80 YEARS: QUALITY
MADE IN GERMANY

Stand 12.02.2026

Vertragliche Regelungen und Vereinbarungen zur Auftragsverarbeitung (AVs)

gemäß Artikel 28 DSGVO

Vertrag zur Auftragsverarbeitung

- Rev. 01 -

Auftraggeber	Auftragnehmer
Nutzer der Anwendung DERManager 2.0	HEINE Optotechnik GmbH & Co. KG
	Dornierstr. 6
	82205 Gilching

Inhaltsverzeichnis

Hinweis bzgl. geschlechtsneutraler Formulierung
Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Im folgenden Text werden, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um Fachbegriffe, Definitionen, Zitate o. ä. handelt, werden im Text nicht durch Paarformeln ersetzt. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren. Wenn aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wird, impliziert dies ebenfalls keine Benachteiligung der anderen Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

1 Allgemeines

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung i. S. d. Artikel 28 EU-Datenschutzgrundverordnung (DSGVO) und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i. S. d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

Zur Sicherstellung der geeigneten Garantien nach den Artikeln 44 ff DSGVO werden die im 0 befindlichen SCC Bestandteil dieses Vertrages. Die Angaben des Annex I der SCC entsprechen den Klauseln in diesem Vertrag.

2 Gegenstand der Vereinbarung

Das digitale Verwaltungssystem HEINE DERManager 2.0 wird als „Cloud-Service“ angeboten.

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen (Zutreffendes bitte auswählen):

☐ Um überprüfen zu können, ob der im bisherigen System des Kunden vorhandene Datenbestand mit dem System des DERManagers 2.0 kompatibel ist, stellt der Auftraggeber dem Auftragsverarbeiter vorab seinen Datensatz für eine **Testmigration** zur Verfügung. Erst wenn eine Kompatibilität mit den Systemen positiv festgestellt wurde, schließt der Auftraggeber einen entsprechenden Vertrag mit HEINE über die Nutzung des DERManagers 2.0 ab. Dieser umfasst sodann die entgeltliche Überlassung zur zeitlich unbegrenzten, nicht ausschließlichen Nutzung der Software HEINE DERManager 2.0, die Pflegeleistungen für die Software sowie die Schulungen und die Unterstützungsleistungen bei der Anpassung der Software an die speziellen Anforderungen des Auftraggebers.

Der Auftragnehmer erbringt folglich folgende Auftragsverarbeitungen:

Die Übertragung der personenbezogenen Daten des Auftraggebers von einem externen Datenträger (z. B. externe Festplatte) auf den DERManager 2.0, um prüfen zu können, ob eine Übertragbarkeit vorhanden ist.

☒ Der Auftragnehmer bietet die Dienstleistung DERManager 2.0 im Rahmen eines **Abonnements** an. Dabei werden die Daten des Auftraggebers im Rahmen der Behandlungsdokumentation (Erfassung und Übertragung der personenbezogenen Daten durch den Auftraggeber per DERManager 2.0 App, Browser oder kompatiblen digitalen Dermatoskopen) auf einem Cloud-Server des Auftragnehmers gespeichert. Der Auftraggeber hat die Möglichkeit eine Nutzerverwaltung durchzuführen und Zugriffe auf seine in der Cloud gespeicherten Daten zu ermöglichen.

Der Auftragnehmer erbringt folglich folgende Auftragsverarbeitungen:

HEINE führt für den Auftraggeber die Übertragung der personenbezogenen Daten an den Cloud-Server und die Speicherung der personenbezogenen Daten für den Auftraggeber auf dem Cloud-Server durch, um diesem die Daten vorzuhalten und abrufbar zu machen. Des Weiteren erbringt HEINE für seine Kunden Supportdienstleistungen per E-Mail, Telefonkontakt oder Remote-Software (z. B. TeamViewer) im Zusammenhang mit dem DERManager 2.0, um Problemanalysen und Fehlerbehebungen durchführen zu können.

