Data Processing Agreement

between

The Data Controller:
Appendix D

&

The Data Processor:

RetinaLyze System A/S
CVR: 32345417
Bernstorffsvej 20
DK-2900 Hellerup
Denmark

1 Content

1. Data Processing Agreement preamble

a. This Data Processing Agreement sets out the rights and obligations that apply to the Data Processor's handling of personal data on behalf of the Data Controller.

b. This Agreement has been designed to ensure the Parties' compliance with Article 28, sub-section 3 of ***Regulation 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 and repealing Directive 95/46/EC (General Data Protection Regulation)***, which sets out specific requirements for the content of data processing agreements.

c. The Data Processor's processing of personal data shall take place for the purposes of fulfilment of the Parties' 'Master Agreement'. Nordic Contract for 2015 commencing on 6th of March 2015.

d. The Data Processing Agreement and the 'Master Agreement' shall be interdependent and cannot be terminated separately. The Data Processing Agreement may however – without termination of the 'Master Agreement' – be replaced by an alternative valid data processing agreement.

e. This Data Processing Agreement shall take priority over any similar provisions contained in other agreements between the Parties, including the 'Master Agreement'.

f. Four appendices are attached to this Data Processing Agreement. The Appendices form an integral part of this Data Processing Agreement.

g. Appendix A of the Data Processing Agreement contains details about the processing as well as the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

h. Appendix B of the Data Processing Agreement contains the Data Controller's terms and conditions that apply to the Data Processor's use of Sub-Processors and a list of Sub-Processors approved by the Data Controller.

i. Appendix C of the Data Processing Agreement contains instructions on the processing that the Data Processor is to perform on behalf of the Data Controller (the subject of the processing), the minimum-security measures that are to be implemented and how inspection with the Data Processor and any Sub-Processors is to be performed.

j. The Data Processing Agreement and its associated Appendices shall be retained in writing as well as electronically by both Parties.

k. This Data Processing Agreement shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the General Data Protection Regulation or other legislation.

2. The rights and obligations of the Data Controller

a. The Data Controller shall be responsible to the outside world (including the data subject) for ensuring that the processing of personal data takes place within the framework of the General Data Protection Regulation and the Danish Data Protection Act.

b. The Data Controller shall therefore have both the right and obligation to make decisions about the purposes and means of the processing of personal data.

c. The Data Controller shall be responsible for ensuring that the processing that the Data Processor is instructed to perform is authorised in law.

3. The Data Processor acts according to instructions

a. The Data Processor shall solely be permitted to process personal data on documented instructions from the Data Controller unless processing is required under EU or Member State law to which the Data Processor is subject; in this case, the Data Processor shall inform the Data Controller of this legal requirement prior to processing unless that law prohibits such information on important grounds of public interest, cf. Article 28, sub-section 3, para a.

b. The Data Processor shall immediately inform the Data Controller if instructions in the opinion of the Data Processor contravene the General Data Protection Regulation or data protection provisions contained in other EU or Member State law.

4. Confidentiality

a. The Data Processor shall ensure that only those persons who are currently authorised to do so are able to access the personal data being processed on behalf of the Data Controller. Access to the data shall therefore without delay be denied if such authorisation is removed or expires.

b. Only persons who require access to the personal data in order to fulfil the obligations of the Data Processor to the Data Controller shall be provided with authorisation.

c. The Data Processor shall ensure that persons authorised to process personal data on behalf of the Data Controller have undertaken to observe confidentiality or are subject to suitable statutory obligation of confidentiality.

d. The Data Processor shall at the request of the Data Controller be able to demonstrate that the employees concerned are subject to the above confidentiality.

5. Security of processing

a. The Data Processor shall take all the measures required pursuant to Article 32 of the General Data Protection Regulation which stipulates that with consideration for the current level, implementation costs and the nature, scope, context and purposes of processing and the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

b. The above obligation means that the Data Processor shall perform a risk assessment and thereafter implement measures to counter the identified risk. Depending on their relevance, the measures may include the following:

   i. Pseudonymisation and encryption of personal data
   ii. The ability to ensure 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.
   iv. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

c. The Data Processor shall in ensuring the above – in all cases – at a minimum implement the level of security and the measures specified in Appendix C to this Data Processing Agreement.

d. The Parties' possible regulation/agreement on remuneration etc. for the Data Controller's or the Data Processor's subsequent requirement for establishing additional security measures shall be specified in the Parties' 'Master Agreement'.

