HEINE Optotechnik GmbH & Co. KG, Dornierstr. 6, 82205 Gilching, Germany
Tel. +49 (0) 81 05 / 77 28 - 0, Fax +49 (0) 81 05 / 77 28 - 202, E-Mail: info@heine.com, **www.heine.com**

Contractual regulations and agreements on order processing (AVs)

in accordance with Article 28 GDPR

Contract for order processing
- Rev. 01 -

Client	Contractor
Users of the DERManager application	HEINE Optotechnik GmbH & Co KG Dornierstr. 6 82205 Gilching

Table of contents

1 General information 3
2 Object of the agreement 3
3 Rights and obligations of the client 4
4 Rights and obligations of the contractor 4
5 Control authorisations 5
6 Subcontracting relationships 5
7 Data protection officer of the contractor 6
8 Confidentiality obligation 7
9 Safeguarding the rights of data subjects 7
10 Confidentiality obligations 7
11 Remuneration 7
12 Technical and organisational measures for data security 7
13 Duration of the order 8
14 Termination 8
15 Right of retention 9
16 Final provisions 9
17 Attachments 9
Attachment 1 Subcontractor 9
Appendix 2 Technical and organisational measures of the contractor 9
Appendix 3 Technical and organisational SaSG 9
Appendix 4 SCC 9

Note regarding gender-neutral wording
A gender-equal society requires gender-neutral language. In the following text, appropriate formulations are used where possible and appropriate (e.g. pair formulae, derivations). Personal designations that are technical terms, definitions, quotations or similar are not replaced by pair formulae in the text. Corresponding terms are to be interpreted in a gender-neutral manner in the interests of equal treatment. If, for reasons of easier readability, only one gender is shown for personal nouns and pronouns, this also does not imply any discrimination against the other genders, but should be understood as gender-neutral in the sense of linguistic simplification.

1 General information

1.1 The Contractor processes personal data on behalf of the Client. This contract contains the written order for commissioned processing within the meaning of Article 28 of the EU General Data Protection Regulation (GDPR) and regulates the rights and obligations of the parties in connection with data processing.

1.2 Insofar as the term "data processing" or "processing" (of data) is used in this contract, the definition of "processing" within the meaning of Art. 4 No. 2 GDPR shall apply.

1.3 In order to ensure the appropriate guarantees in accordance with Article 44 et seq. of the GDPR, the SCC contained inAnnex 4 shall become an integral part of this contract. The information in Annex I of the SCC corresponds to the clauses in this contract.

2 Object of the agreement

2.1 The digital management system HEINE DERManager is offered as a "Cloud Service".

The Client's order to the Contractor includes the following work and/or services (please select as appropriate):

☐ In order to be able to check whether the data available in the client's previous system is compatible with the DERManager system, the client shall make its data set available to the processor in advance for a **test migration**. Only when compatibility with the systems has been positively established shall the client conclude a corresponding contract with HEINE for the use of DERManager. This then includes the transfer for an unlimited period of time for the non-exclusive use of the HEINE DERManager software, the maintenance services for the software as well as the training and support services for the customisation of the software to the special requirements of the client.

The contractor therefore performs the following order processing services:

The transfer of the client's personal data from an external data carrier (e.g. external hard drive) to the DERManager in order to be able to check whether portability exists.

☒ The Contractor offers the DERManager service as part of a subscription. The client's data is stored on the contractor's cloud server as part of the treatment documentation.

The contractor therefore performs the following order processing services:

HEINE stores the personal data for the customer on the cloud server in order to make the data available and accessible to the customer. Furthermore, HEINE provides support services for its customers by email, telephone contact or remote software (e.g. TeamViewer) in connection with DERManager in order to be able to carry out problem analyses and troubleshooting.

☒ The client uses the HEINE DERManager on a local device. A DERManager app is stored on the client's mobile device. Within this app, the user has the option of forwarding the images taken with a HEINE dermatoscope to the DERManager system.

