Model Data Processing Agreement for the Association of Healthcare Providers (BoZ)

united in

This document is a translation of the [*Model Verwerkersovereenkomst Brancheorganisaties Zorg (Model Data Processing Agreement for the Association of Healthcare Providers (BoZ)*] In the event that the English translation is inconsistent with the original Dutch text, the Dutch text shall prevail.

12 December 2017

DATA PROCESSING AGREEMENT

THE UNDERSIGNED:

1. Wetenschap Balans , having its registered office at Lichtenauerlaan 102-120, 3062 ME, Rotterdam and registered with the Chamber of Commerce under company number KVK 57822, duly represented by Dr. T.(Ton) J.E.M. Bakker (hereinafter referred to as: '**Data Controller**'); and
2. BPSD Care AB, having its registered office at Scheelevägen 27, 223 70 Lund, Sweden and registered with the Swedish Chamber of Commerce under company number 559011-8302 duly represented by Richard Bibby, (hereinafter referred to as '**Processor**').

hereinafter also to be jointly referred to as 'the Parties' and individually as 'the Party'.

WHEREAS:

(a) The Processor shall provide services on behalf of the Data Controller, as described in the agreements outlined in Annex 1.
(b) The services provided shall include the processing of Personal Details, including information on patients' health.
(c) The Processor shall process the information concerned exclusively at the behest of the Data Controller, and shall not use it for its own purposes.
(d) On 25 May 2018, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) will enter into force.
(e) The Parties wish to record in this Data Processing Agreement their arrangements with regard to the processing of Personal Details to be carried out as part of the services to be provided.
(f) This Data Processing Agreement shall replace any and all similar agreements previously concluded between the parties, where applicable.

DECLARE THAT THEY HAVE AGREED AS FOLLOWS:

Article 1. Definitions

1.1. In this Data Processing Agreement, the following capitalised terms shall have the following meanings:

a)	General Data Protection Regulation, also known as the 'GDPR'	Regulation (EU) 2016/679 of the European Parliament and 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, and

		repealing Directive 95/46/EC.
b)	Party Involved	a natural person whose identity has been or can be identified (Article 4.1 of the General Data Protection Regulation).
c)	Third parties	a third party within the meaning of Article 4.10 of the General Data Protection Regulation.
d)	Data Protection Officer	an officer within the meaning of Article 37 et seq. of the General Data Protection Regulation.
e)	Incident	i a complaint or request for information by a Party Involved with regard to the processing of Personal Details by the Processor; ii an investigation or confiscation of Personal Details by government officials or a suspicion that such may occur at some point in the future; iii a violation of Personal Details within the meaning of Article 4.12 of the General Data Protection Regulation; iv any unauthorised access, removal, damage, loss or any other unlawful act of processing of Personal Details.
f)	Employee	A natural person who works for or at either Party and is involved in the performance of this Data Processing Agreement.
g)	Agreement(s)	The agreements, mentioned in Annex 1, governing the provision of products and/or services.
h)	Party	The Data Controller or the Processor.
i)	Parties	The Data Controller and the Processor.
j)	Personal Details	Any information on a natural person whose identity has been or can be identified within the meaning of Article 4.1 of the General Data Protection Regulation.
k)	Sub-Processor	Any non-subordinate third party hired by the Processor to help process Personal Details as part of the Agreement, not being Employees.
l)	Processor	The Processor within the meaning of Article 4.8 of the General Data Protection Regulation.
M	Data Processing Agreement	This agreement.
n)	Data Controller	The data controller within the meaning of

		Article 4.7 of the General Data Protection Regulation.
o)	Personal Data Protection Act (Wbp)	The Act of 6 July 2000, governing the protection of personal details (Personal Data Protection Act), including later amendments.

1.2. The aforementioned expressions, and others, shall be interpreted in a manner consistent with the General Data Protection Regulation. Until 25 May 2018, terms shall be interpreted in a manner consistent with the comparable provision of the Personal Data Protection Act.