6. Use of Sub-Processors

a. The Data Processor shall meet the requirements specified in Article 28, sub-section 2 and 4, of the General Data Protection Regulation in order to engage another processor (Sub-Processor).

b. The Data Processor shall therefore not engage another processor (Sub-Processor) for the fulfilment of this Data Processing Agreement without the prior specific or general written consent of the Data Controller.

c. In the event of general written consent, the Data Processor shall inform the Data Controller of any planned changes with regard to additions to or replacement of other data processors and thereby give the Data Controller the opportunity to object to such changes.

d. The Data Controller's requirements for the Data Processor's engagement of other sub-processors shall be specified in Appendix B to this Data Processing Agreement.

e. The Data Controller's consent to the engagement of specific sub-processors, if applicable, shall be specified in Appendix B to this Data Processing Agreement.

f. When the Data Processor has the Data Controller's authorisation to use a sub-processor, the Data Processor shall ensure that the Sub-Processor is subject to the same data protection obligations as those specified in this Data Processing Agreement on the basis of a contract or other legal document under EU law or the national law of the Member States, in particular providing the necessary guarantees that the Sub-Processor will implement the appropriate technical and organisational measures in such a way that the processing meets the requirements of the General Data Protection Regulation.

   The Data Processor shall therefore be responsible – on the basis of a sub-processor agreement – for requiring that the sub-processor at least comply with the obligations to which the Data Processor is subject pursuant to the requirements of the General Data Protection Regulation and this Data Processing Agreement and its associated Appendices.

g. A copy of such a sub-processor agreement and subsequent amendments shall – at the Data Controller's request – be submitted to the Data Controller who will thereby have the opportunity to ensure that a valid agreement has been entered into between the Data Processor and the Sub-Processor. Commercial terms and conditions, such as pricing, that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the Data Controller.

h. The Data Processor shall in his agreement with the Sub-Processor include the Data Controller as a third party in the event of the bankruptcy of the Data Processor to enable the Data Controller to assume the Data Processor's rights and invoke these as regards the Sub-Processor, e.g. so that the Data Controller is able to instruct the Sub-Processor to perform the erasure or return of data.

i. If the Sub-Processor does not fulfil his data protection obligations, the Data Processor shall remain fully liable to the Data Controller as regards the fulfilment of the obligations of the Sub-Processor.

7. Transfer of data to third countries or international organisations

a. The Data Processor shall solely be permitted to process personal data on documented instructions from the Data Controller, including as regards transfer (assignment, disclosure and internal use) of personal data to third countries or international organisations, unless processing is required under EU or Member State law to which the Data Processor is subject; in such a case, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest, cf. Article 28, sub-section 3, para a.

b. Without the instructions or approval of the Data Controller, the Data Processor therefore cannot – within the framework of this Data Processing Agreement:
    i. disclose personal data to a data controller in a third country or in an international organisation
    ii. assign the processing of personal data to a sub-processor in a third country
    iii. have the data processed in another of the Data Processor's divisions which is located in a third country
c. The Data Controller's instructions or approval of the transfer of personal data to a third country, if applicable, shall be set out in Appendix C to this Data Processing Agreement.

8. Assistance to the Data Controller

a. The Data Processor, taking into account the nature of the processing, shall, as far as possible, assist the Data Controller with appropriate technical and organisational measures, in the fulfilment of the Data Controller's obligations to respond to requests for the exercise of the data subjects' rights pursuant to Chapter 3 of the General Data Protection Regulation.

    This entails that the Data Processor should as far as possible assist the Data Controller in the Data Controller's compliance with:

    i. notification obligation when collecting personal data from the data subject
    ii. notification obligation if personal data have not been obtained from the data subject
    iii. right of access by the data subject
    iv. the right to rectification
    v. the right to erasure ('the right to be forgotten')
    vi. the right to restrict processing
    vii. notification obligation regarding rectification or erasure of personal data or restriction of processing
    viii. the right to data portability
    ix. the right to object
    x. the right to object to the result of automated individual decision-making, including profiling

b. The Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to Articles 32-36 of the General Data Protection Regulation taking into account the nature of the processing and the data made available to the Data Processor, cf. Article 28, sub-section 3, para f.

    This entails that the Data Processor should, taking into account the nature of the processing, as far as possible assist the Data Controller in the Data Controller's compliance with:

    i. the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing
    ii. the obligation to report personal data breaches to the supervisory authority (Danish Data Protection Agency) without undue delay and, if possible, within 72 hours of the Data Controller discovering such breach unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons
    iii. the obligation – without undue delay - to communicate the personal data breach to the data subject when such breach is likely to result in a high risk to the rights and freedoms of natural persons

iv. the obligation to carry out a data protection impact assessment if a type of processing is likely to result in a high risk to the rights and freedoms of natural persons

v. the obligation to consult with the supervisory authority (Danish Data Protection Agency) prior to processing if a data protection impact assessment shows that the processing will lead to high risk in the lack of measures taken by the Data Controller to limit risk

c. The Parties' possible regulation/agreement on remuneration etc. for the Data Processor's assistance to the Data Controller shall be specified in the Parties' 'Master Agreement'.