The contractor therefore performs the following order processing services:

Transfer of the personal data to be stored from and to the DERManager system.

2.2 The following types of data are regularly processed:

The order processing concerns the following categories of data:

- Personal master data (first name, surname, address details, contact details, user codes and names, authorisations)
- Communication data (e.g. telephone, e-mail)
- User-related change logs
- Patient data (health data and patient history)
- Contract master data (contractual relationship, product or contractual interest)
- Contract billing and payment data
- Information (from third parties, e.g. credit agencies, or from public directories)
- Protocol data (IP address, browser identification, browser version)

2.3 Group of persons affected by the data processing:

- Business partner
- Employees of the client
- Patients
- Contact person

3 Rights and obligations of the client

3.1 The client is the controller within the meaning of Art. 4 No. 7 GDPR for the processing of data on behalf of the contractor. The assessment of the permissibility of the data processing is the sole responsibility of the Client. Pursuant to Section 4 (6), the Contractor has the right to inform the Client of any data processing that it considers to be legally unauthorised.

3.2 As the controller, the client is responsible for safeguarding the rights of data subjects. The Contractor shall inform the Client immediately if data subjects assert their data subject rights against the Contractor. The Contractor shall forward any enquiries from data subjects to the controller without delay. The Contractor shall not process any requests from data subjects without instructions from the Client.

3.3 The Client shall satisfy itself of compliance with the technical and organisational data security measures taken by the Contractor before the start of data processing and thereafter on a regular basis. The Client shall document the result in a suitable manner.

3.4 The client has the right to issue additional instructions to the contractor at any time regarding the type, scope and procedure of data processing. Instructions can

- In writing
- by e-mail
- by telephone

take place. The Client shall immediately confirm verbal instructions to the Contractor in text form (e.g. by e-mail), insofar as these are permitted for instructions in this contract.

3.5 This shall be without prejudice to any provisions regarding compensation for additional expenses incurred by the Contractor as a result of supplementary instructions issued by the Client.

3.6 The client may nominate persons authorised to issue instructions. Persons authorised by the client to issue instructions must be communicated to the contractor in a timely manner.

In the event that the persons authorised to issue instructions at the Client change, the Client shall inform the Contractor of this in writing or in text form.

3.7 The Client shall inform the Contractor immediately if it discovers errors or irregularities in connection with the processing of personal data by the Contractor.

3.8 In the event that there is an obligation to provide information to third parties in accordance with Art. 33, 34 GDPR, the client is responsible for compliance with this obligation.

4 Rights and obligations of the contractor

4.1 The Contractor shall process personal data exclusively within the scope of the agreements made and/or in compliance with any supplementary instructions issued by the Client. The purpose, type and scope of data processing shall be governed exclusively by this contract and/or the instructions of the client. The Contractor is prohibited from processing data in any other way unless the Client has consented to this in writing. The Contractor undertakes to carry out data processing on behalf of the Client only in member states of the European Union (EU) or the European Economic Area (EEA).

4.2 Documents containing personal data and files that are no longer required may only be destroyed in accordance with data protection regulations with the prior consent of the client.

4.3 The Contractor confirms that it has appointed a company data protection officer in accordance with Art. 37 GDPR. The obligation to confirm may be waived at the discretion of the Client if the Contractor can prove that it is not legally obliged to appoint a data protection officer and the Contractor can prove that operational regulations exist that ensure the processing of personal data in compliance with the statutory provisions, the provisions of this contract and any further instructions of the Client.

4.4 In the area of processing personal data in accordance with the order, the contractor guarantees that all agreed measures will be carried out in accordance with the contract.

4.5 The Contractor is obliged to organise its company and its operating procedures in such a way that the data it processes on behalf of the Client is secured to the extent necessary and protected against unauthorised access by third parties. The Contractor shall coordinate any changes in the organisation of data processing on behalf of the Client that are significant for the security of the data with the Client in advance.