1.3. If there is any reference to certain standards in this Data Processing Agreement (e.g. NEN7510), this shall always be considered to refer to the most up-to-date version of said standard. If the standard concerned is no longer active, the most up-to-date version of the standard's natural successor must be read instead.

1.4. Any departures from the text shall only be valid if and to the extent that they are specified in Annex 4. The provisions of Annex 4 shall prevail over the other provisions of this Data Processing Agreement.

Article 2. What this Data Processing Agreement is about

2.1. This Data Processing Agreement relates to the processing of Personal Details by the Processor at the behest of the Data Controller as part of the performance of the Agreement(s).

2.2. The Parties have decided to enter into this Agreement or these Agreements to utilise the Processor's expertise with regard to the processing and securing of Personal Details for the purposes arising from the Agreement(s) and further outlined in this Data Processing Agreement. The Processor guarantees that it is qualified to do this.

2.3. This Data Processing Agreement constitutes an inseparable part of the Agreement(s). In the event that the provisions of the Data Processing Agreement are inconsistent with the provisions of the Agreement(s), the provisions of the Data Processing Agreement shall prevail.

Article 3. The processing of the data

3.1. The Processor guarantees that it will only process Personal Details on behalf of the Data Controller if:

a.) such is necessary for the performance of the Agreement (within the scope specified in Annex 1); or

b.) the Data Controller has provided written instructions to that effect.

3.2. Pursuant to the provisions of Article 3.1.a, the Processor shall process the Personal Details specified in Annex 1 exclusively for the purposes and in the manner described in said annex.

3.3. The Processor shall follow any and all reasonable instructions provided by the Data Controller with regard to the processing of the Personal Details. The Processor shall notify the Data Controller at once if it feels that said instructions constitute a violation of applicable law governing the processing of Personal Details.

3.4. Without prejudice to the provisions of Article 3.1, the Processor shall be allowed to process Personal Details if it is required to do so by a statutory provision (including the court order or

administrative decisions based on it). In such cases, the Processor shall notify the Data Controller of the intended processing of the data and of the statutory provision prior to the processing, unless it is barred by said legislation from notifying the Data Controller beforehand for pressing reasons protecting the common good. Where possible, the Processor shall enable the Data Controller to defend itself against such enforced processing, and shall minimise the extent of the enforced processing to the maximum extent possible in other respects, too.

3.5. The Processor shall demonstrably process the Personal Details in a proper and meticulous manner, in accordance with the requirements to which it is subject under the General Data Protection Regulation, the Personal Data Protection Act (insofar as this is still in effect), and other laws and regulations. As far as this is concerned, the Processor shall at least establish a register of acts of processing within the meaning of Article 30 of the General Data Protection Regulation and furnish the Data Controller with a copy of said register immediately upon request.

3.6. If the services to be provided by the Processor imply the processing of medical records or other special Personal Details, the Processor shall guarantee that its procedures shall not violate health care legislation.

3.7. Unless it has been granted prior explicit written permission to do so by the Data Controller, the Processor shall not process Personal Details or have Personal Details processed by itself or by third parties in countries outside the European Economic Area ('EEA').

3.8. The Processor guarantees that the Employees involved have signed a non-disclosure agreement and shall allow the Data Controller to inspect said non-disclosure agreement upon request.

Article 4. The security and monitoring of Personal Details

4.1. To protect the Personal Details from loss, unauthorised inspection, damage or any other form of unlawful processing, and to guarantee the availability of the data when due, the Processor shall demonstrably implement appropriate and effective technological and organisational measures, which, considering the current state of the art and the costs associated with it, shall be in accordance with the nature of the Personal Details to be processed, as specified in Annex 1. These security measures shall include any measures which may be stipulated in the Agreement. At the very least, the measures shall include the following:

a.) measures designed to guarantee that only authorised Employees can access the Personal Details for the purposes outlined;

b.) measures involving the Processor only granting its Employees and Sub-Processors access to Personal Details through individual named accounts, with the use of said accounts being adequately logged and with the accounts concerned only granting their users access to those Personal Details whose access is necessary for the legal person concerned;

c.) measures designed to protect the Personal Details from unintentional or unlawful destruction, unintentional loss or changes and unauthorised or unlawful retention, processing, access or disclosure;

d.) measures designed to identify weaknesses with regard to the processing of Personal Details in the systems used to provide services to the Data Controller;

e.) measures designed to guarantee that Personal Details are available when due;

f.) measures designed to guarantee that Personal Details are separated in a sensible manner from the Personal Details the Processor processes on its own behalf or on third parties' behalf;

g.) other measures agreed by the Parties, as laid down in Annex 2.

