erfüllung dieser Vereinbarung bekannt werden, darf HSMED nur für Zwecke der Fernwartung verwenden.

(2) Eine Weitergabe dieser Daten an Dritte ist HSMED grundsätzlich untersagt. Ausgenommen hiervon ist die Weitergabe der Daten an den Hersteller bzw. Lieferanten in Verbindung mit notwendigen Supportleistungen inklusive Fernzugriff durch diese. Sie erteilen hierfür ausdrücklich Ihre Zustimmung. Sie haben die Möglichkeit dieser Weitergabe zu widersprechen. Bitte beachten Sie jedoch, dass dann die Fernwartung möglicherweise nicht erfolgreich durchgeführt werden kann. HSMED hat mit den Herstellern bzw. Lieferanten Vereinbarungen geschlossen, die den besonderen Voraussetzungen der Art. 44 ff. DSGVO (Übermittlung in ein Drittland) Rechnung trägt.

5. Technische und organisatorische Sicherheitsmaßnahmen

(1) Über den Einsatz von und die Verbindung zu uns über einen Remoteverbindungs-Client entscheiden ausschließlich Sie durch die Übermittlung Ihrer Remoteverbindungs-Einwahldaten und des seitens des Remoteverbindungs-Clients an uns, nachdem Sie diese Vereinbarung digital durch Klick angenommen haben. Nähere Informationen zu dem verwendeten Remoteverbindungs-Client, dessen Sicherheit und Umgang bezüglich Datenschutzes finden Sie im Internet unter https://www.splashtop.com/de/security

(2) Fernwartungsleistungen dürfen nur begonnen werden, wenn sich das Fernwartungspersonal mit Benutzerkennung und Passwort angemeldet hat.

(3) HSMED protokolliert die Fernwartungsaktivitäten einer Sitzung mit Datum, Uhrzeit und Benutzerkennung automatisch, überprüft die Protokolle und bewahrt sie dem Zweck entsprechend so lange wie nötig, mindestens jedoch ein Jahr lang auf. Im Bedarfsfall, z.B. wenn es sich um komplexe,

länger dauernde Vorgänge handelt, können ganze Sitzungen oder Teile einer Sitzung auch aufgezeichnet und entsprechend gespeichert werden.

(4) Sie räumen HSMED nur die Zugriffsrechte ein, die diese zur Durchführung der Fernwartungsleistung tatsächlich benötigt. Sie stellen sicher, dass HSMED nur insoweit auf gespeicherte personenbezogene Daten zugreifen kann, als dies zur Durchführung der Fernwartungsarbeiten unerlässlich notwendig ist. HSMED darf von den ihr eingeräumten Zugriffsrechten nur in dem für die Durchführung der Fernwartungsleistungen unerlässlich notwendigen Umfang Gebrauch machen.

(5) HSMED darf personenbezogene Daten im Wege eines Filetransfers oder Downloads für Zwecke der Fehleranalyse und -behebung nur dann von Ihren Systemen abziehen und auf ihr eigenes kopieren, wenn dies zur Durchführung der Fernwartungsarbeiten bzw. Problemanalyse unerlässlich notwendig ist. Dies erfolgt grundsätzlich nur lokal in Deutschland auf gesicherten Datenträger unserer Fernwartungsmitarbeiter und soweit nicht ein Fall von Ziffer 4 (2) (Weitergabe an Hersteller zwecks Analyse und Problemlösung) betroffen ist.

(6) **Anlage 1** zu dieser Vereinbarung legt die technischen und organisatorischen Maßnahmen ("TOM") fest, die HSMED zur Sicherung und zum Schutz der personenbezogenen Daten vor- und einhält. Auf schriftliche Anfrage wird HSMED die TOM Ihnen und gegebenenfalls der zuständigen Aufsichtsbehörde gegenüber nachweisen. Die TOM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist HSMED gestattet, alternative adäquate Maßnahmen umzusetzen, soweit dabei das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(7) Sie sind berechtigt, die Fernwartungsarbeiten von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.

