Data Processing Agreement

Preamble

This Data Processing Agreement (DPA) specifies the data protection obligations of the contracting parties arising from the contract referring to this DPA (hereinafter referred to as the "Main Contract").

All obligations described in this contract shall apply to all activities related to the Main Contract in which employees of the Contractor or third parties commissioned by the Contractor come or may come into contact with personal data of the Client.

This DPA contains two use cases,

1. the operation of SaaS applications and
2. remote maintenance of the client's IT systems and devices.

As far as information in this DPA refers to only one application case, the case distinction is indicated in the following text by corresponding headings.

§ 1 Definitions

The definitions according to Art. 4 of EU Directive 2016/679 (General Data Protection Regulation, GDPR) apply. The following definitions also apply:

(1) Anonymization

Process by which personal data are irreversibly altered, either by the data controller alone or in cooperation with another party, in such a way that the data subject can no longer be identified, either directly or indirectly.

(2) Third country

A country that is outside the EU/EEA.

(3) Main Contract

Contract (usually a service contract) in which all details of the processing are described.

(4) Subcontractor

Service provider commissioned by the Contractor whose services and/or work are required by the Contractor to provide the services described in this contract to the Client.

(5) Processing by order

Processing on behalf is the processing of personal data by a contractor on behalf of the client.

(6) Instruction

An instruction is a written order issued by the client for the contractor to handle personal data in accordance with data protection regulations (e.g. anonymization, blocking, deletion, disclosure). The instructions are initially set out in the Main Contract and can then be amended, supplemented or replaced by the client in writing by means of individual instructions (individual instructions).

§ 2 Object of the order

The contractor processes personal data on behalf of the client. This includes activities that are named in the Main Contract and specified in the service description contained therein. In particular, the following data are part of the data processing:

Use case 1: Operation of SaaS applications

Type of data	Purpose of data processing	Circle of those affected
Last name, first name, ID, user name, password	User administration	Customer employees (administrators, medical professionals or trainers)
Surname, first name, date of birth, gender, ethnicity	Management of master data	Patients or studio members or employees and participants in the Occupational Health Management
Bioimpedance measured values	Recording, analysis and display of body composition	Patients or studio members or employees and participants in the Occupational Health Management

Use case 2: Remote maintenance

Type of data	Purpose of data processing	Circle of those affected
Personal data not further defined	Access to data as part of remote maintenance	Patients or studio members or employees of the customer

§ 3 Responsibility

(1) Within the scope of this contract, the client is responsible for compliance with the statutory provisions, in particular for the lawfulness of data processing ("controller" within the meaning of Art. 4 No. 7 GDPR).

(2) The contents of this DPA apply accordingly if the testing or maintenance of automated processes or data processing systems is carried out on behalf of the client and access to personal data cannot be ruled out.

(3) Clients and contractors must ensure that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality. To this end, all persons who have access to the client's personal data in accordance with the contract must be bound to data secrecy and instructed about their data protection obligations. Each party is responsible for obligating its own personnel. Furthermore, the persons deployed must be informed that data secrecy continues to apply even after the end of their work.

(4) The Client and the Contractor shall be responsible for compliance with the relevant data protection laws with regard to the data to be processed.

§ 4 Duration of the order

(1) The term of this DPA is based on the term of the Main Contract.

(2) The contracting parties are aware that no (further) commissioned processing may be carried out without the existence of a valid DPA, e.g. upon termination of the present contractual relationship.

(3) The right to terminate the contract without notice for good cause remains unaffected.

(4) Notices of termination must be in writing to be effective.

§ 5 Authority of the client to issue instructions

(1) The data shall be handled exclusively within the framework of the agreements made and in accordance with the documented instructions of the client. Exceptions to this are cases in which the Contractor is required to process data for compelling legal reasons. In such

situations, the Contractor shall inform the Client of the relevant legal requirements prior to the start of processing as far as possible.

The Client reserves the right to issue comprehensive instructions regarding the type, scope and procedure of data processing within the scope of the order description set out in this agreement, which it may specify in individual instructions.

(2) Changes to the object of processing and procedural changes are covered by the client's authority to issue instructions and must be documented accordingly. If the Contractor considers a change to the order to be significant, the Contractor shall have the right to object. If the Client insists on the change despite the Contractor's objection, this change shall be regarded as good cause and shall permit termination without notice of the DPA contract affected by the instruction and the components of the corresponding Main Contract affected by this DPA.

