DATA PROCESSING AGREEMENT
of TANITA Europe B.V.

This Data Processing Agreement is entered into between TANITA Europe B.V., a Dutch limited liability company with corporate seat in Amsterdam and registered office at Hoogoorddreef 56 E, 1101 BE Amsterdam, the Netherlands and registered with the Dutch Chamber of Commerce under no. 34283024 (the “Data Processor”);
And you as a user of the My Tanita Healthcare App. For the purpose of this agreement you will be referred to as the Data Controller.
Data Controller and Data Processor, each a 'Party' and together referred to as the 'Parties'.

WHEREAS:
a) The Data Controller and Data Processor have concluded the Agreement relating to the use, by the Data Controller, of an app distributed by the Data Processor for the Data Controller’s commercial purposes;
b) The Data Controller’s use of the Data Processor’s app will involve the collection of third-party personal data, including Sensitive Personal Data. This data will be processed, on the Data Controller’s behalf and on its instruction, by the Data Processor;
c) Under article 14 of the Dutch Data Protection Act and, as from 25 May 2018, the General Data Protection Regulation, parties are required to conclude a data processing agreement;
d) Parties will enter into this Data Processing Agreement in order to fulfil their obligations under the Dutch Data Protection Agreement and, as from 25 May 2018, the General Data Protection Regulation.

1. DEFINITIONS

The following terms as used in this Data Processing Agreement shall, unless the context clearly indicates to the contrary, have the meanings set forth in this Clause:

'Agreement' means the end user licence agreement and general terms and conditions of use applicable to the Data Controller’s use of the Data Processor’s app, including any changes thereto and any further agreement agreed to between the Parties that refers to this Data Processing Agreement;

'Applicable Laws' means all laws, including the Dutch Data Protection Act and, as of 25 May 2018, the GDPR, that are applicable to the Processing of Personal Data.

'Data Breach' means any breach of security leading to or that may have led to accidental or unlawful destruction, loss, alteration, compromise, disclosure of, or access to Personal Data, stored, transmitted or otherwise processed in the context of the Agreement;

'Data Processing Agreement' means the present data processing agreement including the annexes hereto;

'GDPR' means the General Data Protection Regulation (Regulation (EU) No 2016/679);

'Personal Data' means any information relating to an identified or identifiable natural person, obtained in relation to the Agreement, as set out in Annex 1;

'Processing' or 'Process' means any operation or set of operations which is performed on Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction;

'Sensitive Personal Data' means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life;

'Sub Processor' means any processor, as defined in the GDPR, engaged by the Data Processor who agrees to Process Personal Data on behalf of the Data Controller;

'Technical and Organisational Measures' means the technical and organisational measures as defined in the GDPR.

2. OBLIGATIONS OF THE DATA PROCESSOR

2.1. The Data Processor shall:

a) Process Personal Data in accordance with Applicable Laws;
b) not Process any Personal Data other than in accordance with the Data Controller’s instructions as set out in Annex 1;
c) only store the Personal Data for as long as the Data Controller requires and correct, anonymise, block or delete the relevant Personal Data at the Data Controller’s instructions; and
d) ensure that the only persons able to process or access any particular Personal Data in Data Processor’s or Sub Processor’s possession, custody or control in the performance of the Agreement are the Data Processor’s or Sub Processor’s employees who need to process or access such Personal Data in order to carry out their duties in connection with the Agreement.

3. TECHNICAL AND ORGANISATIONAL MEASURES

3.1. The Data Processor shall:

a) adopt and maintain suitable Technical and Organisational Measures.
b) taken into account the nature of the processing as well as with all the means at its disposal provide the Data Controller with all reasonable assistance in ensuring compliance with regard to the obligations arising from Applicable Laws, especially articles 32 up to and including 36 of the GDPR when applicable.

3.2. The Data Processor shall ensure that the Technical and Organisational Measures are:

a) appropriate, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of

varying likelihood and severity for rights and freedoms of persons, that, where appropriate, may include, but are not limited to:
i. the pseudonymisation and encryption of personal data;
ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
iii. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

b) adopted and applied in such a way that the Data Controller, with regard to the processing that is entrusted to the Data Processor, constantly acts in compliance with the Applicable Laws.