(8) HSMED hat einen Datenschutzbeauftragten bestellt. Dieser ist per E-Mail unter: Datenschutzbeauftragter@henryschein.at erreichbar (weitere Kontaktdaten werden auf Anfrage mitgeteilt). Über etwaige Veränderungen werden wir Sie unverzüglich informieren. Dies gilt nicht als Vertragsänderung.

6. Berechnung

Für technische Fernwartungen / Supportleistungen besteht eine Kostenpflicht. Sie werden über die Kostenpflicht unmittelbar vor Beginn der Fernwartung / des Supports ausdrücklich von HSMED fernmündlich oder per Chat informiert. Die Berechnung der Remoteverbindungs-Zeiten geschieht auf eine Arbeitseinheit (AE) pro angefangene Viertelstunde zum aktuell gültigen Preis. Die Inrechnungstellung erfolgt gemäß den gültigen Geschäftsvereinbarungen per Rechnung oder Lastschriftverfahren.

7. Haftung

Für Schäden des Kunden haftet HSMED – gleich aus welchem Rechtsgrund – nur, sofern diese vorsätzlich oder grob fahrlässig verursacht wurden und die trotz ordnungsgemäßem Einsatz und ordnungsgemäßer Installation der Software entstehen. Diese Einschränkung gilt nicht für Schäden aus der Verletzung des Lebens, des Körpers und der Gesundheit oder sofern nach dem Produkthaftungsgesetz für Schäden zwingend gehaftet wird. (Sorgfalts- und Informationspflicht des Kunden beim Kooperieren mit dem Support bei geöffneter Maschine).

8. Sonstiges

(1) HSMED behält sich vor supportrelevanten Informationen über den Kunden systemisch in einer CRM Datenbank festzuhalten.

(2) HSMED und Sie verpflichten sich, alle Ihnen zur Verfügung gestellten Unterlagen ordnungsgemäß aufzubewahren. Sie tragen Sorge dafür, dass Dritte nicht ohne unsere Einwilligung Einsicht nehmen können. Im Falle von Anfragen Dritter oder einer Aufsichtsbehörde im Zusammenhang mit unserer Vereinbarung arbeiten wir einvernehmlich zusammen.

(3) Im Übrigen gelten die jeweils aktuellen AGB der HSMED, die unter https://henryscheinmed.at/p/agb abgerufen werden können. Weitere Informationen zum Datenschutz enthält unsere Datenschutzerklärung, die Sie unter: https://henryscheinmed.at/p/datenschutz abrufen können.

9. Salvatorische Klausel

Sollten eine der Bestimmungen dieser Vereinbarung unwirksam sein oder werden, so bleibt die Wirksamkeit der übrigen Bestimmungen davon unberührt. Die Parteien verpflichten sich, eine unwirksame oder undurchführbare Bestimmung von Beginn der Unwirksamkeit oder Undurchführbarkeit an, durch eine Übereinkunft zu ersetzen, die dem wirtschaftlichen Ergebnis der unwirksamen oder undurchführbaren Bestimmung am nächsten kommt. § 139 BGB findet keine Anwendung.

Henry Schein Medical Austria GmbH

Technisch-Organisatorische Maßnahmen (TOM) gemäß DSGVO

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

a. Zutrittskontrolle:
- -Manuelles Schließsystem, Sicherheitsschlösser, elektrische Türöffner, Autom. Zugangskontrollsystem, Magnet- oder Chipkarten-/Transponder-Schließsystem,
- -Videoüberwachung der Zugänge, Videoanlagen, Absicherung von Gebäudeschächten, Bewegungsmelder,
- -Personenkontrolle beim Empfang, Protokollierung der Besucher, Werkschutz, Pförtner,
- -Schlüsselregelung (Schlüsselausgabe etc.)
- -Sorgfältige Auswahl von Reinigungs- und Wachpersonal, Tragepflicht von Berechtigungsausweisen,