(3) The Client shall confirm verbal instructions immediately in writing or by e-mail (in text form). The Contractor shall make a note of the date, time and person who issued the verbal instruction, as well as the reason a written instruction could not be issued.

§ 6 Place of performance

(1) The Contractor shall provide the contractual services in the European Union (EU) or in the European Economic Area (EEA), any subcontractors at the service locations of the subcontractors in the European Union (EU) or in the European Economic Area (EEA) agreed with the Client in Section 12.

(2) The Client agrees to the relocation of a place of performance within the country of performance for which consent has been given if it can be proven that the same level of safety is provided there and no legal provisions applicable to the Client speak against this relocation. The burden of proof lies with the contractor.

(3) If the place of service provision is relocated to countries that are members of the EU/EEA and have a level of data protection that satisfies and verifies this contract, the client will be informed in writing.

(4) If the Contractor is not informed by the Client within a period of four weeks after receipt of the notification pursuant to para. 3 of the relocation of reasons that do not permit a relocation, the Client shall be deemed to have given its consent to this relocation.

(5) If the Contractor wishes to provide the services owed in whole or in part from a location outside the EU/EEA in a so-called secure "third country" or plans to relocate the provision of services there, the Contractor shall obtain the prior written consent of the Client. In this case, the Contractor shall ensure compliance with and implementation of the legal requirements to ensure an adequate level of data protection in the event of relocation and cross-border data traffic.

(6) If the transfer of services to another country is possible in accordance with the above provisions, this shall apply accordingly to any access or any view of the data by the Contractor, e.g. within the framework of internal controls or for the purposes of development, the performance of tests, administration or maintenance.

§ 7 Obligations of the Contractor

(1) The Contractor shall design the internal organization in its area of responsibility in such a way that it meets the specific requirements of data protection. The Contractor shall take technical and organizational measures to adequately secure the Client's data against misuse and loss in accordance with the requirements of the relevant data protection regulations; the Contractor must provide evidence of these measures to the Client and, if applicable, to supervisory authorities upon request. This proof includes the implementation of the measures resulting from Art. 32 GDPR.

The technical and organizational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative,

demonstrably adequate measures. In doing so, it must be ensured that the contractually agreed level of protection is not undercut. Significant changes must be documented. A description of these technical and organizational measures in the currently valid version can be found at https://www.seca.com/legal.

(2) The Contractor itself shall keep a record of the processing activities taking place at its premises within the meaning of Art. 30 GDPR. Upon request, it shall provide the client with the information required for the overview in accordance with Art. 30 GDPR. Furthermore, it shall make the register available to the supervisory authority upon request.

(3) The Contractor shall support the Client in any necessary data protection impact assessment with all information available to it. If prior consultation with the competent supervisory authority is necessary, the Contractor shall also support the Client in this regard.

(4) The Contractor is obliged to treat as confidential all knowledge of the Client's trade secrets and data security measures acquired during the contractual relationship.

(5) Andreas Rieschick (e-mail data.privacy@seca.com) is currently appointed as the Contractor's data protection officer. The Client must be informed immediately in writing of any change of data protection officer. The Contractor shall ensure that the requirements for the data protection officer and his activities pursuant to Art. 38 GDPR are met.

(6) The Contractor shall inform the Client immediately of any breaches by the Contractor or the persons employed by the Contractor within the scope of the order of the Client's personal data protection regulations or the stipulations made in the contract. The Contractor shall take the necessary measures to secure the data and to minimize possible adverse consequences for the data subjects and shall consult with the Client immediately in this regard. The Contractor shall support the Client in fulfilling the information obligations towards the respective competent supervisory authority or the persons affected by a breach of the protection of personal data in accordance with Art. 33, 34 GDPR.

(7) If a data subject contacts the Contractor directly to correct or delete their data, the Contractor will forward this request to the Client without delay.

(8) Any data carriers provided and all copies or reproductions made thereof shall remain the property of the Client. The Contractor shall store these carefully so that they are not accessible to third parties. The Contractor shall be obliged to provide the Client with information at any time insofar as its data and documents are affected.

(9) If the Client is obliged under applicable data protection laws to provide a data subject with information on the processing of that person's data, the Contractor shall support the Client in providing this information, provided that the Client has requested the Contractor to do so in writing.