2.2 Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

Die Auftragsverarbeitung betrifft folgende Kategorien von Daten:

- Personenstammdaten (Vorname, Nachname, Adressangaben, Kontaktdaten, Benutzercodes und-namen, Berechtigungen)
- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Anwenderbezogene Änderungsprotokolle
- Patientendaten (Gesundheitsdaten und Patientenhistorie)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Vertragsabrechnungs- und Zahlungsdaten
- Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Protokolldaten (IP-Adresse, Browserkennung, Browserversion)
- Biometrische Daten zur Entsperrung der App

2.3 Kreis der von der Datenverarbeitung betroffenen Personen:

- Geschäftspartner
- Mitarbeiter des Auftraggebers
- Patienten
- Ansprechpartner

3 Rechte und Pflichten des Auftraggebers

3.1 Der Auftraggeber ist Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Auftraggeber. Dem Auftragnehmer steht nach Ziff. 4 Abs. 6 das Recht zu, den Auftraggeber auf seiner Meinung nach rechtlich unzulässige Datenverarbeitungen hinzuweisen.

3.2 Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber

informieren, wenn betroffene Personen ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen. Der Auftragnehmer wird etwaige Anfragen betroffener Personen unverzüglich an den Verantwortlichen weiterleiten. Der Auftragnehmer bearbeitet keine Anfragen betroffener Personen ohne Weisung des Auftraggebers.

3.3 Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber wird das Ergebnis in geeigneter Weise dokumentieren.

3.4 Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können

- schriftlich
- per E-Mail
- per Telefon

erfolgen. Der Auftraggeber soll mündliche Weisungen, sofern diese in diesem Vertrag für Weisungen zulässig sind, unverzüglich in Textform (z. B. per E-Mail) gegenüber dem Auftragnehmer bestätigen.

3.5 Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

3.6 Der Auftraggeber kann weisungsberechtigte Personen benennen. Weisungsberechtigte Personen des Auftraggebers sind zeitnah dem Auftragnehmer zu übermitteln.

3.7 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

3.8 Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4 Rechte und Pflichten des Auftragnehmers

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

4.2 Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.

4.3 Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Die Pflicht zur Bestätigung kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

4.4 Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

4.5 Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

4.6 Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der

betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

4.7 Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigte Personen erfolgt ist, unverzüglich mitzuteilen. Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

4.8 Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete

- besondere Arten personenbezogener Daten (Art. 9 DSGVO) oder
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen (auch i. S. v. Art. 10 DSGVO) oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.
Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei entsprechenden Meldepflichten unterstützen.

4.9 Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, auf geeignete Weise von Daten anderer Auftraggeber trennen.

4.10 An der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten durch den Auftraggeber hat der Auftragnehmer mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

4.11 Der Auftragnehmer soll dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Weisungsempfangsberechtigte Person des Auftragnehmers ist:

Product Owner Digital Dermatoscopy

4.12 Hat eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Auftraggeber eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. Der Auftragnehmer hat bei der Durchführung mitzuwirken und dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

4.13 Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. **35** DSGVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. **36** DSGVO zu unterstützen.

5 Kontrollbefugnisse

5.1 Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

5.2 Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i. S. d. Absatzes 1 erforderlich ist.

5.3 Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

5.4 Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

5.5 Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i. S. d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten, die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

6 Unterauftragsverhältnisse

6.1 Die Beauftragung von Subunternehmern durch den Auftragnehmer ist gestattet. Der Auftragnehmer hat den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter zu informieren, wobei die Subunternehmer konkret und vollständig mitzuteilen sind. Der Auftraggeber hat das Recht innerhalb einer Frist von 14 Tagen ab der Information durch den Auftragnehmer Einspruch aus sachlichem Grund gegen die beabsichtigte Beauftragung zu erheben. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der „Fehler! Verweisquelle konnte nicht gefunden werden.“ zu diesem Vertrag angeben.

6.2 Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i. S. d. Art. 37 DSGVO bestellt hat, es sei denn, dieser ist nicht bestellpflichtig.

