APPENDIX 1: PROCESSING OF PERSONAL DATA

1 Definitions

”**Data Protection Legislation**” means the GDPR and the applicable national legislation on the processing of Personal Data;

”**GDPR**” means the General Data Protection Regulation of the European Union (2016/679/EU);

”**Personal Data**” means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

”**Personal Data Breach**” means an event leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data Processed;

“**Processing**” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2 General

2.1 This Data Processing Appendix (“**DPA**”) sets out the terms and conditions under which Supplier Processes Customer’s Personal Data. The purpose of this DPA is to take into account the responsibilities and obligations set by the GDPR.

2.2 Customer is the data controller of Customer’s Personal Data Processed in connection with the Service (as defined in the Agreement). As a data controller, Customer determines the purposes and means of the Processing of Personal Data. Supplier is the data processor, who Processes the said Personal Data on behalf of and by the order of the Customer as agreed in this DPA. Parties shall agree more specifically in Schedule 1.1 on the categories of data subjects, categories of Processing carried out by Supplier, data security procedures and the purpose for which Supplier Processes the Customer’s Personal Data.

2.3 Parties understand that authorities may issue orders and guidelines within the scope of the GDPR after the signing of the Agreement. Parties commit to, if necessary, amend this DPA mutually in writing based on such orders and guidelines.

2.4 Parties shall inform each other of the contact details of their possible data protection officers.

3 Responsibilities of Customer

3.1 Customer is responsible for the lawfulness and completeness of the instructions on the Processing of Personal Data set out in Schedule 1.2 and that there are no defects or errors in the said instructions.

3.2 Customer is responsible for the Personal Data provided to Supplier and the lawfulness of the Processing in accordance with the terms of this DPA. Customer is responsible for providing all appropriate notices and information related to the Processing of Personal Data to the data subjects in accordance with Data Protection Legislation. Supplier does not monitor the content, quality or timeliness of the Personal Data provided by Customer.

3.3 Customer shall ensure that the purpose and grounds for Processing are in compliance with the Data Protection Legislation. Customer shall also ensure that Personal Data has been collected in accordance with the Data Protection Legislation and that Customer has the right to transfer the Personal Data to be Processed by Supplier.

3.4 Parties do not intend to transfer any of the controller's legal obligations arising from the Data Protection Legislation to the Supplier with this DPA.

4 Responsibilities of Supplier

4.1 Supplier shall Process the Personal Data in accordance with the Data Protection Legislation and the written instructions set out in Schedule 1.2, unless otherwise required by law applicable to Supplier. In such case, Supplier shall inform Customer of such legal requirement before the Processing, unless the applicable law prohibits such notification. For the sake of clarity, Customer will always be deemed to have instructed Supplier to provide the services related to the Processing of Personal Data agreed under the Agreement.

4.2 Supplier provides the Service to its customers as a standardised SaaS service and shall endeavour to do this in a consistent, secure and efficient manner and taking into account the technical requirements related to data protection. Parties understand that this may limit the Supplier's possibility to implement changes to the Service based on Customer's instructions. Therefore, Parties shall always agree on changes to the instructions on the Processing of Personal Data set out in Schedule 1.2 and their possible cost effects separately in writing.

4.3 Taking into account the nature of the Processing, Supplier shall assist and support Customer with appropriate technical and organisational measures chosen by Supplier so that Customer can fulfil its obligation to respond to requests concerning the exercise of the following rights of the data subjects, as set out in Chapter III of the GDPR (provided that the data subject has the said right under the GDPR):

a) right of access to the Personal Data;
b) right to rectification and erasure;
c) right to restriction of Processing;
d) right to Personal Data portability; and
e) right to object to Processing of Personal Data.

4.4 In case a Party receives a request concerning the use of the data subject's rights, the Party receiving the request shall notify the other Party of the request immediately and at the latest on the first weekday following the receipt of the request, if fulfilment of the request requires any actions from the other Party and cannot be addressed through the functionalities build in the Service. The notification will contain all information necessary to the other Party to fulfil the request. Supplier is entitled to charge Customer for all actions taken to fulfil the request of the data subject on a time and materials basis in accordance with its price list applicable at the time.

4.5 Taking into account the nature of the Processing, Supplier shall assist Customer in ensuring compliance with the following obligations under Articles 32 to 36 of the GDPR (taking into account the nature of the Processing and the information available to Supplier):

a) ensuring the security of Processing by implementing appropriate technical and organisational measures;
b) notification of Personal Data Breaches to supervisory authority and the data subjects;

c) participating in data protection impact assessment if such impact assessment is necessary under Article 35 of the GDPR; and
d) participating in the prior consultation of the supervisory authority if such prior consultation is necessary under Article 36 of the GDPR.

