Data Processing Agreement

BETWEEN:

The practice owner, (hereinafter: “**Controller**”)

AND

Insight Pharma Services B.V., a company incorporated under Dutch law, having its registered office in Apeldoorn, the Netherlands, contactable via Postbus 1534, 3800 BM Amersfoort, the Netherlands, as registered by the Dutch Chamber of Commerce under number 30231055, (hereinafter: “**Processor**”)

each individually referred to as “**Party**” and jointly referred to as “**Parties**”

AGREE TO THE FOLLOWING:

Clause 1. Subject of this Data Processing Agreement

1.1. This Data Processing Agreement applies only to the processing of personal data in connection with the subscription to meamedicapro.com pursuant to the Netherlands ICT Terms and Conditions of 2014 between the Parties (hereinafter: the “**Service Agreement**”).

1.2. In the event of a conflict between the provisions of this Data Processing Agreement and the provisions of the Service Agreement, the provisions of the Service Agreement shall prevail.

1.3. Terms such as “processing”, “personal data”, “controller” and “processor” shall have the meaning given to them in the General Data Protection Regulation (hereinafter “**GDPR**”).

Clause 2. Purposes of the processing

2.1 Processor undertakes, under the terms of this Data Processing Agreement, to process personal data on behalf of the Controller. An overview of the processing tasks that Processor will handle, the categories of personal data, and the purposes for which the personal data are processed are set out in Annex 1.

2.2 Processor shall not process the personal data other than as instructed by the Controller and shall not process the personal data for any purpose other than as specified by the Controller. Processor is allowed to make anonymized data available for scientific research on the use of medication and the associated effects. The Controller will inform Processor in writing of the processing purposes insofar as they have not yet been mentioned in this Data Processing Agreement.

2.3 The personal data to be processed on behalf of the Controller will remain the property of the Controller and/or the relevant data subjects.

Clause 3. Obligations of the Processor

3.1 With regard to the processing mentioned in Annex 1, the Processor will ensure compliance with the applicable laws and regulations, including at the very least the laws and regulations in the area of personal data protection, such as the General Data Protection Regulation.

3.2 Upon the request of the Controller, the Processor will inform Controller of the measures taken by it regarding its obligations under this Data Processing Agreement.

Clause 4. Transfer of personal data

4.1 Processor may process personal data in countries within the European Economic Area. Transfer to countries outside the European Economic Area is prohibited without the prior, explicit, and written consent of the Controller.

Clause 5. Allocation of responsibility

5.1 For the purposes of processing, Processor shall make available ICT resources to be used by the Controller for the purposes set out in this Data Processing Agreement. Processor itself performs processing operations only on the basis of separate agreements.

5.2 Processor is solely responsible for processing the personal data under this Data Processing Agreement, in accordance with the instructions of the Controller, and under the express (ultimate) responsibility of the Controller. For any other processing of personal data, including in any case, but not limited to, the collection of personal data by the Controller, processing for purposes not communicated by the Controller to the Processor, processing by third parties and/or for other purposes, Processor is expressly not responsible.

5.3 Controller guarantees that the content, use and instruction to process the personal data referred to in this Agreement are not unlawful and do not infringe any rights of third parties.

Clause 6. Security

6.1 Processor shall take appropriate technical and organizational measures to secure personal data against loss or against any form of unlawful processing (such as unauthorized access, corruption, alteration or disclosure of the personal data).

6.2 In any case, Processor has taken the following measures:

a) Logical access control using single sign-on from the secure dental information system requiring tokens consisting of an encrypted combination of the client key and a time stamp;
b) Encryption of digital files containing personal data;
c) Security of network connections via Secure Socket Layer (SSL) technology;
d) Monitoring of assigned privileges.

6.3 The measures referred to under 6.1 and 6.2, taking into account the state of the art and the costs of implementation, guarantee an appropriate level of security given the risks involved in the processing and the nature of the data to be protected. The purpose of these measures is also to prevent unnecessary collection and further processing of Personal Data.

6.4 Processor shall take the measures pursuant to the standards of ISO 27001.

6.5 Controller will only make personal data available to Processor for processing if it is satisfied that there is an appropriate level of security at Processor.

Clause 7. Notification requirement

7.1 In the event of a data breach (which is defined as: a security breach that results in a significant likelihood of adverse consequences, or has adverse consequences, for the protection of personal data that Processor processes on behalf of Controller), Processor shall notify the affected patients within 36 hours, but no later than 72 hours after the discovery of the data breach.

7.2 Processor shall provide the patients with the following information: (i) the nature of the incident; (ii) the date and time the incident occurred and was discovered; (iii) (the number of) data subjects affected by the incident; (iv) which categories of personal data are affected by the incident; and (v) the security measures – such as encryption – taken to prevent unlawful processing of the Personal Data. If at the time of the notification as described in paragraph 1 of this Clause, Processor does not yet have all of the above information, Processor shall post the missing information within a reasonable period of time.

Clause 8. Requests from data subjects

8.1 In the event that a data subject makes a request to the Processor for access, as referred to in Clause 15 of the GDPR, or for rectification, supplementation, amendment, or blocking, as referred to in Clauses 16 to 18 of the GDPR, the Processor shall forward the request to the Controller and the Controller shall process the request. Processor may notify the data subject of the forwarding.

8.2 At the request of Controller, Processor will cooperate in the handling of requests from data subjects. Controller shall bear the costs for this.

9. Engaging sub-processors

9.1. Processor may make use of a third party in the context of this Data Processing Agreement, without the need to obtain additional permission from Controller, subject to the condition that Controller can prohibit the use of the third party, provided that there are legitimate reasons justifying the prohibition.