6.3 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzenden Weisungen des Auftraggebers auch gegenüber den Subunternehmern gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

6.4 Der Auftragnehmer hat mit dem Subunternehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

6.5 Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 5 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

6.6 Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass bei dem jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gemäß den Artikeln 44 ff. DSGVO gewährleistet ist. Dies kann insbesondere in Ländern außerhalb des EWR-Raumes und ohne Vorhandensein eines Angemessenheitsbeschlusses der EU-Kommission, durch den Abschluss einer Vereinbarung auf Basis der EU-Standardvertragsklauseln, vorhandenen Binding Corporate Rules oder eines Code of Conduct erfolgen. Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

6.7 Nicht als Unterauftragsverhältnisse i. S. d. Absätze 1 bis 5 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Wartungs- und Prüfungsleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit die Wartung und

Prüfung solche IT-Systeme betreffen, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden. Die Parteien sind sich darüber einig, dass vorgenannte Wartungs- und Prüfleistungen eine „Auftragsverarbeitung“ i. S. d. Art. 28 DSGVO darstellen.

7 Datenschutzbeauftragter des Auftragnehmers

Beim Auftragnehmer ist als fachkundiger Datenschutzbeauftragter benannt:

Herr Sven Lenz
Deutsche Datenschutzkanzlei – Datenschutzkanzlei Lenz GmbH & Co. KG
Bahnhofstraße 50
87435 Kempten
Deutschland

E-Mail: **dsb@heine.com**
Web: www.deutsche-datenschutzkanzlei.de

Der Fachkundenachweis über die Qualifikation des Datenschutzbeauftragten liegt diesem Vertrag bei.
Ein Wechsel des Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen. Auf Anfrage des Verantwortlichen ist der aktuelle Fachkundenachweis zur Verfügung zu stellen.

8 Vertraulichkeitsverpflichtung

8.1 Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

8.2 Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen

des Datenschutzes vertraut macht und diese auf die Wahrung der Vertraulichkeit verpflichtet.

8.3 Dem Auftragnehmer ist bewusst, dass der Auftraggeber als Arzt/Ärztin einer besonderen Schweigepflicht nach § 203 Strafgesetzbuch unterliegt. Der Auftragnehmer wird daher alle Beschäftigten, die Leistungen im Zusammenhang mit dem Auftrag des Auftraggebers erbringen, in schriftlicher Form verpflichten, alle Daten des Auftraggebers, insbesondere die für den Auftraggeber verarbeiteten personenbezogenen Daten vertraulich zu behandeln, sowie die bei der Durchführung der Arbeiten mit den besonderen personenbezogenen Daten (Art. 9 DSGVO) beschäftigten Mitarbeiter einer gesonderten Schweigepflicht nach § 203 Strafgesetzbuch zu unterwerfen. Diese Verpflichtung der Beschäftigten ist auf Anfrage dem Auftraggeber nachzuweisen.

9 Wahrung von Betroffenenrechten

9.1 Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

9.2 Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

9.3 Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit der Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

10 Geheimhaltungspflichten

10.1 Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Informationen Dritten zugänglich zu machen.

10.2 Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

11 Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

12 Technische und organisatorische Maßnahmen zur Datensicherheit

12.1 Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als „**0**“ zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Vorwege mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

12.2 Der Auftragnehmer wird die von ihm getroffenen technische und organisatorische Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

Der Auftragnehmer wird dem Auftraggeber die von ihm nach Art. 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung des nach Art. 32 DSGVO und des in diesem Vertrag geregelten Schutzniveaus in dokumentierter Form und in geeigneter Weise zur Verfügung stellen. Sofern die

Parteien nicht gesondert vereinbaren, dass die in der „**0**“ aufgeführten technischen und organisatorischen Maßnahmen durch die nach diesem Absatz neu zur Verfügung gestellte Dokumentation der technischen und organisatorischen Maßnahmen zur Datensicherheit ersetzt werden, bleiben die in „**0**“ genannten Maßnahmen Vertragsbestandteil und sind vom Auftragnehmer entsprechend zu erfüllen.