4.2. The Processor's methods demonstrably comply with the requirements of ISO27001 and/or NEN 7510. Furthermore, the Processor has implemented an appropriate, written security policy for the processing of Personal Details, which at the very least outlines the measures referred to in Article 4.1.

4.3. The Processor demonstrably meets the security requirements for network connections outlined in NEN7512.

4.4. The Processor demonstrably meets the requirements with regard to logging, as outlined in NEN7513.

4.5. The Processor demonstrably meets the requirements of other NEN standards insofar as these have been declared applicable to the healthcare industry.

4.6. Upon the first request of the Data Controller, the Processor shall submit a certificate issued by an independent and competent third party that shows that the Processor's methods comply with the requirements arising from this article, provided that the Processor has been issued with such a certificate.

4.7. The Data Controller is entitled to monitor (or cause to be monitored) the Processor's compliance with the measures referred to in Articles 4.1 to 4.4 (inclusive). At least once per year, upon the request of the Data Controller, the Processor shall enable the Data Controller to inspect the Processor's processing methods at a time to be determined by mutual agreement, and also if the Data Controller feels that there are grounds to do so due to (a suspicion of) information- or privacy-related incidents. The Processor shall cooperate with such an investigation to the maximum extent reasonable. If, in response to such an investigation, the Data Controller provides the Processor with reasonable instructions for revisions of its security policy, the Processor shall act on such instructions within a reasonable time frame.

4.8. The Parties acknowledge that security requirements change all the time and that effective security requires frequent assessments and regular updating of outdated security measures. Therefore, the Processor shall periodically evaluate the measures implemented by virtue of Article 4, and, where necessary, shall update said measures so as to ensure that the obligations arising from Article 4 continue to be fulfilled. The preceding provisions do not affect the Data Controller's right to enforce (or cause to be enforced) additional measures where necessary.

Article 5. Monitoring, obligation to provide information and incident management

5.1. The Processor shall actively monitor for violations of the security measures and shall notify the Data Controller on the results of said monitoring in accordance with Article 5.

5.2. When an Incident occurs, has occurred or may be about to occur, the Processor is required to notify the Data Controller at once and to provide any relevant information on:

1) the nature of the Incident;
2) the Personal Details that (may) have been affected;
3) the actual and likely consequences of the Incident;
4) the measures which have been or will be taken to resolve the Incident or to minimise the consequences or damage to the maximum extent possible.

5.3. Without prejudice to the other obligations arising from this article, the Processor shall be required to implement any measures it can be reasonably expected to implement so as to undo the damage caused by the Incident as soon as possible or minimise further consequences to the maximum extent possible. The Processor shall consult the Data Controller without delay so as to make further arrangements regarding the foregoing.

5.4. The Processor shall cooperate with the Data Controller at any time, and shall follow the instructions given by the Data Controller and enable the Data Controller to conduct a proper investigation of the Incident, formulate a proper response to the Incident and take appropriate subsequent steps, including notifying the Dutch Data Protection Authority and/or the Party Involved as stipulated by Article 5.8.

5.5. The Processor shall at all times have written procedural guidelines ready at hand which shall enable it to furnish the Data Controller with an immediate response to the Incident and to collaborate with the Data Controller in an effective manner so as to handle the Incident. The Processor shall furnish the Data Controller with a copy of such procedural guidelines upon the request of the Data Controller.

5.6. Alerts sent pursuant to Article 5.2 shall be addressed directly to the Data Controller, or, where relevant, to Employees of the Data Controller who have been identified in writing by the Data Controller during the term of the Data Processing Agreement. If the Data Controller has appointed a Data Protection Officer, the alerts must be sent to said Data Protection Officer.