9. Notification of personal data breach

a. On discovery of personal data breach at the Data Processor's facilities or a sub-processor's facilities, the Data Processor shall without undue delay notify the Data Controller. The Data Processor's notification to the Data Controller shall, if possible, take place within 48 hours after the Data Processor has discovered the breach to enable the Data Controller to comply with his obligation, if applicable, to report the breach to the supervisory authority within 72 hours.

b. According to Clause 9.2., para b, of this Data Processing Agreement, the Data Processor shall – taking into account the nature of the processing and the data available – assist the Data Controller in the reporting of the breach to the supervisory authority. This may mean that the Data Processor is required to assist in obtaining the information listed below which, pursuant to Article 33, sub-section 3, of the General Data Protection Regulation, shall be stated in the Data Controller's report to the supervisory authority:

i. The nature of the personal data breach, including, if possible, the categories and the approximate number of affected data subjects and the categories and the approximate number of affected personal data records

ii. Probable consequences of a personal data breach

iii. Measures which have been taken or are proposed to manage the personal data breach, including, if applicable, measures to limit its possible damage

10. Erasure and return of data

a. On termination of the processing services, the Data Processor shall be under obligation, at the Data Controller's discretion, to erase or return all the personal data to the Data Controller and to erase existing copies unless EU law or Member State law requires storage of the personal data.

11. Inspection and audit

a. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and this Data Processing Agreement, and allow for and contribute to audits, including inspections performed by the Data Controller or another auditor mandated by the Data Controller.

b. The procedures applicable to the Data Controller's inspection of the Data Processor are specified in Appendix C to this Data Processing Agreement.

c. The Data Controller's inspection of sub-processors, if applicable, shall as a rule be performed through the Data Processor. The procedures for such inspection are specified in Appendix C to this Data Processing Agreement.

d. The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or

representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

12. The Parties' agreement on other terms

a. (Separate) terms relating to the consequences of the Parties' breach of this Data Processing Agreement, if applicable, shall be specified in the Parties' 'Master Agreement'.
b. Regulation of other terms between the Parties shall be specified in the Parties' 'Master Agreement'.

13. Commencement and termination

a. This Data Processing Agreement shall become effective on the date of both Parties' signature to the Agreement.
b. Both Parties shall be entitled to require this Data Processing Agreement renegotiated if changes to the law or inexpediency of the provisions contained herein should give rise to such renegotiation.
c. The Parties' agreement on remuneration, terms etc. in connection with amendments to this Data Processing Agreement, if applicable, shall be specified in the Parties' 'Master Agreement'.
d. This Data Processing Agreement may be terminated according to the terms and conditions of termination, incl. notice of termination, specified in the 'Master Agreement'.
e. This Data Processing Agreement shall apply as long as the processing is performed. Irrespective of the termination of the 'Master Agreement' and/or this Data Processing Agreement, the Data Processing Agreement shall remain in force until the termination of the processing and the erasure of the data by the Data Processor and any sub-processors.

14. Data Controller and Data Processor contacts/contact points

a. The Parties may contact each other using the following contacts/contact points:
    i. See Appendix D.
b. The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Appendix A - Information about the processing

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

- That the Data Controller is able to use the web application which is owned and managed by the Data Processor to analyse images.

The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):

- That the Data Processor makes available RetinaLyze WebApp to the Data Controller and hereby stores personal data about the Data Controller's clients.

The processing includes the following types of personal data about data subjects:

- Name
- Social security number
- Photo of the retina
- Result of analysis

Processing includes the following categories of data subject:

- Persons who have had images uploaded through the RetinaLyze WebApp from the Data Controller

The Data Processor's processing of personal data on behalf of the Data Controller may be performed when this Data Processing Agreement commences. Processing has the following duration:

- Processing shall not be time-limited and shall be performed until this Data Processing Agreement is terminated or cancelled by one of the Parties.

Appendix B - Terms of the Data Processor's use of sub-processors and list of approved sub-processors

B.1 Terms of the Data Processor's use of sub-processors, if applicable

The Data Processor has the Data Controller's general consent for the engagement of sub-processors. The Data Processor shall, however, inform the Data Controller of any planned changes with regard to additions to or replacement of other data processors and thereby give the Data Controller the opportunity to object to such changes. Such notification shall be submitted to the Data Controller a minimum of 1 month prior to the engagement of sub-processors or amendments coming into force. If the Data Controller should object to the changes, the Data Controller shall notify the Data Processor of this within 14 days of receipt of the notification. The Data Controller shall only object if the Data Controller has reasonable and specific grounds for such refusal.