3.3. The Data Controller may request that the Data Processor take additional security measures.

4. USE OF SUB CONTRACTORS

4.1. The Data Controller grants general authorisation to the Data Processor to engage Sub Processors. The Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of sub processors; the Data Controller may object to such changes.

4.2. The Data Controller grants specific authorisation to the Data Processor to make use of, cloud server services from Amazon Web Services, (currently operating in Germany, Ireland and the UK), for Data Processing purposes.

4.3. In the event Data Processor enters into data processing agreements with relevant sub processors, the sub processor will abide by the same obligations as the data processor under this data processing agreement, meeting the requirements of relevant legislation.

5. TRANSFER OF PERSONAL DATA

5.1. The Data Processor may not transfer Personal Data to a country outside the European Economic Area (the ‘EEA’), unless the Data Controller instructs the Data Processor in writing prior to the transfer or the Data Processor is obliged to transfer Personal Data pursuant to a legal obligation. In case a legal obligation requires the processor to transfer personal data outside the EEA, the Data Processor will inform the Data Controller prior to the transfer, unless it is unable or unauthorised to do so.

5.2. If the Data Controller instructs the Data Processor to transfer personal data to a country outside the EEA the Data Processor is only permitted to transfer and process personal data to this country where:

a) The country in question offers an adequate level of protection according to the EU ‘white list’ of countries offering adequate data protection standards; or
b) EC Model Clauses are concluded between the Data Controller and the Data Processor or a Sub Processor, as set out under article 46(2)(c) and (d) GDPR; or

c) The transfer is allowed based on another legal ground under Applicable Laws and the Data Controller has explicitly consented with a transfer based on such legal ground.

5.3. Where Personal Data is transferred to a Sub Processor located in a country outside the EEA and there are no EC Model Clauses as set out under Clause 5.2(b) available that regulates the transfer between two processors, the Data Controller instructs and authorises the Data Processor to instruct the Sub Processor in Data Controller's name and vis-a-vis the Sub Processor's to conclude EC Model Clauses.

6. AUDITS

6.1. The Data Controller may audit the Data Processor's compliance with this Data Processing Agreement, in particular, the implementation of the Technical and Organisational Measures under this Agreement at any time, subject to a written request stating the Data Controller's reasonable reasons for the audit, provided at least 30 days prior to the date of the intended audit.

6.2. The Data Processor shall provide the Data Controller and its auditors with all reasonable cooperation, access to its Processing facilities and assistance in relation to each audit. Audits must not involve any unjustified interference with Processor's rights, business development, facilities, procedures and systems.

6.3. The Data Controller shall cover all expenses in connection with any such audit, including any expenses incurred by the Data Processor.

7. CONFIDENTIALITY

7.1. The Data Processor shall keep all Personal Data strictly confidential and ensures, prior to the disclosure of Personal Data to its employees, subcontractors or employees of subcontractors, that these persons are bound by the same conditions of confidentiality.
7.2. Subject to Clause 7.1, the Data Processor may disclose Personal Data when a law requires the Data Processor to disclose Personal Data or when the Data Controller instructs the disclosure of Personal Data

7.3. The obligation of confidentiality shall also apply after termination of this Data Processing Agreement.

8. NOTIFICATION OF A DATA BREACH

8.1. As part of the obligations incumbent on the Data Processor with regard to the security of personal data, the Data Processor shall establish and maintain procedures designed to reasonably detected Data Breaches and then implement the correct measures, including recovery measures.

8.2. The Data Processor will promptly, as soon as possible under the circumstances, notify the Data Controller, as set out in Clause 8.3, about (i) any legally binding request for disclosure of Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, and (ii) a Data Breach.

8.3. The Data Processor will notify the Data Controller about every Data Breach as well as:

a) the start and end time and date and the location of such event;
b) the nature and scale of such event;
c) the department or part of the system in which the event occurred;
d) the time needed to reverse damage of the Data Breach;
e) the nature and scope of Personal Data records concerned;
f) the categories and approximate number of data subjects concerned;
g) the likely consequences of such event, including the consequences for the Data subject and a proposal to prevent damage and other negative consequences;
h) measures taken or to be taken to mitigate the consequences of the Data Breach; and
i) the name and contact details of the data protection officer or other contact point where more information about the Data Breach can be obtained.