5.7. The Processor is not allowed to provide the parties involved or any other third parties with information on Incidents, except in cases where the Processor is legally required to do so or the Parties have otherwise agreed.

5.8. If and insofar as the Parties have agreed that the Processor will maintain direct contact with the authorities or any other third parties with regard to an Incident, the Processor shall keep the Data Controller updated on these contacts at all times.

Article 6. Obligation of cooperation

6.1. Under the General Data Protection Regulation and other privacy legislation, Parties Involved have certain rights. The Processor shall fully cooperate with the Data Controller to ensure that the Data Controller can fulfil its obligations arising from these entitlements.

6.2. The Processor shall forward to the Data Controller without delay any complaint or request made by a Party Involved with regard to the processing of Personal Details.

6.3. The Processor shall furnish the Data Controller with any relevant information regarding aspects of the manner in which it has processed Personal Details at the first request of the Data Controller to do so, thus allowing the Data Controller to demonstrate, partly on the basis of the information provided, that it complies with applicable privacy regulations.

6.4. In addition, the Processor shall provide the Data Controller, at the first request of the Data Controller, with any support required to help it fulfil the legal obligations it has under applicable privacy regulations (such as performing a privacy impact assessment).

Article 7. The hiring of Sub-Processors

7.1. The Processor shall not outsource activities which involve or require the processing of Personal Details to a Sub-Processor without prior written permission from the Data Controller. The foregoing does not apply to the Sub-Processors listed in Annex 1.

7.2. If the Data Controller agrees to the hiring of a Sub-Processor, the Processor shall impose the same requirements to which it is subject itself under this Data Processing Agreement and legislation, or even stricter requirements, on this Sub-Processor. The Processor shall record these arrangements in writing and shall ensure that the Sub-Processor complies with them. Upon request, the Processor shall furnish the Data Controller with a copy of the agreement(s) it has entered into with the Sub-Processor.

7.3. Notwithstanding the Data Controller's permission for the hiring of a Sub-Processor who will process (some) Personal Details at the Processor's behest, the Processor shall remain fully liable to the Data Controller for the consequences of the outsourcing of duties to a Sub-Processor. If the Data Controller agrees to an outsourcing of duties to a Sub-Processor, such shall not alter the fact that the hiring of Sub-Processors from a country outside the European Economic Area is subject to authorisation, in accordance with Article 3.7 of this Data Processing Agreement.

Article 8. Liability

8.1. The Parties shall be severally responsible and liable for their own acts.

8.2. Any limitations of liability in the Agreement shall apply*mutatis mutandis* to this Data Processing Agreement, on the understanding that:

a.) any (implicit or explicit) exclusions of liability for the loss of and/or damage to Personal Details are excluded;

b.) any (implicit or explicit) exclusions of liability for fines imposed by the Dutch Data Protection Authority or another supervisory body which are directly related to an attributable shortcoming on the part of the Processor, or conduct or negligence attributable to the Processor, are excluded.

8.3. The Processor shall indemnify the Data Controller and compensate the Data Controller for any claims, actions or rights by third parties and any fines imposed by the Dutch Data Protection Authority directly arising from an attributable shortcoming on the part of the Processor and/or its Sub-Processors in the fulfilment of its obligations under this Data Processing Agreement and/or any violation by the Processor and/or its sub-contractors/Sub-Processors of the applicable legislation governing the processing of Personal Details.

8.4. In the event that the Parties are severally liable to third parties, which includes the Party Involved, or in the event that they are jointly fined by the Dutch Data Protection Authority, they shall be required to contribute to the damages and costs in proportion to the percentage of the responsibility they each bear, in accordance with the provisions of Book 6, Title 1, Section 2 of the Dutch Civil Code, unless the General Data Protection Regulation provides otherwise, in which case the General Data Protection Regulation shall prevail.

8.5. If no limitation of liability on the part of the Data Controller is included in the Agreement, the limitation on the part of the Processor stipulated in clause 2 shall also apply to the Data Controller.

