Appendix 2. Data processing agreement (DPA)

1 ABOUT THE DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") regulates the parties' rights and obligations in connection with COMPANY ("**Data Processor**") processing personal data on behalf of the Customer ("**Data Controller**") pursuant to:

- the Act of 15 June 2018, No. 38 relating to the processing of personal data (Personal Data Act);
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (hereinafter referred to as the "GDPR");
- the Act relating to Personal Health Data Filing Systems and Processing of Health Data of 20 June 2014, No. 43 (Personal Health Data Filing Systems Act);
- the Act relating to the processing of health data when performing health care of 20 June 2014, No. 42 (Health Records Act); and
- any acts, regulations or other rules that amend or replace the above rules.

The governing laws and regulations stated in the provisions of personal data protection legislation or relevant health care legislation shall take precedence over DPA if the information in this DPA conflicts with such legislation. In the event of conflict between this DPA and the Subscription Terms, the latter one shall take precedence.

2 DEFINITIONS

The terms "personal data", "processing", "data controller", "data processor", "personal data breach" and "health data" shall be understood as they are defined in Article 4 of the GDPR, the Personal Health Data Filing System Act, Section 2 and the Health Record Act, Section 2.

3 THE PURPOSE OF THE DATA PROCESSING AGREEMENT

The purpose of the DPA is to comply with the requirements for data processor agreements according to the General Data Protection Regulation ((EU) 2016/679).

4 SCOPE

DPA applies to all health and personal data handled and processed by Data Processor on behalf of Data Controller based on the Subscription Terms.

5 THE PROCESSING OF PERSONAL DATA: PURPOSE OF PROCESSING, INFORMATION AND PROCESSING ACTIVITIES.

The Data Processor processes data on behalf of the Data Controller in connection with providing the Service to the Customer.

The Data Processor will process the following types of personal data on behalf of the Data Controller:

- Name, personal identifier, contact information, IP address, title and other data inserted into the Service by the Data Controller or the Data Controller's representatives or Users.
- Name, age, personal identifier, gender, contact information, IP address of the patients or research subjects.
- Feedback interview forms
- Log and usage data, such as IP address, device model, operating system, location, crash logs
- Special categories of personal data: health data:
    - Vital signs (Blood pressure, heart rate, Oxygen saturation, Respiratory rate, Temperature, Weight), lung auscultation, heart auscultation.
    - Health based questionnaire data.
    - Diseases and known allergies.

The personal data is connected to the following categories of data subjects:

- Users added by the Data Controller.
- Patients added by the Data Controller or their authorized Users.
- Research subjects added by the Data Controller or their authorized Users.

The processing involves processing activities necessary to offer the Service to the Customer, including:

- Sending out emails to existing customers.
- Registration of Customer's organization.
- Collection and storing of health data.
- Automated analysis based on health data.
- Anonymization of data.
- Retrain/improve existing CE marked algorithms.
- Post-market analysis of product.
- Exporting anonymized data.
- Collect and structuring of feedback from feedback forms.
- Registration of new users.
- Collection of audit logs.

The Data Processor shall only process personal data for the following purposes:

- To facilitate account creation and authentication and otherwise manage user accounts.
- To respond to user inquiries/offer support to users.
- To send administrative information to users.

- To enable user-to-user communications.
- To request feedback through feedback forms.
- To detect unauthorized crashes, investigating crashes or errors.
- To anonymize the data.
- To remove any possibility of reidentification of the subjects when investigation of logs and data or improving the services.
- For fulfilling post-market surveillance obligations per MDR.
- For complying with applicable laws and regulations.
- For fulling the agreement with the Data Controller relating to the offering the Service.

The Data Processor shall not process personal data in any other manner than what is agreed on in this DPA which sets out the documented instructions from the Data Controller. This includes that the Data Processor is not allowed to process personal data for other purposes than as stated above or its own purposes or to disclose personal data to third parties.

6 FRAMEWORKS FOR PROCESSING HEALTH AND PERSONAL DATA

Data Controller has complete control over the health and personal data processed by Data Processor under this DPA.

