APPENDIX 1: Data processing agreement

between

Frederiksberglægen (Pernille Lund)
Gammel Kongevej 164, 2. Tv
1850 Frederiksberg C, Denmark
VAT no: DK 36275138

(the Data Controller)

and

VentriJect Aps
Ryvangs Allé 81
2900 Hellerup, DK
VAT: DK 39424371

(the Data Processor)

(collectively, Parties, individually, Party)

1. THE DATA PROCESSING AGREEMENT AND THE MAIN AGREEMENT

1.1 **Main Agreement**. The Parties have entered into an agreement processing and storage of subject information, in relation to estimation of VO_2-max (the Main Agreement). In this connection, the Data Processor must process personal data on behalf of the Data Controller. Therefore, the following data processing agreement (the Data Processing Agreement) has been concluded.

1.2 **Interdependence.** The Main Agreement and the Data Processing Agreement are interdependent. When the Main Agreement is terminated, the Data Processing Agreement terminates as well. The Data Processing Agreement may, however, be terminated separately or amended, provided that both Parties agree.

1.3 **Priority.** The Data Processing Agreement takes precedence over the Main Agreement so that terms of the Main Agreement in conflict of terms in the Data Processing Agreement give way for the terms of the Data Processing Agreement.

2. THE DATA CONTROLLER'S OBLIGATIONS

Legal processing. The Data Controller shall ensure that the processing of personal data under the Data Processing Agreement takes place in accordance with the Regulation 2016/679, the General Data Protection Regulation (GDPR), data protection provisions in other EU or national law to which the Data Controller is subject (collectively, Data Protection Law) and the Data Processing Agreement and must ensure that there is a processing basis for the processing that the Data Processor is instructed to carry out, in accordance with clause 3.1 below.

3. THE DATA PROCESSOR'S OBLIGATIONS

3.1 **Instructions**. The Data Processor may only process personal data in accordance with documented instructions from the Data Controller unless this is required by Data Protection Law.

The instructions are as follows:

a) The Data Processor processes health and demographic information about persons undergoing analysis with Seismofit® for the purpose of estimating VO_2-max.

3.1.1 **Unlawful instructions**. The Data Processor shall immediately notify the Data Controller if, in his or her opinion, an instruction is in breach of Data Protection Law.

3.1.2 **Change of instructions**. If instructions change, the Data Controller is, to the extent that the Parties agree, obliged to make sure that the Data Processing Agreement is updated and to send an updated version signed by the Data Controller to the Data Processor for signature.

3.2 **Confidentiality**. The Data Processor may only grant access to personal data processed on behalf of the Data Controller to persons who are subject to the Data Processor's instructions, who have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality, and only to the extent necessary for carrying out the Data Controller's instructions. The list of persons who have been granted access to personal data must be reviewed on an ongoing basis. Based on this review, access to personal data may be closed if access is no longer necessary, and the personal data must no longer be available to these persons. The Data Processor must, at the request of the Data Controller, be able to demonstrate that the persons in question, who are subject to the Data Processor's instructions, are subject to the above-mentioned duty of confidentiality.

3.3 **Risk assessment**. The Data Controller must assess the risks involved in the processing activities and implement security measures to address these risks. For this assessment, the Data Controller shall make the necessary information available to the Data Processor which enables him or her to identify and assess such risks.

3.4 **Assistance with security**. The Data Processor shall assist the Data Controller in complying with the Data Controller's obligation under Article 32 of the GDPR by, inter alia: to make the necessary information available to the Data Controller regarding the technical and organizational security measures already implemented by the Data Processor and all other information necessary for the Data Controller's compliance with its obligation under Article 32 of the GDPR.

3.5 **Sub-data processors.** The following provisions apply to the extent the Data Processor uses sub-data processors in connection with the processing under the Data Processing Agreement.