8.6. Furthermore, any limitation of liability on the part of the Party concerned shall expire in the event of wilful misconduct or gross negligence on the part of the Party concerned.

8.7. The Parties shall ensure that their liability is sufficiently covered.

Article 9. Costs

9.1. The costs associated with the processing of information which are inherent in the normal performance of the Agreement shall be deemed to be incorporated into the fees already owed under the Agreement.

9.2. The Data Controller shall be invoiced for any form of support or any other additional service the Processor will be required to provide under this Data Processing Agreement or at the request of the Data Controller, including all requests for additional information, at the rates specified in Annex 3.

9.3. The preceding provision shall not apply if the duties to be performed are related to a shortcoming attributable to the Processor under this Data Processing Agreement. In such cases the duties shall be performed free of charge (without prejudice to the Data Controller's right to recoup the costs actually incurred from the Processor).

Article 10. Duration and termination

10.1. This Data Processing Agreement shall enter into force on the date of signing, and the duration of this Data Processing Agreement shall be identical to the duration of the Agreement(s) mentioned in Annex 1, including any extensions thereof.

10.2. Once the Data Processing Agreement has been signed by both Parties, it shall constitute an integral and inseparable part of the Agreement(s). Termination of the Agreement(s) on any grounds whatsoever (termination/cancellation) shall result in the Data Processing Agreement being terminated on the same grounds (and vice versa), unless the Parties agree otherwise (as appropriate).

10.3. Obligations which, by their very nature, are meant to continue to apply even after the termination of this Data Processing Agreement shall continue to apply after the termination of this Data Processing Agreement. Such provisions shall include those which arise from provisions governing confidentiality, liability, dispute resolution and applicable law.

10.4. Either Party shall be entitled, without prejudice to the relevant provisions of the Agreement, to suspend the performance of this Data Processing Agreement and the associated Agreement, or to cancel it with immediate effect without judicial intervention, in the event that:

a.) the other Party is dissolved or otherwise ceases to exist;

b.) the other Party has demonstrably fallen very short in the fulfilment of the obligations arising from this Data Processing Agreement and has failed to remedy this attributable shortcoming within 30 days of the Party being served a written notice of failure to perform;

c.) a Party has been declared bankrupt or has applied for a moratorium.

10.5. Given the extent to which the Data Controller is dependent on the Processor, and given the risk of discontinued business in the event of incidents and disasters (such as a party going into liquidation), the Processor hereby declares that it is willing, at the first request of the Data Controller, to enter into additional agreements with the Data Controller so as to minimise the aforementioned risks. Such additional agreements may include (but will not be limited to):

a.) the making of arrangements regarding a periodical restoration to the Data Controller or delivery to a third party of the data processed by the Processor, and/or

b.) the conclusion of an agreement, with a third party, to the effect that the third party concerned shall be severally bound to ensure or guarantee the performance of the Agreement, and/or

c.) the conclusion of a tri-partite agreement with a third party to the effect that the third party concerned shall at all times have access to all the data required to carry out (some of) the duties to be carried out under the Agreement instead of, or in addition to, the Processor, possibly on the basis of a new agreement.

10.6. The Processor shall have an exit plan for the fulfilment of any obligations arising from this Data Processing Agreement, in the event that the Agreement or Data Processing Agreement is terminated prematurely. The Processor shall furnish the Data Controller with a copy of the aforementioned plan upon first request.

10.7. The Data Controller shall be entitled to cancel this Data Processing Agreement and the Agreement with immediate effect if the Processor indicates that it is no longer able to meet the reliability requirements to which the processing of Personal Details is subject due to developments in the law and/or the administration of justice.

10.8. The Processor must notify the Data Controller in a timely fashion prior to an intended takeover or a transfer of ownership.

10.9. The Processor is not allowed to transfer this Data Processing Agreement and the rights and obligations arising from this Data Processing Agreement to a third party without explicit written permission from the Data Controller.

Article 11. Retention period, restoration and destruction of Personal Details

11.1. The Processor shall not retain the Personal Details longer than strictly necessary, which includes the statutory retention period or any retention period agreed between the Parties, as laid down in Annex 1. Under no circumstances shall the Processor retain the Personal Details after the termination of this Data Processing Agreement. It is up to the Data Controller to decide if the data are to be retained, and if so, for how long.