4.6 Supplier shall assist Customer only to the extent required of a data processor in the Data Protection Legislation. Supplier is entitled to charge Customer for the aforementioned measures on a time and materials basis in accordance with its price list applicable at the time.

5 Data Security

5.1 Parties undertake to implement the technical and organisational measures commonly used in the industry to protect the Personal Data. In connection with agreeing on the implementation of such measures, Parties shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. When assessing appropriate level of security, Parties shall also take into account the risks of the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

Such measures include e.g.:

a) pseudonymisation and encryption of Personal Data;
b) the ability to ensure the continuing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident; and
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of Processing.

5.2 The aforementioned measures are examples of how Parties may ensure the security of the Processing of Personal Data. Parties shall separately agree in Schedule 1.1 on the aforementioned measures or other data security procedures that Supplier shall implement in the Processing of Personal Data. Customer shall ensure appropriate and sufficient data security of the equipment and IT environment under its control.

5.3 Customer shall inform Supplier of all issues related to the Personal Data provided by Customer, such as risk assessment and the inclusion of special categories of Personal Data, which issues affect the technical and organizational measures implemented under this DPA. For the sake of clarity, possible changes to the data security procedures agreed in Schedule 1.1 and the cost effects of such changes shall always be agreed separately in writing.

5.4 Supplier shall ensure that the persons Processing Personal Data are committed to confidentiality or are under an appropriate statutory obligation of confidentiality. Supplier shall implement necessary measures to ensure that the said persons only process Personal Data in accordance with the instructions set out in Schedule 1.2.

6 Transfer of personal data

Supplier does not transfer Personal Data outside the EU and EEA.

7 Subcontractors

7.1 Supplier is entitled to use subcontractors in the provision of the service and the related Processing of Personal Data. The subcontractors used in the Processing of Personal Data at the time of signature of the Agreement are listed in Schedule 1.1. Supplier shall be responsible that its subcontractors Process the Personal Data in accordance with this DPA and the Data Protection Legislation.

7.2 Supplier shall notify Customer if it plans on changing or adding subcontractors participating in the Processing of Personal Data. Customer is entitled to object to such changes on reasonable grounds. Customer shall notify Supplier of the objection without undue delay after receiving the said notice from Supplier. Should Customer not accept the change or the addition of a subcontractor, Supplier has the right to terminate the Agreement with thirty (30) days' notice.

8 Personal Data Breaches

8.1 Each Party shall notify the other Party without undue delay, if it becomes aware of a Personal Data Breach. When notifying Supplier of a Personal Data Breach, Customer shall provide to Supplier all information that can be deemed to help in the investigation, restriction and prevention of the Personal Data Breach. Parties may separately agree on the notification procedure more specifically. Unless otherwise agreed by the Parties, the notification will be made to the contact person informed by each Party.

8.2 When notifying Customer of a Personal Data Breach, Supplier shall, to the extent such information is available to Supplier, provide Customer with the following information:

a) a description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned (as far as the information is available to Supplier);
b) the contact information of Supplier's data protection officer or other contact point where more information can be obtained;
c) a description of the likely consequences of the Personal Data Breach; and
d) a description of the measures taken by Supplier to address the Personal Data Breach and the measures taken by Supplier to mitigate the adverse effects of the Personal Data Breach.

8.3 If the Personal Data Breach is caused by a reason that is under the responsibility of Customer, Customer shall be liable for Supplier's costs resulting from the Personal Data Breach. Customer shall be responsible for notifying the supervisory authority and the data subjects of the Personal Data Breach as set out in the GDPR.

9 Records of processing activities

9.1 Supplier shall maintain a record of Processing activities carried out behalf of Customer. The record contains the following information:

a) the name and contact details of Customer, Supplier and Supplier's possible data protection officer and information about possible subcontractors;
b) the purposes of Processing carried out behalf of Customer;

10 Right to audit

10.1 During the term of the Agreement, Customer or an independent third-party auditor appointed by Customer, which third party may not be Supplier's competitor, shall have the right to audit Supplier's compliance with the obligations addressed to it under this DPA. The subject of the audit will be Supplier's relevant material related to the Processing of Customer's Personal Data and Supplier's systems and premises used in the Processing of Customer's Personal Data. The audit may be carried out no more than once per year and Supplier shall be notified of the audit in writing at least thirty (30) days in advance. However, Supplier shall always allow the regulatory authority supervising Customer's business to conduct audits targeted at Customer's data processor's operations. The relevant parts of this DPA will be applied to such audits.