(10) The Contractor shall inform the Client immediately of any inspections and measures by the supervisory authorities or if a supervisory authority investigates the Contractor.

(11) The Contractor shall notify the Client immediately if, in its opinion, an instruction issued by the Client violates statutory provisions. The Contractor shall be entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Client.

(12) Should the Client's data be jeopardized by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Client immediately. The Contractor shall immediately inform all controllers in this context that the sovereignty and ownership of the data lies exclusively with the Client as the controller within the meaning of the GDPR.

(13) The contractor shall not use the data provided for any purposes other than the fulfillment of the contract without an additional legal basis and shall not use any means of processing that have not been previously approved by the client.

(14) The Contractor shall not store any patient data on systems that are outside the control of the Client.

(15) If the contractor is obliged by Union or Member State law to process the data in another way, the contractor shall notify the client of these legal requirements prior to processing. The notification shall not be made if the relevant national law prohibits such notification due to an important public interest.

(16) The Contractor shall monitor and document the fulfillment of the aforementioned obligations and provide the Client with suitable evidence thereof upon request.

§ 8 Remote access for testing/maintenance of a system or other services via remote access

Use case 2: Remote maintenance

The following additional rights/obligations of the client/contractor apply to the performance of remote access for the testing and/or maintenance of automated processes or data processing systems or for remote access for other services:

(1) Remote access in the context of testing and/or maintenance work on workplace systems will only be carried out after approval by the respective authorized person / responsible employee of the client.

(2) Remote access in the context of testing and/or maintenance work on automated processes or data processing systems will only be carried out with the consent of the client if access to personal data cannot be ruled out with certainty.

(3) The Contractor's employees shall use appropriate identification and encryption procedures.

(4) Before carrying out remote access, the Client and the Contractor shall agree on any necessary data security measures in their respective areas of responsibility.

(5) Remote access in the context of inspection and/or maintenance work shall be documented and logged. The client is entitled to monitor inspection and maintenance work before, during and after it is carried out. In the case of remote access, the client is - as far as technically possible - entitled to follow this from a control screen and to cancel it at any time.

(6) The Contractor shall only make use of the access rights granted to it to automated processes or data processing systems (in particular IT systems, applications) of the Client to the extent - also in terms of time - that is necessary for the proper execution of the commissioned maintenance and inspection work.

(7) Insofar as activities for error analysis are required during the provision of services, for which knowledge (e.g. also read access) or access to active data (production / real data) of the client is necessary, the contractor shall obtain the prior consent of the client.

(8) Activities for error analysis that require a data dump of the active operating data require the prior consent of the client. In the case of data extraction of the active operating data, the Contractor shall delete these copies, irrespective of the medium used, after rectification of the error. Effective data may only be used for the purpose of error analysis and exclusively on the equipment provided by the Client or the Contractor, provided that the Client has given its prior consent. Active data may not be copied to mobile storage media (such as USB memory sticks or similar devices) without the consent of the Client.

(9) Remote access in the context of inspection and/or maintenance work and all activities required in this context, in particular activities such as deletion, data transfer or error analysis, shall be carried out taking into account technical and organizational measures for the protection of personal data. In this context, the Contractor shall take the technical and organizational measures as described in the Annex.

§ 9 Obligations of the client

(1) The client is solely responsible for assessing the permissibility of the data processing and for safeguarding the rights of the data subjects. Within its area of responsibility, the client shall ensure that the legally required prerequisites (e.g. by obtaining declarations of consent for the processing of the data) are created so that the contractor can provide the agreed services without infringing the law.

(2) The Client must inform the Contractor immediately and in full if it discovers errors or irregularities with regard to data protection regulations when checking the results of the order.

(3) The client is responsible under data protection law with regard to the procedures used by the contractor and approved by the client for the automated processing of personal data and - in addition to the contractor's own obligation - also has the obligation to keep a record of processing activities.

(4) The client is responsible for the information obligations resulting from Art. 33, 34 GDPR towards the supervisory authority or those affected by a breach of the protection of personal data.

(5) The client shall stipulate the measures for the return of the data carriers provided and/or the deletion of the stored data after completion of the order by contract or by instruction.