11.2. When this Data Processing Agreement is terminated, or, where applicable, at the end of the agreed retention period, or upon the written request of the Data Controller, the Processor shall irrevocably destroy or cause to be destroyed the Personal Details, or restore them to the Data Controller. At the request of the Data Controller, the Processor shall submit evidence of the irrevocable destruction or removal of the data. If the data are to be restored, such shall be done electronically, in a commonly used, well-structured and documented data format. If a restoration, irrevocable destruction or removal of the data is impossible, the Processor shall notify the Data Controller of this fact at once. In such cases, the Processor shall guarantee that it shall treat the Personal Details confidentially and that it shall cease processing them.

Article 12. Intellectual property rights

12.1. If the (collection of) Personal Details is protected by any intellectual property rights, the Data Controller shall grant the Processor permission to use the Personal Details as part of the performance of this Data Processing Agreement.

Article 13. Final provisions

13.1. The recitals constitute a part of this Data Processing Agreement.

13.2. In the event that one or more provisions of this Data Processing Agreement are rendered null or void, the other provisions shall remain in force completely.

13.3. In any cases not covered by this Data Processing Agreement, the Parties shall decide on a course of action by mutual agreement.

13.4. The Processor's Agreement will be governed by Dutch law.

13.5. If any dispute should arise, the Parties shall make a concerted effort to resolve said dispute by mutual agreement. This includes the possibility of resolving the dispute by means of mediation or arbitration by a party to be determined by mutual agreement.

13.6. Disputes with regard to, or in relation to, this Data Processing Agreement shall be heard exclusively by the competent court of law or arbitrator(s) named in the Agreement.

Wetenschap Balans	BPSD Care AB
Dr. T.(Ton) J.E.M. Bakker	Richard Bibby Sales and Projects
Town/city: _____	Town/city: _____
Date:_____	Date:_____

This document is a translation of the [*Model Verwerkersovereenkomst Brancheorganisaties Zorg (Model Data Processing Agreement for the Association of Healthcare Providers (BoZ)*]
In the event that the English translation is inconsistent with the original Dutch text, the Dutch text shall prevail.

Annex 1: Agreements, description of Personal Details, the nature of the acts of processing, etc.

This Data Processing Agreement constitutes an annex to the following Agreements and relates to the following acts of processing of Personal Details.

Effective date	Reference / number / title of contract	Brief description of services	Nature of the act of processing	Type of Personal Details	Categories of Parties Involved	PURPOSES OF THE PROCESSING	Authorised sub-processors	Agreements regarding retention periods
2019-09-06	BPSD Partner Agreement.	Provision of Training and IT system for persons suffering from BPSD.	Processing of person details regarding the severity, cause and care plan of persons suffering from BPSD.	Person BSN, name, age, gender. NPI scores, Possible underlying reasons for BPSD, Other measurement scales such as MMSE, Barthel Index, PAIC, and care plan going forward.	Patients suffering from BPSD.	Research project for Balans	Hosting services shall be on a physical server located in the Netherlands.	

Annex 2: Description of other security measures

Background

1) BPSD Care shall provide Wetenschap Balans with a web based IT system for registering BPSD measurements on person living in the Netherlands.
2) This IT system forms part of the BPSD Program of Care.
3) Licenses, terms of use, support and maintenance of BPSD Program of Care and IT system are described in a separate agreement.

DPA

1) The BPSD Program of Care IT system will be installed on a server located within the Netherlands.
2) Data collected by the IT system will be held in a secure SQL server database on a server located within the Netherlands.
3) The server(s) used to deploy the IT system shall be well protected by firewalls, secure two factor login.
4) Network traffic to/from the IT system shall be encrypted.
5) User login shall be only possible using a two factor login; in this case a sms service shall be used.
6) Backups of the system database shall be made on a regular database and these backups shall be protected with the same measures employed with the live system.

Annex 3: Specification of rates

None.