4.6 The Contractor shall inform the Client immediately if, in its opinion, an instruction issued by the Client violates statutory regulations. The Contractor shall be entitled to suspend the implementation of the instruction in question until it is confirmed or amended by the Client.

4.7 The Contractor is obliged to notify the Client immediately of any breach of data protection regulations or of the contractual agreements made and/or the instructions issued by the Client that has

occurred in the course of the processing of data by the Contractor or other persons involved in the processing. Furthermore, the Contractor shall inform the Client immediately if a supervisory authority takes action against the Contractor in accordance with Art. 58 GDPR and this may also concern a control of the processing that the Contractor performs on behalf of the Client.

4.8 In the event that the Contractor establishes or facts justify the assumption that the goods processed by it for the Client are

- special categories of personal data (Art. 9 GDPR) or
- personal data that is subject to professional secrecy or
- personal data relating to criminal offences or administrative offences or the suspicion of criminal offences or administrative offences (also within the meaning of Art. 10 GDPR) or
- personal data relating to bank or credit card accounts

If the Contractor has unlawfully transmitted or otherwise unlawfully come to the knowledge of third parties, the Contractor must immediately and fully inform the Client of the time, type and scope of the incident(s) in writing or text form (fax/e-mail). The information must contain a description of the nature of the unlawful acquisition of knowledge. The information shall also include a description of the possible detrimental consequences of the unlawful acquisition of knowledge. The Contractor is also obliged to inform the Client immediately of the measures taken by the Contractor to prevent the unlawful transmission or unauthorised access by third parties in the future.

The Contractor is aware that the Client may be subject to a reporting obligation pursuant to Art. 33 GDPR, which provides for notification to the supervisory authority within 72 hours of becoming aware of it. The Contractor shall support the Client with the corresponding reporting obligations.

4.9 The contractor shall separate the data that it processes on behalf of the client from the data of other clients in an appropriate manner.

4.10 The Contractor shall co-operate in the preparation of the list of processing activities by the Client. He must provide the client with the necessary information in an appropriate manner.

4.11 The Contractor shall name to the Client the person(s) authorised to receive instructions from the Client. The person authorised to receive instructions is the Contractor:

Product Owner Digital Dermtoscopy

4.12 If a form of processing is likely to result in a high risk to the rights and freedoms of natural persons, the client must carry out an assessment of the consequences of the intended processing operations for the protection of personal data. The contractor shall co-operate in the implementation and provide the client with the necessary information in an appropriate manner.

4.13 The contractor is obliged to support the client in the preparation of a data protection impact assessment in accordance with Art. 35 GDPR and any prior consultation with the supervisory authority in accordance with Art. 36 GDPR.

5 Control authorisations

5.1 The Client shall have the right to monitor compliance with the statutory provisions on data protection and/or compliance with the contractual provisions agreed between the parties and/or compliance with the Client's instructions by the Contractor at any time to the extent necessary.

5.2 The Contractor shall be obliged to provide the Client with information insofar as this is necessary to carry out the inspection within the meaning of paragraph 1.

5.3 The Client may request to inspect the data processed by the Contractor for the Client as well as the data processing systems and programmes used.

5.4 The Client may carry out the inspection within the meaning of paragraph 1 at the Contractor's business premises during normal business hours after prior notification with reasonable notice. The Client shall ensure that the inspections are only carried out to the extent necessary to ensure that the Contractor's business operations are not disproportionately disrupted by the inspections.

5.5 The Contractor is obliged to provide the Client with the necessary information in the event of measures taken by the supervisory authority against the Client within the meaning of Art. 58 GDPR, in particular with regard to information and control obligations, and to enable the respective competent supervisory authority to carry out an on-site inspection. The Client shall be informed by the Contractor of any corresponding planned measures.