Unless otherwise agreed or pursuant to statutory regulations, the Data Controller is entitled to access all personal data being processed on behalf of the Data Controller and the systems used for this purpose. Such access will be available for the Data Controller through the Service by logging in.

7 THE DATA CONTROLLER'S OBLIGATIONS

Data Controller shall comply with the obligations stated in personal data protection legislation (see Article 24 of the GDPR, relevant health legislation, other special legislation and this DPA). Data Controller is responsible for adhering to the privacy principles (see Article 5 of the GDPR) and shall, among others, ensure that the data is processed purposefully based on a valid legal basis.

8 THE DATA PROCESSOR'S DUTIES

Data Processor undertakes to process health and personal data in accordance with applicable regulations, this DPA, the Subscription Terms, Data Controller's documented instructions and other agreements between the Parties, as well as the Norms for Information Security in the Health and Care Sector. Data Processor shall not by any act or omission put Data Controller in a position that would violate the provisions of regulations and Acts set forth in Clause 1 of this DPA.

The Data Processor is subject to an obligation of confidentiality regarding documentation and personal data that the Data Processor gets access to under the DPA. This provision also applies

after the termination of the DPA. The Data Processor is obliged to ensure that persons who process the data for the Data Processor, have committed themselves to confidentiality (including signing declarations of confidentiality), and shall upon request disclose such declarations to the Data Controller or the authorities.

Data Processor must not:

a. process health and personal data to a greater degree, other manner or for any other purpose than what is stipulated in this DPA, the Subscription Terms and any later written agreements between the Parties;
b. process health and personal data beyond what is necessary to fulfil Data Controller's obligations under applicable agreements;
c. distribute, hand over, transfer or retrieve health and personal data in any shape or form for or from third parties on its own initiative unless imposed by law or agreed with Data Controller in advance or approved by Data Controller in writing;

Data Processor shall:

a. maintain control of all categories of processing activities carried out on behalf of Data Controller (see Article 30, No. 2 of the GDPR and Clause 5 of this DPA);
b. give Data Controller access to and the right to inspect health and personal data that is processed by Data Processor on behalf of Data Controller;
c. take all reasonable measures to assist Data Controller by ensuring that health and personal data are correct and updated at all times;
d. establish routines for erasing data;
e. ensure that all persons who receive access to personal data processed on behalf of Data Controller are familiar with this DPA and applicable agreements between the Parties, and are subject to the provisions of the Agreements thereof;
f. give Data Controller the necessary assistance to enable Data Controller to fulfil its obligations towards the data subjects, which includes responding to requests from data subjects who wish to exercise their rights set forth in Chapter III of the GDPR;
g. without undue delay notify Data Controller if Data Processor believes that an instruction contravenes the GDPR or other provisions on personal data protection;
h. assist Data Controller to ensure compliance with the obligations set forth in Articles 35-36 of the GDPR regarding a data protection impact assessment and prior consultation with the Norwegian Data Protection Authority;
i. Data Processor shall immediately notify Data Controller if a request is received from an authority to divulge personal data processed under this Data Processor Agreement. Unless disclosure is imposed by law, Data Processor shall not fulfil such requests without Data Controller's prior written consent.
j. The Data Processor shall not process personal data outside the EU/EEA, unless otherwise stated in this DPA. If the transferring of personal data to a country outside the EU/EEA or to an international organization outside the EU/EEA is required according to law in a EU/EEA member state which the Data Processor is subject to or EU/EEA law, the Data Processor shall inform the Data Controller of such requirement prior to the processing, unless the law prohibits such information from being given.

9 THE DATA PROCESSOR'S OPPORTUNITY TO USE SUB-PROCESSORS

Data Controller permits Data Processor to use sub-processor(s) to satisfy its obligations under this DPA and Subscription Terms. Data Processor shall only use the sub-processor(s) listed below. The applicable data location is the location chosen by the Customer in the Subscription Form.