(6) The Client shall be obliged to treat as confidential all knowledge of the Contractor's trade secrets and data security measures acquired in the course of the contractual relationship.

(7) The Client shall ensure that the requirements resulting from Art. 32 GDPR with regard to the security of processing are complied with on its part. This applies in particular to remote access by the contractor to the client's databases.

§ 10 Control rights of the client

(1) The client has selected the contractor on the basis that it offers sufficient guarantees to implement appropriate technical and organizational measures in such a way that the processing is carried out in accordance with the requirements of the GDPR and ensures the protection of the rights of the data subject. It shall document the result of its selection.
For example, he can
- take into account data protection-specific certifications or data protection seals and certification marks,
- obtain written self-declarations from the contractor,
- obtain a certificate from an expert or
- after timely notification during normal business hours without disrupting operations, personally or through a competent third party, who may not be in a competitive relationship with the contractor, to ensure compliance with the agreed regulations.

(2) If the Contractor or the persons employed by the Contractor within the scope of the order have violated the Client's regulations on the protection of personal data or the stipulations made in the contract, a related audit can also be carried out without timely notification. Disruption to the Contractor's operations should also be avoided as far as possible in this case.

(3) The Contractor shall support the implementation of the order control by means of regular checks by the Client with regard to the execution or fulfillment of the contract, in particular compliance with and, if necessary, adjustment of regulations and measures for the execution of the order. In particular, the Contractor undertakes to provide the Client, upon written request and within a reasonable period of time, with all information required to carry out an inspection.

(4) The Client must inform the Contractor immediately and in full if it discovers errors or irregularities with regard to data protection regulations during the inspection.

§ 11 Correction, restriction of processing, deletion and return of data carriers

(1) During the ongoing assignment, the Contractor shall only correct, delete or block the contractual data at the instruction of the Client.

(2) If destruction is to be carried out during the ongoing assignment, the Contractor shall only undertake the demonstrably data protection-compliant destruction of data carriers and other materials based on a corresponding individual order from the Client. This shall not apply if a corresponding provision has already been made in the main contract.

(3) In exceptional cases to be determined by the client, the goods shall be stored or handed over.

(4) Upon completion of the provision of the processing services, the contractor must either delete or return all personal data to the client at the client's discretion, unless there is an obligation to store the personal data under Union law or the national law applicable to the contractor. The log of the deletion must be presented upon request.

(5) If additional costs are incurred due to deviating specifications for the release or deletion of the data, a prior written agreement on the bearing of costs is required.

(6) If it is essential to transport the storage medium before deletion, the Contractor shall take appropriate measures to protect it, in particular against theft, unauthorized reading, copying or modification. The measures and the deletion procedures to be used shall be agreed in addition to the service descriptions as required.

(7) Documentation that serves as proof of proper data processing in accordance with the order shall be retained by the Contractor beyond the end of the contract in accordance with the

respective retention periods. The Contractor may hand them over to the Client at the end of the contract in order to discharge the Client.

(8) The client may request the correction, deletion, restriction of processing (blocking) and surrender of data by the contractor at any time, i.e. both during the term and after termination of the contract, if the contractor has the opportunity to comply with this request.

(9) The Contractor shall correct, delete or block the contractual data if instructed to do so by the Client. The destruction of data carriers and other materials in compliance with data protection regulations shall be carried out by the Contractor based on an individual order by the Client, unless otherwise agreed in the contract. In special cases to be determined by the Client, storage or handover shall take place. If a data subject contacts the Contractor directly for the purpose of correction or deletion of their data, the Contractor shall forward this request to the Client without delay.

(10) If it is not possible for the client to take back the data, the client shall inform the contractor in writing in good time. The contractor is then entitled to delete personal data on behalf of the client.

§ 12 Subcontractors

(1) The Contractor is entitled to use the subcontractors specified below for the processing of data on behalf of the Contractor. The change of subcontractors or the commissioning of further subcontractors is permitted under the conditions specified in paragraph 3.