B.2 Approved sub-processors

The Data Controller shall on commencement of this Data Processing Agreement approve the engagement of the following sub-processors:

Name	CVR no.	Address	Description of processing
Amazon Web Services, Inc.	NTT0415 USASR008	410 Terry Ave North Seattle , WA 98109-5210 , US	Cloud provider of virtual servers, storage and databases in EU. All servers used to process and store information is provided by Amazon Web Services.
InSoft SL		Av.Veinticino de Julio 34, 38004 S/S de Tenerife, Spain	R&D Partner in Glaucoma Algorithm. Performs image analysis on Fundus images only.

The Data Controller shall on the commencement of this Data Processing Agreement specifically approve the use of the above sub-processors for the processing described for that party. The Data Processor shall not be entitled – without the Data Controller's explicit written consent – to engage a sub-processor for 'different' processing than the one that has been agreed or have another sub-processor perform the described processing.

Appendix C - Instruction pertaining to the use of personal data

C.1 The subject of/instruction for the processing

The Data Processor's processing of personal data on behalf of the Data Controller shall be carried out by the Data Processor performing the following:

- The Data Processor has been instructed to perform image analysis, and to deliver a result of this analysis, while storing images and results for later access.

C.2 Security of processing

The level of security shall reflect:

- That the processing involves a large volume of personal data which are subject to Article 9 of the General Data Protection Regulation on 'special categories of personal data' which is why a 'high' level of and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.
- The Data Processor shall hereafter be entitled and under obligation to make decisions about the technical.
- The Data Processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the Data Controller (on the basis of the risk assessment that the Data Controller has performed):
    - Redundant data storage.
    - Multiple incremental data backup
    - Data backups with a timetable which appropriately reflects data changes
    - Session time outs
    - Utilization of user identification credentials
    - Physical security of data processing facilities
    - Use of adequate firewall and encryption technologies to protect the gateways and pipelines through which the data travels
    - Sensitive Personal Data is encrypted during transmission using up to date versions of TLS or other security protocols using industry standard encryption algorithms and keys
    - Customer sensitive Personal Data and other confidential customer data are encrypted at rest within the system
    - Protection of data must meet legal standards for storing Personal Data.
    - All entries and changes to the Database must be logged.
    - Role-based access control implemented in a manner consistent with principle of least privilege
    - Access to host servers, applications, databases, routers, switches, etc., is logged

C.3 Storage period/erasure procedures

Personal data are stored with the Data Processor until the Data Controller requests that the data are erased or returned.

C.4 Processing location

Processing of the personal data under this Data Processing Agreement cannot be performed at other locations than the following without the Data Controller's prior written consent:

- Amazon Web Services within the EU.

C.5 Instruction for or approval of the transfer of personal data to third countries

If the Data Controller does not in this clause or by subsequent written notification provide instructions or consent pertaining to the transfer of personal data to a third country, the Data Processor shall not be entitled within the framework of this Data Processing Agreement to perform such transfer.

C.6 Procedures for the Data Controller's inspection of the processing being performed by the Data Processor

The Data Controller or the Data Controller's representative shall perform a yearly inspection with regards to the compliance of this Data Processing Agreement at the Data Processor's facilities.

In addition to the planned inspection, the Data Controller shall be entitled to inspect the Data Processor when the Data Controller deems that this is required.

The Data Controller's costs, if applicable, relating to physical inspection shall be defrayed by the Data Controller. The Data Processor shall, however, be under obligation to set aside the resources (mainly time) required for the Data Controller to be able to perform the inspection.

C.7 Procedures for inspection of the processing being performed by sub-processors, if applicable

The Data Processor shall once every year at the Data Processor's expense obtain an inspection report from an independent third party with regards to the Sub-Processor's compliance with this Data Processing Agreement and its associated Appendices.

The Parties have agreed that the following types of inspection report may be used: SOC 1 Type II Report. Inspection report shall without delay be submitted to the Data Processor and/or the Data Controller for information.

Data Controller may need to sign NDA with sub-processor, to be able to access SOC Report.

Appendix D - Company and contact information signing sheet

Date of agreement: _____

The Data Controller:

Company name: _____

Address: _____

Postcode: _____ City: _____

State: _____ Country: _____

VAT: _____

Signed on behalf of:

Company name: _____ RetinaLyze System A/S

By: By:

Name: _____ Name: Thomas Degn Nielsen

Title: _____ Title: CEO

Data Controller and Data Processor contacts/contact points:

Data Controller: Data Processor:

Contact Person: _____ Contact Person: Morten Møller

Title: _____ Title: CTO

E-mail: _____ E-mail: mom@retinalyze.com

Phone: _____ Phone: +45 71 990 321