EU Location:

Name	Org. nr.	Address	Delivery type (processing)	Processing site
Amazon Web Services EMEA SARL, Norwegian branch	921 416 873	c/o Kvale Advokatfirma DA Haakon VIIs gate 10 0161 OSLO	Cloud provider for hosting of our platform and our services	Ireland

In addition, the Data Processor has the right to use other sub-processors but is obliged to inform the Data Controller of any intended changes concerning the addition or replacement of other processors, so that the Data Controller has the opportunity to object to the changes. The information shall be given at least 60 days prior to the planned changes taking effect. If the Data Controller objects to the change, the Data Controller has the right to terminate the DPA with 30 days notice.

The Data Processor shall remain fully liable to the Data Controller for the performance of any sub-processors, and respects the conditions referred to in the General Data Protection Regulation article 28 paragraph 4 for engaging another processor. The Data Controller is aware that the Data Processor uses the sub-processors mentioned in section 4, and that the information security obligations related to the processing performed by these are governed specifically by COMPANY's internal Information Security Management System.

The Data Processor shall remain fully liable to the Data Controller for the performance of any sub-processors.

10 TRANSFER OF PERSONAL DATA OUTSIDE THE EU / EEA

The Data Processor uses the sub-processor outside the EU/EEA as documented in section 9.

Apart from this, the Data Processor may not process or use sub-processors that process personal data outside the EU/EEA. Processing outside EU/EEA is subject to prior written approval from the Data Controller. The Data Processor shall ensure that there is a legal basis for the processing of data outside the EU/EEA, or facilitate the establishment of such legal basis.

If due to transferring health and personal data to another country, regardless of whether it is inside the EU/EEA or outside the EU/EEA (third countries) Data Controller needs to perform a special risk assessment, Data Processor shall, upon written request by the Data Controller, provide all necessary documentation about security, risk and compliance related to the relevant

sub-processors, so Data Controller has all the information necessary to perform such a special risk assessment.

11 SECURITY

The Data Processor undertakes to pass and implement all technical, organisational and security measures to ensure an appropriate security level at all times for the risk attached to processing health and personal data.

The Data Processor shall at the minimum:

a. establish and comply with all necessary technical and organisational measures with regard to confidentiality, integrity, availability and robustness when processing health and personal data to ensure satisfactory data security in accordance with the provisions of the Personal Data Act, including the requirements set forth in Article 32 of the GDPR and applicable healthcare legislation;
b. ensure that the requirement for built-in privacy and privacy as a standard setting is actualised in the Data Processor's solutions. This includes building in features to fulfil the principles of privacy as well as a functionality to protect the Data Subject's rights, including the right to restriction of processing;
c. have internal control routines;
d. have routines in place for authorisation and control to ensure that only Data Processor's employees who actually need access to the systems and information to carry out necessary assignments to execute the Service/Assignment Agreement have such access. The access level shall conform to the real needs related to executing the assignment. Strong authentication shall be established for accessing health data;
e. establish the necessary systems and routines to protect data security and follow up on deviations, which shall include, e.g. routines for deviation reports, backup routines, normal situation recovery, removing the cause of any deviation and preventing recurrence. Upon request, Data Processor shall give Data Controller access to relevant security documentation for processing health and personal data;
f. uncover, register, report and close data security deviations, including logging and documenting any attempt to gain unauthorised access and other personal data breaches in the data processing systems. Data Processor shall store such documentation;
g. if a personal data breach is found or suspected, Data Controller must be notified without undue delay. The notification should explain the cause of the deviation, the time and date it was uncovered, the categories of and approximate number of data subjects who were affected, the categories of and approximate number of registrations of personal data that were affected, the name of the data protection officer and his or her contact information or another point of contact where more information can be gathered, the assumed consequences of the deviations and which immediate measures were implemented or considered for dealing with the deviation. If all the information cannot be provided at the same time, it may be provided incrementally without further undue delay;
h. document every deviation, including the actual facts related to the deviation, its impact and any implemented remedies;

i. notify the Data Controller without undue delay of any unauthorised disclosure of personal data;
j. register all authorised and unauthorised access to data. All queries must be recorded so they can be tracked to individual users (i.e. Data Processor's employees and sub-suppliers, and Data Controller). The logs should be stored until it is considered they are no longer required or in accordance with the Agreement or as stipulated in the Service/Assignment;
k. assist Data Controller in ensuring compliance with the obligations set forth in Articles 32 – 34 of the GDPR, including, but not limited to:
    a. processing security;
    b. notifying the supervisory authority of a violation or personal data breach;
    c. informing the data subject of the personal data breach;
l. notify Data Controller of matters related to Data Processor's obligations under the Service/Assignment Agreement that weaken or are assumed to weaken data security;
m. obtain Data Controller's written consent before implementing any changes to the data processing that Data Processor carries out under this Agreement that are or may be significant to data security.