Ergänzend zu den in der „**0**“ aufgeführten technischen und organisatorischen Maßnahmen ergreift der Auftragnehmer zur Gewährleistung der besonders schutzbedürftigen Patientendaten des Auftraggebers im Rahmen des HEINE DERManagers 2.0 die folgenden technischen und organisatorischen Maßnahmen:

- Erstellen von Benutzerprofilen mit eingeschränkten Benutzerrechten für die eingesetzten IT-Systeme
- Authentifikation mit Benutzername und Passwort oder (bevorzugt) mit kryptographischem Schlüssel
- Verschlüsselung jeglicher Verbindungen mit den IT-Systemen
- Verzicht auf mobile Datenträger
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Absicherung von Verbindungen via Firewalls
- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Starke Mandantentrennung durch separate virtuelle Maschinen mit separater Datenbank

- Trennung von Produktiv- und Testsystem
- Eine Pseudonymisierung durch den Auftraggeber findet nicht statt. Die konkrete Zuordnung der Patientendaten ist für die Funktion der Software unerlässlich.
- Alle Verbindungen zu den IT-Systemen sind verschlüsselt (Transportverschlüsselung). Ruhende Daten, wie z.B. Sicherungskopien, werden nicht standardmäßig verschlüsselt.
- Über die Verschlüsselung als Möglichkeit zum Schutz der personenbezogenen Daten entscheidet der Auftraggeber. Entscheidet sich der Auftraggeber für die Möglichkeit der Datenverschlüsselung, kann der Auftragnehmer anbieten, den Schlüssel zur ggf. Wiederherstellung der Daten ebenfalls aufzubewahren. Sollte dies nicht der Fall sein und der Auftragnehmer den Schlüssel verlieren, so sind alle damit verschlüsselten Daten unwiederbringlich verloren.
- die Übertragung der Daten vom System zum Anwender wird durch die Zugangsregeln der Software eingeschränkt
- die Übertragung findet verschlüsselt statt
- bei der Übertragung kommen Algorithmen zur Fehlerkorrektur zum Einsatz
- die Anmeldung am System wird protokolliert
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzer-namen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Verpflichtung der Mitarbeiter des Auftragnehmers auf die Wahrung der Vertraulichkeit
- Auftragnehmer hat Datenschutzbeauftragten bestellt

- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

13 Dauer des Auftrages

13.1 Der Vertrag beginnt mit der Bestellung der Arbeiten und/oder der Leistungen gemäß Ziffer 0 und wird auf unbestimmte Zeit geschlossen. Die Laufzeit des Vertrags ist an die Laufzeit des Abonnements gekoppelt.

13.2 Der Vertrag ist jederzeit zum Ende des laufenden Abonnements kündbar. Die Laufzeit eines Abonnements beträgt 1 Monat. Der Vertrag verlängert sich jeweils um einen weiteren Monat, wenn keine Kündigung erfolgt.

13.3 Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

14 Beendigung

14.1 Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen; die Löschung erfolgt innerhalb einer Übergangsfrist von einem Monat. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.

14.2 Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

15 Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

16 Schlussbestimmungen

16.1 Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

16.2 Für Nebenabreden ist die Schriftform erforderlich.

16.3 Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

17 Anlagen

Anlage 1 Unterauftragnehmer

1. Datenzentrum
SaSG GmbH & Co. KG
Kapplweg 12
D - 86511 Schmiechen

Tel.: +49 (0) 82 06 - 5 27 90 – 0
E-Mail: **info@sasg.de**
Web: www.sasg.de

Handelsregister (HRA) 18415

Persönlich haftender Gesellschafter:
SaSG Verwaltungsgesellschaft mbH Handelsregister (HRB) 29326

Vertretungsberechtigter Geschäftsführer: Peter Heidenreich

2. Modul Trichoscan
Datinf GmbH
Wilhelmstr. 42
72074 Tübingen

Geschäftsführer: Dr. Ulf Ellwanger, Dr. Holger Lüdtke

Fon: 07071-253696-6
Email: **info@datinf.de**
Web: **http://www.datinf.de**

Handelregister: Stuttgart HRB 382401
USt.-Identnummer: DE225543033

3. Remote Support

TeamViewer Germany GmbH
Bahnhofsplatz 2
73033 Göppingen
Deutschland

Geschäftsführer: Oliver Steil, Michael Wilkens, Peter Turner, Mei Dent

Telefon: +49 7161 60692 50
E-Mail: contact@teamviewer.com

Handelsregister: Ulm HRB 534075
USt.-Identnummer: DE245838579

Anlage 2 Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3 Technische und organisatorische Maßnahmen SaSG

Anlage 4 SCC