Use case 1: Operation of SaaS applications

Name and address of the subcontractor	Description of the partial services	Place of service provision
Amazon Web Services EMEA Sàrl Avenue John F. Kennedy 38 1855 Luxembourg Luxembourg	Infrastructure and application hosting	Frankfurt a.M. region (Germany)
Blue Bridge UAB J. Jasinskio g. 16A 01112 Vilnius Lithuania	Function management and 24/7 monitoring of the cloud environment	Vilnius (Lithuania)

Use case 2: Remote maintenance

Name and address of the subcontractor	Description of the partial services	Place of service provision
TeamViewer Germany GmbH Bahnhofsplatz 2, 73033 Göppingen, Germany	Remote maintenance software (if the TeamViewer license from seca is used to establish the remote maintenance connection).	Remote maintenance from seca headquarters; use of TeamViewer servers within the European Union

(2) The Contractor shall carefully select the subcontractor 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 organizational measures required under Art. 32 GDPR to protect personal data.

(3) In the event of a planned change of subcontractor or the planned commissioning of a new subcontractor, the Contractor shall inform the Client in text form in good time, but no later than six weeks before the change or new commissioning ("Information"). The client shall have the right to object to the change or new assignment of the subcontractor in text form within

four weeks of receipt of the "Information", stating the reasons. If no objection is made by the client within four weeks of receipt of the "Information", this shall be deemed to constitute the client's consent to the change or reassignment of the subcontractor concerned. In the event of an objection, both contracting parties shall have a special right of termination with a notice period of at least 14 days to the end of a calendar month.

(4) If the Contractor is authorized within the meaning of this Agreement to use the services of a subcontractor to carry out certain processing activities on behalf of the Client, the same obligations shall be imposed on this subcontractor by way of a contract as are set out in this Agreement between the Client and the Contractor, in particular with regard to the data protection and data security requirements between the contracting parties to this Agreement and the Client's control and verification rights described in this DP Agreement. Sufficient guarantees must also be provided to ensure that the appropriate technical and organizational measures are implemented in such a way that the processing is carried out in accordance with the requirements of the GDPR.

(5) Upon written request, the Client is entitled to obtain information from the Contractor about the data protection obligations of the subcontractor, if necessary also by inspecting the relevant contractual documents.

(6) A subcontractor relationship requiring approval does not exist if the contractor commissions third parties as an ancillary service to the main service, such as personnel, postal and shipping services.

However, the contractor is obliged to make appropriate and legally compliant contractual agreements and to take control measures to ensure the protection and security of the client's data, even in the case of ancillary services outsourced.

(7) If the subcontractor fails to comply with its data protection obligations, the contractor shall be liable to the client for compliance with the obligations of that subcontractor.

§ 13 Right of retention

The defense of the right of retention, regardless of the legal grounds, of the contractual data and any existing data carriers is excluded.

§ 14 Liability

(1) The client and contractor are jointly liable to the respective data subject for any damage caused by processing that does not comply with the GDPR.

(2) The Contractor shall only be liable for damage resulting from processing carried out by him in which
   a. it has not complied with the obligations resulting from the GDPR and specifically imposed on processors, or
   b. he acted in disregard of the lawfully issued instructions of the client or
   c. he has acted contrary to the lawful instructions of the client.

(3) Insofar as the Client is obliged to pay damages to the party concerned, it reserves the right of recourse against the Contractor.

(4) However, in the internal relationship between the Client and the Contractor, the Contractor shall only be liable for damage caused by processing if it
   a. has not complied with its obligations specifically imposed on it by the GDPR or
   b. has acted in disregard of the lawfully issued instructions of the client or against these instructions.

(5) Further liability claims according to the general laws remain unaffected.

§ 15 Clients from Switzerland and the United Kingdom

(1) If the client is domiciled in the Swiss Confederation, the corresponding articles of the Swiss Federal Act on Data Protection (FADP) shall apply instead of the articles of the GDPR

referenced   in   this   document.

The following table provides an overview of the assignment of the referenced articles

Contents	DS-GVO	DSG	Referenced in
Definitions of terms	Art. 4	Art. 5	§ 1, § 3
List of processing activities	Art. 30	Art. 12	§ 7
Technical and organizational measures	Art. 32	Art. 8	§ 7, § 9, § 13
Notification of breaches of the protection of personal data	Art. 33, 34	Art. 24	§ 7, § 9
Data protection officer / consultant	Art. 38	Art. 10	§ 7

(2) If the client is based in the United Kingdom, the General Data Protection Regulation of the United Kingdom (UK GDPR) shall apply instead of the EU GDPR. The numbers of the articles of the EU GDPR referenced in this document correspond to those of the UK GDPR.