The Data Processor shall document routines and other measures made to comply with these requirements regarding the information system and security measures. The documentation shall be available at request by the Data Controller and the authorities.

In the event of a breach of this Agreement or the provisions of personal data protection legislation, health care legislation or other relevant legislation, Data Controller can demand changes to processing procedures or instruct the Data Processor to stop processing the data with immediate effect.

Any notification to the authorities regarding personal data breaches shall be given by the Data Controller, but the Data Processor shall notify any breach directly to the Data Controller. The Data Controller is responsible for reporting the breach to the Data Protection Authorities.

The Data Processor's obligations to assist the Data Controller in fulfilling the obligations of the General Data Protection Regulation article 32 to 36, is considered fulfilled by the Data Processor's obligations according to this DPA. Considering the nature of the processing performed by the Data Processor and the information available for Data Processor, this assistance is considered sufficient. To the extent the Data Controller requires additional assistance from the Data Processor, the Data Processor may offer such assistance as a separately paid service. The Data Processor may also refuse, unless the Data Processor's assistance is necessary in order to be able to fulfil the Data Controller's obligations.

12 DOCUMENTATION AND SECURITY AUDITS

The Data Processor shall have documentation that proves that the Data Processor complies with its obligations under this DPA and the General Data Protection Regulation. The documentation shall be available for the Data Controller on request. The Data Processor shall regularly conduct

security audits, and the Data Controller shall have an opportunity to access results of the audit. The Data Controller shall be entitled to conduct audits and inspections regularly, for systems etc. covered by this DPA, in accordance with the requirements of the General Data Protection Regulation. Audits may be carried out by the Data Controller or a third party mandated by the Data Controller in agreement with the Data Processor. To the extent the Data Controller requires additional assistance from the Data Processor, the Data Processor may offer such assistance as a separately paid service. The Data Processor may also refuse, unless the Data Processor's assistance is necessary in order to be able to fulfil the Data Controller's obligations.

Should an audit uncover any deviation from the obligations in applicable privacy rules or the Agreement, Data Processor shall remedy the deviation without undue delay. Data Controller can demand Data Processor to stop all processing activities or parts thereof until Data Controller has approved such remedying.

Each Party covers their own costs for inspections carried out by relevant supervisory authorities and up to one annual audit initiated by Data Controller.

13 FULFILLING THE RIGHTS OF THE DATA SUBJECTS

The Data Processor's processing on behalf of the Data Controller is not of a nature which makes it necessary or reasonable for the Data Processor to fulfil or assist in fulfilling the Data Controller's obligations towards data subjects. To the extent the Data Controller requires assistance from the Data Processor, the Data Processor may offer such assistance as a separately paid service. The Data Processor may also refuse, unless the Data Processor's assistance is necessary in order to be able to fulfil the Data Controller's obligations.

14 THE DURATION OF THE DPA AND THE PROCESSING

The DPA applies as long as the Data Processor processes personal data on behalf of the Data Controller according to the subscription terms.

15 TERMINATION

The DPA may be terminated in accordance with the termination clauses in the subscription terms. A termination of the subscription terms also constitutes a termination of the DPA.

16 RETURN, DELETION AND/OR DESTRUCTION OF DATA UPON TERMINATION OF THE DPA

COMPANY can on-demand export the Customer's data which may be requested by the Customer during the term of the Agreement.

The Data Processor will permanently erase all personal data and other data relating to the Customer and personal data for which the Customer is a Data Controller in accordance with the

timelines set out in the subscription terms unless the Data Processor is required by law to store the personal data.