6 Subcontracting relationships

6.1 The commissioning of subcontractors by the Contractor is permitted. The Contractor must always inform the Client of any intended change with regard to the involvement or replacement of other processors, whereby the subcontractors must be notified specifically and in full. The Client shall have the right to object to the intended assignment on objective grounds within a period of 14

days from the date of notification by the Contractor. The Contractor shall specify all subcontracting relationships already existing at the time of conclusion of the contract in the "**Annex 1** " to this contract.

6.2 The Contractor must select the subcontractor carefully and check before commissioning that the subcontractor can comply with the agreements made between the Client and the Contractor. In particular, the Contractor must check in advance and regularly during the term of the contract that the subcontractor has taken the technical and organisational measures required under Art. 32 GDPR to protect personal data. The result of the inspection must be documented by the Contractor and forwarded to the Client upon request. The contractor is obliged to obtain confirmation from the subcontractor that the subcontractor has appointed a company data protection officer within the meaning of Art. 37 GDPR, unless this is not required to be appointed.

6.3 The Contractor must ensure that the regulations agreed in this contract and any supplementary instructions from the Client also apply to the subcontractors. The Contractor shall regularly monitor compliance with these obligations.

6.4 The Contractor shall conclude an order processing contract with the subcontractor that fulfils the requirements of Art. 28 GDPR. The client shall be provided with a copy of the order processing contract upon request.

6.5 In particular, the Contractor is obliged to ensure through contractual provisions that the control authorisations (Section 5 of this contract) of the Client and supervisory authorities also apply to the subcontractor and that corresponding control rights of the Client and supervisory authorities are agreed. It must also be contractually stipulated that the subcontractor must tolerate these control measures and any on-site inspections.

6.6 If subcontractors in a third country are to be involved, the contractor must ensure that the respective subcontractor guarantees an adequate level of data protection in accordance with Articles 44 et seq. GDPR is guaranteed.

This can be done in particular in countries outside the EEA and without the existence of an adequacy decision by the EU Commission, by concluding an agreement based on the EU standard contractual clauses, existing Binding Corporate Rules or a Code of Conduct.

Upon request, the Contractor shall provide the Client with evidence of the conclusion of the aforementioned agreements with its subcontractors.

6.7 Services that the contractor utilises from third parties as a purely ancillary service in order to carry out the business activity are not to be regarded as subcontracting relationships within the meaning of paragraphs 1 to 5. These include, for example, cleaning services, pure telecommunication services with no specific connection to services provided by the contractor for the client, postal and courier services, transport services and security services. The contractor is nevertheless obliged to ensure that appropriate precautions and technical and organisational measures have been taken to guarantee the protection of personal data, even in the case of ancillary services provided by third parties. Maintenance and testing services constitute subcontracting relationships requiring consent, insofar as the maintenance and testing relate to IT systems that are also used in connection with the provision of services for the client. The parties agree that the aforementioned maintenance and testing services constitute "commissioned processing" within the meaning of Art. 28 GDPR.

7 Data protection officer of the contractor

The Contractor has appointed an expert data protection officer:

Mr Sven Lenz
Deutsche Datenschutzkanzlei - Datenschutzkanzlei Lenz GmbH & Co. KG
Bahnhofstrasse 50
87435 Kempten
Germany

Email: dsb@heine.com
Web: www.deutsche-datenschutzkanzlei.de

The certificate of qualification of the data protection officer is enclosed with this contract.
The controller must be informed immediately of any change of data protection officer. The current certificate of competence must be made available at the request of the controller.

8 Confidentiality obligation

8.1 When processing data for the Client, the Contractor is obliged to maintain the confidentiality of data that it receives or becomes aware of in connection with the order. The Contractor undertakes to observe the same confidentiality rules as those incumbent on the Client. The Client is obliged to inform the Contractor of any special confidentiality rules.

8.2 The Contractor warrants that it is aware of the applicable data protection regulations and that it is familiar with their application. The Contractor further warrants that it will familiarise the employees engaged in the performance of the work with the data protection provisions applicable to them and that it will oblige them to maintain confidentiality.