9.2. Processor shall ensure that the sub-processor is bound by the same or equivalent obligations as those that apply to Processor under this Data Processing Agreement. Processor guarantees proper compliance with these obligations by the sub-processor and shall be liable to the Controller for any damages caused by the sub-processor as if Processor had caused the damages itself.

9.3. The engagement of sub-processors in accordance with the provisions of this Clause does not alter the fact that the involvement of sub-processors in a country outside the European Economic Area without an adequate level of protection requires permission under Clause 4.

Clause 10. Secrecy and confidentiality

10.1 Processor shall treat all Personal Data as strictly confidential and shall inform all its employees and representatives involved in the processing of the Personal Data of the confidential nature of such information and the Personal Data. Processor shall ensure that such persons have signed an adequate non-disclosure agreement.

10.2 This duty of confidentiality, as referred to in Clause 10.1, does not apply insofar as the Controller has given its prior explicit and written consent to provide the information to third parties or if the provision of the information to third parties is reasonably necessary in view of the nature of the task given and the performance of this Data Processing Agreement, or if there is a legal obligation to provide the information to a third party.

Clause 11. Audit

11.1 Controller has the right to have audits conducted by an independent third party bound by confidentiality for the purpose of verifying Processor's compliance with all obligations under this Data Processing Agreement and anything directly related to it. Controller shall not initiate an audit before it has requested and assessed the reports, certifications and other means of verification available at Processor, and has substantiated why such reports, certifications and means of verification are insufficiently conclusive as to Processor's compliance with this Data Processing Agreement. An audit initiated by Controller shall be announced at least two weeks in advance and shall take place not more than once a year.

11.2 Processor shall cooperate during the audit and shall, in a timely way, make available all information reasonably relevant to the audit, including supporting data such as system logs, and employees.

11.3 The findings resulting from the audit conducted will be assessed by the Parties in mutual consultation and, following this, may or may not be implemented by one of the Parties or by both Parties jointly.

11.4 The costs of the audit shall be borne by the Controller, unless the audit shows that the Processor is or has been culpably and substantially in breach of this Data Processing Agreement and/or any applicable legislation. In that case, the Processor shall bear half of the costs of the audit.

Clause 12. Liability

12.1 The Parties' liability vis-a-vis each other for damage as a result of attributable failure in the performance of the Data Processing Agreement, or as a result of tort or otherwise, shall be limited per event (whereby a connected series of events counts as one event) to compensation for direct damage and to the amount paid out by the insurer of the party causing the damage. The parties shall not be liable to each other for indirect damage.

12.2 Direct damage means: damage directly caused to tangible property (property damage) as well as loss or corruption of personal data of the Controller or damage to the software of the Processor, and the reasonable and demonstrable costs incurred by the party sustaining the damage in order to demand that the party sustaining the damage properly fulfil its obligations, the reasonable and demonstrable costs to determine the cause and scope of the damage the party causing the damage can be held liable for, and the reasonable and demonstrable costs incurred by the party suffering the damage to prevent or limit the damage the party causing the damage can be held liable for. Indirect damage means: all damage that is not direct damage, including loss of profit, loss of savings, reduced goodwill, damage due to business interruption and damage due to not achieving marketing objectives.

12.3 The exclusions and limitations referred to in this Clause will cease to apply if and insofar as the damage results from intent or deliberate recklessness on the part of Processor or its management.

12.4 Unless fulfilment is permanently impossible, the Parties' liability vis-à-vis each other for attributable failure in the fulfilment of the Agreement shall only arise if the Party suffering the loss gives the other Party written notice of default, in which a reasonable period for remedy of the failure is set, and the Party causing the damage continues to be in breach of its obligations after that period. The notice of default must contain as complete and detailed a description of the failure as possible, so that the Party causing the damage is given the opportunity to respond adequately.

12.5 The parties shall have and maintain adequate liability insurance in accordance with this Data Processing Agreement during the term of the Data Processing Agreement.

Clause 13. Duration, termination and amendment

13.1 This Data Processing Agreement takes effect upon the activation of the administration module and the start of the first subscription, and automatically terminates upon the termination or expiry of the Service Agreement, or the moment that Processor has erased or returned all data in accordance with Clause 13.3 – depending on whichever moment is later.

13.2 This Data Processing Agreement may only be amended in writing. The parties mutually undertake to cooperate fully and proactively in amending this Data Processing Agreement, if new or amended (privacy) laws or regulations give cause to do so.

13.3 Upon termination of this Data Processing Agreement or because of any other compelling reason, the Processor shall, upon the written request of the Controller, destroy and/or return the Personal Data to the Controller. Where a patient has activated an account on mymedicijn.nl, the data will be returned to the patient and the link with the physician will be severed. If sub-processors are involved in the processing of Personal Data, Processor shall notify them of the termination of the Data Processing Agreement and instruct them to destroy the Personal Data or transfer it to the Controller, at the Controller's discretion.

Clause 14. Applicable law and dispute resolution

14.1 The Data Processing Agreement and the performance thereof are governed by Dutch law.

14.2 All disputes which may arise between the Parties in connection with the Data Processing Agreement will be submitted to the competent court of the district of the Central Netherlands.

Annex 1:
Tasks to be performed for the processing of personal data

Processor will perform the following Processing Activities on behalf of Controller:

- Storing the data of Controller and making it available upon request, including personal data;
- Performing management activities with regard to the Controllers' patient administration.

The aforementioned Processing concerns the following category or categories of Personal Data:

- Data regarding the clients of Controller, including contact details and medical data, such as data concerning medication use, medication history, conditions, allergies, anamnesis, and data concerning treatment.

The aforementioned processing takes place for the following purposes:

- Providing online services to the Controller at the Controller's request, including data storage;
- Management with regard to the Controllers' patient administration.