10.2 Supplier shall participate in the audit and provide to the auditor information required to demonstrate Supplier's compliance with the requirements addresses to it under this DPA. The audit may not interfere with Supplier's operation of services and the auditor will not be entitled to access information of Supplier's customers or partners. Should Customer not be the one performing the audit, the auditor will enter into a confidentiality agreement with Supplier prior to the execution of the audit.

10.3 Customer shall bear all costs resulting from the audit and compensate Supplier for all costs incurred as a result of the audit. If the audit reveals material deficiencies in Supplier's performance, Supplier shall bear its own resulting from the audit.

11 Termination of the processing of Personal Data

11.1 Upon termination of the Agreement and provision of service related to the Processing of Personal Data, Supplier undertakes, in accordance with Customer's written request, to delete or return the Personal Data to Customer. Additionally, upon termination of the Agreement, Supplier shall delete all existing copies of the Personal Data, unless Supplier is required to store the said Personal Data under applicable law or regulation. Supplier is entitled to charge Customer for the return or destruction of the Personal Data on a time and material basis in accordance with its price list applicable at the time. Parties may agree more specifically on the practices related to the deletion or return of Personal Data.

12 Damage caused by the processing of Personal Data

12.1 If a data subject suffers damages due to a breach of the GDPR, each Party shall itself be liable for the damage caused to the data subject in accordance with Article 82 of the GDPR. Each Party shall also itself be liable for any administrative fines imposed by a supervisory authority to it in accordance with Article 83 of the GDPR.

12.2 The limitation of liability clause of the Agreement is applied to this DPA.

13 Schedules

Schedule 1.1 Description of the Personal Data and data security procedures

Schedule 1.2 Instructions on the Processing of Personal Data

Schedule 1.1: Description of the Personal Data and data security procedures

Parties may amend or update this schedule in writing, if necessary.

1 Purpose of Processing

Supplier shall process Personal Data only to prove Customer cloud Service and related support services.

2 Contents of Processing

Supplier shall perform the following Processing activities on the Personal Data:

- Collection
- Recording
- Organisation
- Structuring
- Storage
- Adaptation, alteration
- Retrieval
- Consultation
- Use
- Making data available (disclosure of data by e.g. transmission or dissemination)
- Alignment or combination
- Restriction
- Erasure and destruction
- Other processing operations

3 Categories of data subjects and Personal Data

Supplier shall Process the following categories of data subjects and Personal Data:

- Information related to Users of the Service

    a) Personal information, such as name, etc.
    b) Invoicing information (credit card details)
    c) Usage history of Service (services used and information related to service transactions)

- Information related to Patients that Customer has created to the Service

    a) Information sent by technical devices used by Patient
        - These include measurements of welfare and heath devices, such as, weight, blood pressure and activity.
    b) Information saved by Patient him/herself in the Service
        - Any written information data Patient enters to the Service. The patients are expected to write about their wellbeing and changes in health status.
    c) Information saved by Customer
        - Personal information, such as name, contact information, date of birth, person id, etc.
        - Health data, such as, medication, diagnoses, nurses' and doctors' written notes
    d) Information produced by the Service
        - Observations artificial intelligence of the Service creates based on Patient's data

4 Applicable data security procedures

Supplier shall comply with its own data security guidelines when Processing Personal Data. Supplier shall also implement the following data security procedures:

- Personal Data in encrypted in Supplier's database
- All connections to Supplier's servers and encrypted
- Connections between Supplier's servers and Suppliers database are encrypted

5 Subcontractors of Supplier

Supplier uses the following subcontractors in the Processing of Personal Data under this DPA:

- Amazon Web Services Inc (cloud service platform)
- MongoDB Inc (database)
- Nets Denmark A/S (credit card invoicing)
- Zendesk Inc (support center service)

Schedule 1.2: Instructions on the Processing of Personal Data

These instructions on the Processing of Personal Data concern Customer's requirements for situations where Supplier provides services to Customer that include Processing of Customer's Personal Data as described in the DPA. These instructions supplement Supplier's obligations set out in the DPA concerning the Processing of Personal Data and data security.

1 Digital processing of personal data

Supplier creates one Super Admin user to the Service on behalf of Customer. The Customer is responsible for creating other users and managing their of access rights.

Customer is responsible for setting up needed firewalls and other technical security means to protect itself against unauthorised use of Personal Data. In addition, Customer is to take care of physical data security of devices its users use in accessing Personal Data.

Supplier provides Customer needed tools to delete Personal Data according to the GDPR. Customer is to take care of deletion of Personal Data using the above-mentioned tools when Customer's right to store and access data has ended.

2 Reporting and communications

Supplier will report to Customer all major changes in its security procedures and notify of any security threats related to Personal Data.