8.3 The Contractor is aware that the Client, as a doctor, is subject to a special duty of confidentiality pursuant to Section 203 of the German Criminal Code. The Contractor shall therefore obligate all employees who provide services in connection with the Client's order in writing to treat all data of the Client, in particular the personal data processed for the Client, confidentially and to subject the employees employed in the performance of the work with the special personal data (Art. 9 GDPR) to a separate duty of confidentiality in accordance with Section 203 of the German Criminal Code. This obligation of the employees must be proven to the client upon request.

9 Safeguarding the rights of data subjects

9.1 The client is solely responsible for safeguarding the rights of the data subject.

9.2 Insofar as the cooperation of the Contractor is necessary for the protection of data subject rights - in particular to information, correction, blocking or deletion - by the Client, the Contractor shall take the necessary measures in each case in accordance with the Client's instructions.

9.3 This shall be without prejudice to provisions on any compensation for additional expenses incurred by the Contractor as a result of cooperation services in connection with the assertion of data subject rights vis-à-vis the Client.

10 Confidentiality obligations

10.1 Both parties undertake to treat all information that they receive in connection with the execution of this contract as confidential for an unlimited period of time and to use it only for the execution of the contract. Neither party is authorised to use this information in whole or in part for purposes other than those just mentioned or to make this information accessible to third parties.

10.2 The above obligation shall not apply to information which one of the parties has demonstrably received from third parties without being obliged to maintain confidentiality or which is publicly known.

11 Remuneration

The remuneration of the contractor shall be agreed separately.

12 Technical and organisational measures for data security

12.1 The Contractor undertakes to the Client to comply with the technical and organisational measures required to comply with the applicable data protection regulations.

The status of the technical and organisational measures in place at the time the contract is concluded is attached to this contract as "**Annex 2** ". The parties agree that changes to the technical and organisational measures may become necessary in order to adapt to technical and legal circumstances. The Contractor shall coordinate any significant changes that may affect the integrity, confidentiality or availability of the personal data with the Client in advance. Measures that only entail minor technical or organisational changes and do not negatively affect the integrity, confidentiality and availability of the personal data can be implemented by the Contractor without consultation with the Client. The Client may request an up-to-date version of the technical and organisational measures taken by the Contractor at any time.

12.2 The Contractor shall check the effectiveness of the technical and organisational measures it has taken on a regular basis and also on an ad hoc basis. In the event that there is a need for optimisation and/or changes, the Contractor shall inform the Client.

The Contractor shall provide the Client with the technical and organisational measures taken by it in accordance with Art. 32 GDPR to ensure the level of protection in accordance with Art. 32 GDPR and the level of protection regulated in this contract in a documented form and in a suitable manner. Unless the parties separately agree that the technical and organisational measures listed in "**Annex 2** " are replaced by the new documentation of the technical and organisational

measures for data security provided in accordance with this paragraph, the measures specified in "**Annex 2** " shall remain part of the contract and must be fulfilled accordingly by the Contractor.

In addition to the technical and organisational measures listed in the "**Annex 2** ", the Contractor shall take the following technical and organisational measures to ensure the Client's particularly sensitive patient data within the framework of the HEINE DERManager:

- Creating user profiles with restricted user rights for the IT systems used
- Authentication with username and password or (preferably) with cryptographic key
- Encryption of all connections with the IT systems
- Dispensing with mobile data carriers
- Encryption of data carriers in laptops / notebooks
- Securing connections via firewalls
- Creation of an authorisation concept
- Management of rights by system administrators
- Number of administrators reduced to the "bare minimum"
- Password policy
- Logging of access to applications, in particular when entering, changing and deleting data
- Strong client separation through separate virtual machines with separate database
- Separation of production and test system
- Pseudonymisation by the client does not take place. The specific allocation of patient data is essential for the function of the software.
- All connections to the IT systems are encrypted (transport encryption). Data at rest, such as backup copies, are not encrypted by default.
- The client decides on encryption as an option for protecting personal data. If the client decides in favour of the option of data encryption, the contractor can also offer to keep the key in order to restore the data if necessary. If this is not the case and the contractor loses the key, all data encrypted with it will be irretrievably lost.
- the transfer of data from the system to the user is restricted by the software's access rules
- the transmission is encrypted
- Error correction algorithms are used during transmission
- logging on to the system is logged
- Traceability of data entry, modification and deletion through individual user names (not user groups)
- Assignment of rights to enter, change and delete data on the basis of an authorisation concept
- Selection of the contractor under due diligence aspects (in particular with regard to data security)
- Obligation of the Contractor's employees to maintain confidentiality
- Contractor has appointed a data protection officer
- Ongoing review of the contractor and its activities

13 Duration of the order

13.1 The contract begins with the ordering of the work and/or services in accordance with section 2.1 and is concluded for an indefinite period. The term of the contract is linked to the term of the subscription.

13.2 The contract can be cancelled at any time at the end of the current subscription. The term of a subscription is 1 month. The contract is extended by a further month if it is not cancelled.

13.3 The Client may terminate the contract at any time without notice if there is a serious breach by the Contractor of the applicable data protection regulations or of obligations under this contract, if the Contractor is unable or unwilling to carry out an instruction of the Client or if the Contractor refuses access by the Client or the competent supervisory authority in breach of the contract.

14 Termination

14.1 After termination of the contract, the Contractor shall hand over to the Client all documents, data and processing or utilisation results that have come into its possession in connection with the contractual relationship. The Contractor's data carriers shall then be physically deleted; deletion shall take place within a transitional period of one month. This also applies to any data backups at the contractor. The deletion must be documented in a suitable manner. Test and scrap material must be destroyed or physically deleted immediately.

14.2 The client has the right to check that the data has been returned to the contractor in full and in accordance with the contract and that it has been deleted. This can also be done by inspecting

the data processing systems at the Contractor's premises. The on-site inspection shall be announced by the client with reasonable notice.

15 Right of retention

The parties agree that the defence of the right of retention by the Contractor within the meaning of Section 273 BGB with regard to the processed data and the associated data carriers is excluded.

16 Final provisions

16.1 If the Client's ownership of the Contractor is jeopardised by third-party measures (such as seizure or confiscation), insolvency proceedings or other events, the Contractor must inform the Client immediately. The Contractor shall immediately inform the creditors of the fact that the data in question is being processed on behalf of the Client.

16.2 Additional agreements must be made in writing.

16.3 Should individual parts of this contract be invalid, this shall not affect the validity of the remaining provisions of the contract.

17 Attachments

Annex 1 Subcontractor

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

Phone: +49 (0) 82 06 - 5 27 90 - 0
Email: info@sasg.de
Web: www.sasg.de
Commercial register (HRA) 18415

Personally liable partner: SaSG Verwaltungsgesellschaft mbH Commercial Register (HRB) 29326

Authorised managing director: Peter Heidenreich

2. Trichoscan module
Datinf GmbH
Wilhelmstr. 42
D - 72074 Tuebingen

Managing Directors: Dr Ulf Ellwanger, Dr Holger Lüdtke

Phone: 07071-253696-6
Email: info@datinf.de
Web: http://www.datinf.de
Commercial register: Stuttgart HRB 382401
VAT ID number: DE225543033

3. Remote support
TeamViewer Deutschland GmbH
Bahnhofsplatz 2
D - 73033 Göppingen

Managing Directors: Oliver Steil, Michael Wilkens, Peter Turner, Mei Dent
Phone: +49 7161 60692 50
Email: contact@teamviewer.com
Commercial register: Ulm HRB 534075
VAT ID number: DE245838579

Annex 2 Technical and organisational measures of the contractor

Annex 3 Technical and organisational measures SaSG

Annex 4 SCC