3.5.1 **General authorisation**. The Data Processor has authorised the Data Controller's use the following sub-data processors for the processing under the Data Processing Agreement:

Full company name, address and VAT-no.	**Processing description**
Microsoft Azure Kanalvej 7, 2800 Kongens Lyngby, Denmark CVR: DK13612870 **Data Center Location** Leopardstown, Dublin, Ireland.	Data hosting and processing.
Send Grid Twilio Ireland Limited, 25-28 North Wall Quay, Dublin 1, Ireland	Email for user password reset.
CloudFlare United States **Data Center Location** All around the world: https://www.cloudflare.com/network/	Protection against DDoS attack and hosting of VentriJect Web Portal, used for creating users of the VentriJect App.
Atlassian United States **Data Center Location** United States and Europe	Support ticket system.
Datadog HQ 620 8th Ave., 45th Fl., New York, NY 10018 USA **Data Center Location:** Germany	Logging of activities in API and App for support and system-error-logging. Customer emails are masked and subject data is not included in this process.
Keepit Per Henrik Lings Allé 4, 7th 2100 Copenhagen Denmark	Backup of Google Workspace and Azure DevOps

Data Center Location: Denmark	Backups are encrypted in transit and rest.
Rewind Software Inc 333 Preston Street, Suite 200 Ottawa, Ontario K1S 5N4 Canada **Data Center Location:** Germany	Backup of Support ticket system and Customers Guides (hosted by Atlassian). Backups are encrypted in transit and rest.

The Data Processor shall notify the Data Controller in writing of any planned changes regarding the addition or replacement of sub-data processors with at least 30 days' notice. If the Data Controller does not object to such changes or replacements within 14 days of receipt of this notification, the Data Controller shall be deemed to have authorised them.

3.5.2 **Requirements to the sub-data processing agreement**. When the Data Processor uses a sub-data processor for the processing under the Data Processing Agreement, the Data Processor shall impose on the sub-data processor the same data protection obligations as those set out in this Data Processing Agreement.

3.5.3 **Delivery of sub-data processing agreements**. Sub-data processor agreement(s) and any subsequent amendments thereto are sent - at the request of the Data Controller - in copy to the Data Controller.

3.5.4 **The Data Controller as a third-party beneficiary**. In its agreement with the sub-data processor, the Data Processor must include the Data Controller as a beneficiary third party in the event of the Data Processor's bankruptcy, so that the Data Controller can exercise the Data Processor's rights and enforce them against sub-data processors, for instance enabling the Data Controller to delete or return the personal data.

3.5.5 **Liability for sub-data processors**. If the sub-data processor does not fulfill its data protection obligations, the Data Processor remains fully liable to the Data Controller for the fulfillment of said obligations.

3.6 **Transfer to third countries**. The Data Processor uses Microsoft as a Sub-data processor who, in some cases, will transfer personal data to third countries. In this case, appropriate SCC's will be entered into, however there is a risk that the data importer's data protection legislation and case law does not meet the requirements and satisfies the guarantees regarding data protection as those set out under EU law.

3.7 **Assistance to the Data Controller**. The Data Processor assists the Data Controller, taking into account the nature of the processing, by means of appropriate measures in fulfilment of the data controller's obligation to respond to requests for the exercise of the data subject's rights as set

out in Chapter III of the GDPR. In addition, the Data Processor must, taking into account the nature of the processing and the information available to the Data Processor:

a) notify the Data Controller of any personal data breach as soon as possible and no later than 48 hours after becoming aware of the breach;

b) assist the Data Controller in notifying personal data breaches to the competent supervisory authority and provide to the Data Controller the information required pursuant to Article 33(1) of the GDPR;

c) assist the Data Controller in carrying out a data privacy impact assessment (DPIA) of the processing activities under the Data Processing Agreement; and

d) assist the Data Controller in consulting the competent supervisory authority before processing if the DPIA mentioned above shows that the processing involves a high risk for the rights and freedoms of the data subjects.

3.8 **Return and deletion**. Upon termination of the Data Processing Agreement, the Data Processor must:

a) return all personal data that has been processed on behalf of the Data Controller in connection with the processing activities mentioned in clause 3.1 above;

b) delete the personal data, unless under mandatory Data Protection Law the Data Processor is obliged to store such data; and

c) at the request of the Data Controller – confirm to the Data Controller that the deletion has taken place and send documentation thereof.

3.9 **Documentation of compliance**. At the request of the Data Controller, the Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with Data Protection Law and the Data Processing Agreement.

3.10 **Audit and inspection**. The Data Processor provides the Data Controller with the opportunity for and contributes to audits, including inspections, carried out by the Data Controller itself or an auditor authorised by the Data Controller.

4. LIABILITY

The Data Processor is only liable for losses arising from the processing activities under clause 3.1 above to the extent that the loss is due to non-compliance of the Data Processor's obligations under Data Protection Law or the Data Processing Agreement. The Data Processor's total liability under this Data Processing Agreement may not exceed an amount corresponding to the Data Controller's payments to the Data Processor in accordance with the Main Agreement within the last 12 months from the occurrence of the loss.