b. Zugangskontrolle:
- -Kennwörter, autom. Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- -Zuordnung von Benutzerrechten, Erstellen von Benutzerprofilen zu IT-Systemen
- -Passwortvergabe gemäß PW-Richtlinie (Länge / Wechsel), Authentifikation mit Benutzername/Passwort,
- -Gehäuseverriegelungen
- -Einsatz von Virtual Private Networks-Technologie
- -Einsatz von Intrusion-Detection-Systemen
- -Verschlüsselung von mobilen Datenträgern
- -Verschlüsselung von Smartphone-Inhalten
- -Zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- -Hard-/Software Firewalls, Anti-Viren-Software

c. Zugriffskontrolle:
- -Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, inkl. Festlegung von Datenbankrechten
- -Verwaltung der Rechte durch System-Admins
- -Anzahl der System-Admins auf Notwendigstes reduziert
- -Protokollierung von Zugriffen auf Anwendungen, insb. bei Eingabe, Änderung und Löschung von Daten
- -Sichere Aufbewahrung von Datenträgern
- -physische Löschung von Datenträgern vor Wiederverwendung
- -ordnungsgemäße Vernichtung von Datenträgern (DIN 32757); Einsatz von versierten Aktenvernichtern bzw. Dienstleistern; Protokollierung der Vernichtung

d. Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:
- -Mandantenfähigkeit und logische Mandantentrennung (softwareseitig)
- -Sandboxing; physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- -Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- -Versehen der Datensätze mit Zweckattributen / Datenfeldern; Trennung von Produktiv- und Testsystem
- -Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

e. Pseudonymisierung (Artt. 32 Abs. 1a, 25 Abs. 1 DSGVO): Soweit anwendbar und gesetzlich notwendig: Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung weiterer Informationen nicht mehr einer spezifischen Person zugeordnet werden können (wenn weitere Informationen gesondert aufbewahrt werden und entsprechenden TOM unterliegen.

2. Integrität (Art. 32 Abs. 1b DSGVO)

a. Weitergabekontrolle:
- -Einrichtungen von Standleitungen bzw. Virtual Private Networks-Tunneln
- -Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen

b. Eingabekontrolle:
- -Berechtigungskonzepte bzgl. und Protokollierung von Eingabe, Änderung und Löschung von Daten
- -Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- -Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- -Dokumentenmanagement, Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

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

a. Schutz zufälliger/m oder mutwilliger/m Zerstörung/Verlust:
- -Unterbrechungsfreie Stromversorgung
- -Meldewege, Notfallpläne, Temperatur-/Feuchtigkeitsüberwachung, Schutzsteckdosenleisten in Serverräumen
- -Feuer- und Rauchmeldeanlagen; automatische Löschanlage in Serverräumen, bzw. Feuerlöscher am äußeren Eingangsbereich von Serverräumen
- -Alarm bei unberechtigten Zutritten zu Serverräumen
- -Serverräume nicht unter sanitären Anlagen und über der Wassergrenze
- -Virenschutz, Firewall

b. Wiederherstellbarkeit (Art. 32 Abs. 1c DSGVO):
- -Backup-Strategie: Erstellen eines Backup- & Recoverykonzepts (online/offline; on-site/off-site)
- -Testen von Datenwiederherstellung
- -Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

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

a. Datenschutz-Management
b. Incident-Response-Management
c. Datenschutzfreundliche Voreinstellungen
d. Auftragskontrolle / Weisungsgebundenheit:
- -Auswahl des Verarbeiters oder Sub-Verarbeiters unter DSGVO-Sorgfaltsgesichtspunkten
- -Eindeutige Vertragsgestaltung, z.B. durch DSGVO konforme Auftragsverarbeitungsvereinbarung
- -Dokumentation der TOM sowie Kontrollrechte.
- -Verpflichtung der Mitarbeiter des Dienstleisters auf das Datengeheimnis
- -soweit gesetzlich verpflichtet hat Dienstleister Datenschutzbeauftragten bestellt
- -Überprüfung des Dienstleisters und seiner Tätigkeiten
- -Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags