DATA PROCESSING AGREEMENT

Last modified: 10th of July 2025

This Data Processing Agreement including its Attachment(s) ("DPA") forms an integral part of the StrokeViewer End User License Agreement (EULA) or, as applicable, the StrokeViewer User Agreement (UA) ("Agreement") between Licensor (Nicolab) and Licensee, under which Licensor provides its SaaS (software as a service) image processing application to the Licensee. Licensor and Licensee may hereinafter also be jointly referred to as "Parties" and individually as "Party".

WHEREAS

(A) The performance of the Agreement entails, inter alia, the processing of personal data as defined and governed by Regulation (EU) 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");

(B) For the processing of personal data in relation to the Agreement and under this DPA, Licensee is considered the "Controller" and Licensor (Nicolab) is considered the "Processor" who processes the Personal Data on behalf of the Controller. The Parties will be referred to as "Controller" and "Processor".

(C) The Parties seek to implement a DPA that complies with the requirements of the current legal framework in relation to data processing and with the GDPR.

1. Definitions and interpretation

1.1 All definitions used in this DPA that are not defined herein shall have the meaning set forth in the Agreement.

1.1.1 "Attachment" means an Attachment to this DPA;

1.1.2 "Data Protection Law(s)" means all laws and regulations from time to time in force relating to the protection of personal information, that are applicable to the Processing under this DPA, including (where applicable) the General Data Protection Regulation ("GDPR") in the European Union;

1.1.3 "Sub-Processor" means any non-subordinate third party hired by the Processor to help process Personal Data as part of the Agreement, not being employees.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing", "Processor" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The recitals and Attachments to this DPA form an integral and substantial part of this DPA.

2. Subject of the DPA

2.1 This DPA relates to the Processing of Personal Data by the Processor on behalf of the Controller as part of the performance of the Agreement.

2.2 This DPA constitutes an inseparable part of the Agreement. In the event of inconsistencies between the DPA and other documentation that constitute the Agreement, the DPA prevails with respect to data protection and privacy matters.

3. Processing of Personal Data

3.1 The Processor guarantees that it will only process Personal Data on behalf of the Controller on the documented instructions of the Controller unless otherwise required by the applicable law to which the Processor is subject, in which case the Processor shall inform the Controller

if this is not prohibited under that law. Where possible the Processor shall enable the Controller to defend itself against any required Processing by the Processor and shall minimize the extent of the Processing to the maximum extent possible in other respects too.

3.2 The written instructions from the Controller are specified in this DPA and its Attachments.

3.3 Subsequent instructions can be given by the Controller throughout the duration of the Processing in the context of the Agreement. Such instructions shall always be documented and kept in writing, including electronically. If the instructions are inconsistent with, directly contradict or outreach the scope of this DPA, such instructions shall be included in a written addendum, agreed by both Parties. Depending on the instructions concerned, the Processor may decide that it is necessary to amend the underlying Agreement.

3.4 The Controller has the right and obligation to make decisions about the purposes and means of the Processing of Personal Data and is responsible for ensuring compliance with the Data Protection Laws. The Processor shall follow any and all reasonable instructions provided by the Controller with regard to the Processing of the Personal Data. The Processor shall notify the Controller at once if it feels that said instructions constitute a violation of Data Protection Laws. In such case, the Controller has thirty (30) days to revise its written instructions. If the Controller does not provide revised instructions within thirty (30) days or if the Processor deems the revised instructions to violate Data Protection Laws, the Processor has the right to terminate (the relevant part of) the Agreement.

3.5 The Processor shall demonstrably process the Personal Data in a proper and diligent manner, in accordance with the requirements to which it is subject under the Data Protection Laws. As far as this is concerned, the Processor shall at least establish a register of acts of Processing within the meaning of article 30(2) of the GDPR and furnish the 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 categories of Personal Data, the Processor shall guarantee that its procedures shall not violate any applicable health care legislation it is aware of.

4. Security

4.1 Taking 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, the Parties shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, which shall be in accordance with the nature of the Personal Data to be processed, as specified in Attachment 1. These security measures shall include any measures stipulated in the DPA. At the very least, the measures implemented by the Processor shall include the following:

a) measures designed to guarantee that only authorized employees can access the Personal Data for the purposes outlined in Attachment 1;

b) measures involving the Processor only granting its employees and Sub-Processors access to Personal Data 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 Data whose access is necessary for the legal person concerned;

c) measures designed to protect the Personal Data from unintentional or unlawful destruction, unintentional loss or changes and unauthorized retention, Processing, access or disclosure;

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

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

4.2 The Processor's methods demonstrably comply with the requirements of ISO27001, ISO13485 and NEN7510. Processor works with a software development process according to IEC62304 and also follows the risk management standard ISO14971 for Medical Devices and the security standard IEC82304 for medical software. The Processor has implemented an appropriate, written security policy for the Processing of Personal Data.

4.3 The Controller may request the Processor to implement further security measures. Processor shall be required to implement the requested security measures after the Parties have agreed upon them in writing. If the Processor makes any adjustments to its security measures at the Controller's request, the Processor is entitled to invoice the Controller for the costs associated with said adjustments.

4.4 The Processor shall be entitled to enhance or adjust the security measures it has implemented if to its discretion such is necessary for a continued provision of an appropriate level of security. Processor shall inform Controller of any material changes to the security measures before implementing them.

4.5 Although the Controller remains responsible for the implementation of appropriate technical and organizational security measures, the Processor is responsible for the more practical aspects of the implementation of these security measures (the "non-essential means"), such as the choice for a particular type of hard- or software or the detailed security measures. The Processor shall assist the Controller in determining which security measures are appropriate if the Controller requests such assistance.

4.6 The Processor shall only grant access to the Personal Data under this DPA on a need to know basis to persons under the Data Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Sub-Processing

5.1 The Processor shall only outsource activities which involve or require the Processing of Personal Data to a Sub-Processor after prior authorization by the Controller. The Controller hereby provides its authorization to engage the Sub-Processors listed in Attachment 1.

5.2 The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-Processors at least thirty (30) days prior to commencing the sub-processing. The Controller can then object to the change during a timeframe of fifteen (15) days after receiving the information. The Controller can only object on reasonable grounds. In case of objection the Parties will consult with each other about a solution deemed agreeable by both Parties. If Parties cannot agree, either Party may terminate the affected part of the Agreement. If the Controller does not object to the proposed change during the timeframe of fifteen (15) days, the Controller shall be deemed to have provided authorization.

5.3 Any Sub-Processor(s) appointed by the Processor will at least comply with the provisions of this DPA and all obligations arising from the Data Protection Laws.

6. Personal Data Breach and assistance obligations

6.1 Taking into account the nature of the Processing, Processor shall assist the Controller by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Controller obligations, as reasonably understood by Controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 If Processor discovers a Personal Data Breach, Processor will notify the Controller as soon as possible, but within 72 hours at the latest. If there is a Personal Data Breach, Parties will make efforts within the scope of this DPA to prevent (further) loss or unlawful Processing of Personal Data and to prevent any repetition. In the event of a Personal Data Breach, the Parties will take all reasonable measures to limit the consequences of the Personal Data Breach and/or prevent a new one. The Processor shall provide all reasonable assistance to Controller in respect of notifying the relevant Supervisory Authority upon the Controller request.

6.3 The Processor shall provide reasonable assistance to the Controller in relation to Data Protection Impact Assessments, Prior Consultation and/or requests from the Supervisory Authority upon the Controller's request. The Processor shall reasonably cooperate with any investigation and/or request from the Supervisory Authority in consultation with the Controller.

6.4 The Processor shall be entitled to invoice the Controller for any costs it incurs in implementing the measures or providing assistance or cooperation as referred to in this article.

7. Duration and termination

7.1 This DPA comes into effect on the date of last signature of the Proposal, and will stay in force for the duration of the Processing under the Agreement.

7.2 Termination of the Agreement on any grounds whatsoever (termination/cancellation) shall result in the DPA being terminated on the same grounds (and vice versa), unless the Parties agree otherwise (as appropriate).

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

7.4 The Processor is not allowed to transfer this DPA and the rights and obligations arising from this DPA to a third party without explicit written permission from the Controller.

8. Retention period and/or deletion of Personal Data

8.1 The Processor shall not retain the Personal Data longer than strictly necessary, which includes the retention period agreed between the Parties, as laid down in Attachment 1.

8.2 When this DPA is terminated, or, where applicable, at the end of the agreed retention period, or upon the written request of the Controller, the Processor shall terminate its Processing.

8.3 The standard data retention term applied by the Processor is thirty (30) days and six (6) years for log records from the moment the Processing of that Personal Data under this DPA commences. A shorter retention term can be implemented upon the request of the Controller. After the data retention term lapses the Personal Data is automatically deleted. If the Controller wants to receive a copy of the Personal Data before it is deleted it can timely request this to be configured. The aforementioned data retention policy also applies in case of termination of the DPA, meaning that the Personal Data Processed under the DPA will be automatically deleted thirty (30) days after it first being Processed or six (6) years for log records. If the Controller wants to receive a copy of the Personal Data available at the moment of termination, it must request that thirty (30) days prior to the termination taking effect.

8.4 At the request of the Controller, the Processor shall submit evidence of the irrevocable destruction or removal of the Personal Data Processed under this DPA. If a copy of the Personal Data are to be provided to the Controller, such shall be done electronically, in a

commonly used, well-structured and documented data format. If providing a copy or irrevocable destruction or removal of the Personal Data is impossible, the Processor shall notify the Controller of this fact at once. If the Processor incurs any costs for providing evidence or providing a copy of Personal Data to the Controller, it shall be entitled to invoice the Controller.

9. Audit rights

9.1 Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this DPA. Processor shall allow for and contribute to audits, including inspections, at reasonable intervals, by the Controller or an auditor mandated by the Controller in relation to the Processing of the Personal Data provided that it is timely informed about such audits and confidentiality is guaranteed. The results or report of the audit shall be shared with the Processor.

9.2 Information and audit rights of the Controller only arise under article 9.1 to the extent that the DPA does not otherwise give Controller information and audit rights meeting the relevant requirements of Data Protection Laws.