8.4. The Data Processor shall, within 48 hours of discovery of a Data Breach notify, as set out under Clause 8.2 and 8.3, the Data Controller and subsequently keep the Data Controller fully informed about any progress of the recovery or other relevant developments with respect to such event.

8.5. The Data Processor shall without delay take all reasonable measures to reduce and recover the negative impact of a Data Breach. The Data Processor is obliged to inform Data Controller of these measures.

8.6. Unless required under Applicable Law, the Data Processor shall not, on its own initiative, notify data subjects that are affected or likely to be affected by a Data Breach or the supervisory authority that is competent to take notice of a Data Breach.

9. REQUESTS BY DATA SUBJECTS

9.1. The Data Processor will provide all reasonable assistance to ensure that the Data Controller is able to fulfil its legal obligations when a data subject exercises his or her rights under the Applicable Laws.

9.2. As soon as the Data Processor receives a request as mentioned in Clause 9.1, the Data Processor shall promptly inform the Data Controller. The Data Processor shall not respond to the request without the consent of the Data Controller.

9.3. On the instruction of the Data Controller, the Data Processor shall, without delay, correct, erase or otherwise adjust or process the Personal Data

9.4. The Data Processor will promptly inform the Data Controller about any request or complaint of the Data Subject with respect to the processing of its Personal Data

10. LIABILITY

10.1. The Data Processor shall only be liable for damage to the extent that it is caused through a breach of obligations specifically applicable to processors under the GDPR or where it has acted in breach of this Data Processing Agreement. The

Data Controller shall indemnify and hold the Data Processor harmless from all other damage, including fines imposed by regulators, which arise from or in connection with any act or omission in relation to the Data Processing. In particular, the Data Processor shall not be liable for any damage caused by a breach of the Data Controller's legal obligations.

10.2. In determining the factual responsibility for any event giving rise to damage within the meaning of Clause 10.1, logs and measurements generated by the Data Processor's systems shall be decisive, in the absence of any evidence of greater objective probative value provided by the Data Controller.

11. TERM AND TERMINATION

11.1. This Data Processing Agreement is concluded on the moment the Parties signed the same and is effective until termination of the Agreement.

11.2. Parties agree that on the day of termination of this Data Processing Agreement, the Data Processor shall, at the choice and the costs of the Data Controller return all Personal Data and the copies thereof, by means of the Data Controllers choice, to the Data Controller or a third party designated by the Data Controller.

11.3. After the return of the Personal Data, a written rejection of the return of the Personal Data by the Data Controller, or if the Data Controller does not respond within one month after the offer to return the data, the Data Processor will promptly destroy all Personal Data. On request of the Data Controller, the Data Processor will confirm to the Data Controller in writing that it has destroyed the Personal Data.

12. MISCELLANEOUS

12.1. This Data Processing Agreement shall be governed by, and construed in accordance with, the laws of the Netherlands. The competent court in Midden-Nederland, the Netherlands shall exclusively settle disputes.

12.2. No term of this Data Processing Agreement shall be amended or modified, unless such amendments or modifications are made in writing with express reference to this Data Processing Agreement and signed by both parties.

12.3. The Data Processer shall accept any modification of this Data Processing Agreement which is incorporated for the purpose of compliance with Applicable Laws.

Annex 1 DESCRIPTION OF PROCESSING OPERATIONS

Categories of personal data

The Personal Data processed concern the following categories of data:

Name, address, email, date of birth, sex, height, address, country, telephone

Weight, Body fat, Body water, Muscle mass, Physique Rating, Metabolic age, Visceral fat, BMI, Muscle Quality score, Basal Metabolic Rate, Bone mass, BIA, Phase Angel

Processing operations

The Personal Data are collected by the Data Controller by means of its use of the Data Processor's app. The app is used in the course of the Data Controller's profession for purposes including the collection, storage and evaluation/analysis of information, including Personal Data, relating to the Data Controller's clients/patients.

Annex 2 DESCRIPTION OF TECHNICAL AND ORGANISATIONAL MEASURES

This Annex describes the technical and organisational security measures and procedures that the Data Processor shall maintain to protect the security of Personal Dat a) The Data Processor will keep documentation of technical and organisational measures identified below to facilitate audits and for the conservation of evidence. [Insert IT security measures implemented by processor]