9.3 If necessary, the Parties shall consult each other on the findings of the audit and implement measures for improvement.

9.4 The Processor shall be entitled to invoice the Controller for any costs it incurs in relation to its contributions to an audit and/or in implementing the measures pursuant to it.

10. Liability

10.1 In addition to the Agreement, the Parties are each responsible and liable for their own actions. The Parties are liable for and indemnify each other mutually against all claims, actions, fines, claims of the Data Subject, authorities and other third parties, which are caused by or arise directly from an attributable failure in the fulfillment of its obligations under this DPA and Data Protection Laws. Any limitation of liability will furthermore cease to apply to the Party concerned in the event of willful intent or gross negligence on the part of the Party concerned.

10.2 Each Party shall only be liable towards the other Party to the extent that the Party claiming liability informs the potentially liable Party of the event causing the liability immediately but at least within six (6) months from becoming aware of the event itself. Each Party shall provide all reasonable cooperation and assistance to limit any damages.

10.3 The Parties shall ensure that their liability is sufficiently covered by insurance.

11. Data transfer

11.1 The Processor shall only transfer Personal Data in compliance with the Data Protection Laws and following the instructions of the Controller.

11.2 The Data Controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Attachment 3. Where required, the Parties shall adopt appropriate additional (contractual) safeguards to ensure an adequate level of protection of the Personal Data.

11.3 If the Controller is located outside the European Economic Area or will use the Processor's SaaS application in a country outside the European Economic Area. The Controller shall enter into a data transfer agreement based on the Standard Contractual Clause as approved by the European Commission for transfers of Personal Data from a EU Processor to a Controller in a third country, unless another valid transfer mechanism applies.

12. Miscellaneous

12.1 Each Party must keep this DPA and information it receives about the other Party and its business in connection with this DPA ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain;

(c) is in its possession prior to this DPA;

(d) is received by it from a third party without breach of an obligation of confidentiality to the other Party.

12.2 All notices and communications given under this DPA must be in writing and will be delivered personally, sent by post or sent by email to the address or at such other address as notified from time to time by the Parties changing address.

12.3 Nicolab has appointed a data protection officer who can be contacted at: infosec@nicolab.com or +31 20 244 08 52.

12.4 Nicolab reserves the right, in its sole discretion, to amend or update this DPA at any time. In case of amendments or updates Nicolab will notify the Controller.

12.5 An amendment shall become effective and become part of the Controller's instructions thirty (30) days after notifying the Controller. If the Controller does not consent to an amendment notified by Nicolab, the Controller shall inform Nicolab thereof in writing no later than fifteen (15) days after receiving the notification of the amendment. The Parties will reasonably cooperate to resolve any disagreement. Either Party can terminate the (relevant part of the) Agreement if the Parties cannot come to an agreement.

13. Governing law and jurisdiction

13.1 This DPA shall be governed and construed solely in accordance with the laws of the country in which the Processor is located, and the Parties irrevocably submit to the jurisdiction of the courts of that country and to the appeal courts from them.

Attachment 1 – Personal Data Processing details

Description of services	The Processor (Nicolab) provides a Software as a Service (SaaS) image processing application that can display and/or analyze medical (imaging) information. The application automatically analyzes eligible scans received from patients. After the analysis, a report is generated that includes relevant features of the images. The available information is (remotely) accessible to physicians on workstations and mobile devices to support the clinical workflow. 1. (Automatic) analysis of DICOM images using StrokeViewer Algorithms 2. Web DICOM viewer 3. Mobile DICOM viewer 4. Network-wide image sharing 5. Instant messaging 6. Technical support in case of malfunctions or in other cases when deemed necessary 7. Training services
Type of Personal Data	Scans, these (may) contain patient information, including special categories* of Personal Data, such as name, date of birth, patient ID, gender and other DICOM information defined by Data Controller and stroke specific clinical scores (NIHSS and mRS), and any other relevant clinical information.
Categories of those involved	Patients and users of the application.
Purposes of Processing	Processing will only take place in the context of and for the duration of the Agreement for the purpose of: - Service Provision - Communication - Diagnostics and Troubleshooting - Personalization and Customization - Analytics and Research - Legal Compliance
Approved Sub-Processors	Google Cloud, AWS, Stream.io
Retention period	Patient data: Shall be retained for a maximum of 30 days from the moment of submitting the data. The default retention period will be set to 14 days unless the Controller explicitly requests a shorter duration. The log record is kept during the term of the Agreement with the Controller, with a maximum of 6 years.

**Special categories of Personal Data as defined in Data Protection Laws.*

Attachment 2 – Data Transfer Instructions

On commencement of the DPA, the Controller authorises the Processor to perform the following Data Processing operations outside de EEA based on the mechanism to legitimise such transfer as included in the schedule below.

(SUB)-PROCESSOR	THIRD COUNTRY	MECHANISM TO LEGITIMIZE TRANSFER
Google Cloud	World-wide including USA	Standard Contractual Clauses
AWS	World-wide including USA	Standard Contractual Clauses
Stream.io	World-wide including USA	Standard Contractual Clauses