DATA PROCESSING AGREEMENT

Last modified: 17th of May 2024

This Data Processing Agreement including its Attachment(s) forms an integral part of the Agreement between Customer and Nicolab, under which Nicolab provides its SaaS (software as a service) image processing application to the Customer. Nicolab and Customer may hereinafter also be jointly referred to as "Parties" and individually as "Party".

WHEREAS

(A) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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) In the remainder of this Data Processing Agreement, Customer is considered the "Controller" and Nicolab is considered the "Processor" who processes the Personal Data on behalf of the Controller.

1. DEFINITIONS AND INTERPRETATION

1.1 All definitions used in this Data Processing Agreement that are not defined herein shall have the meaning set forth in the Terms and Conditions.

1.1.1. "Attachment" means an Attachment to this Data Processing Agreement;

1.1.2. "Data Protection Law(s)" means all applicable laws and regulations from time to time in force relating to the protection of personal information, including (where applicable) the "GDPR" General Data Protection Regulation in the European Union, "UK-GDPR" General Data Protection Regulation in the United Kingdom and Data Protection Act (Data Processing Agreement) 2018, "HIPAA" Health Insurance Portability & Accountability Act in the United States of America, Privacy Act 1988 of Australia, Privacy Act 2020 of New Zealand, New Federal Act on Data Protection (nFADP) of Switzerland, Thailand Personal Data Protection Act and the Personal Data Protection Act of Taiwan.

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.

2. SUBJECT OF THE DATA PROCESSING AGREEMENT

2.1 This Data Processing Agreement 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 Data Processing Agreement constitutes an inseparable part of the Agreement. In the event of inconsistencies between the Data Processing Agreement and other documentation that constitute the Agreement, the order of priority as stated in the Terms and Conditions shall be followed.

3. PROCESSING OF PERSONAL DATA

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

a) such is necessary for the performance of the Agreement within the scope specified in Attachment 1 of this Data Processing Agreement; or
b) the 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 Data specified in Attachment 1 exclusively for the purposes and in the manner described in said Attachment.

3.3 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.

3.4 Without prejudice to the provisions of article 3.1, the Processor shall be allowed to process Personal Data 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 Controller of the intended Processing of the Personal Data and of the statutory provision prior to the Processing, unless it is barred by said legislation from notifying the Controller beforehand for pressing reasons protecting the common good. Where possible the Processor shall enable the Controller to defend itself against such enforced Processing and shall minimize the extent of the enforced processing to the maximum extent possible in other respects too.

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 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 Personal Data, the Processor shall guarantee that its procedures shall not violate health care legislation.

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, Processor 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 which may be stipulated in the Data Processing Agreement. At the very least, the measures 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.

5. SUB-PROCESSING

5.1 The Processor shall not outsource activities which involve or require the Processing of Personal Data to a Sub-Processor subject to prompt prior notification. The foregoing does not apply to the Sub-Processors listed in Attachment 1.

5.2 The Sub-Processor(s) appointed by the Processor will at least comply with the provisions of this Data Processing Agreement and all obligations arising from the Data Protection Laws.

6. PERSONAL DATA BREACH AND NOTIFICATION OBLIGATION

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 Data Processing Agreement to prevent (further) loss or unlawful Processing of Personal Data and to prevent any repetition. In the event of a Personal Data Breach, Processor will take all reasonable measures to limit the consequences of the Personal Data Breach and/or prevent a new one, against payment of the reasonable costs by the Controller.

7. DURATION AND TERMINATION

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

7.2 Termination of the Agreement 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).

7.3 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.

7.4 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 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 statutory retention period or any retention period agreed between the Parties, as laid down in Attachment 1. Under no circumstances shall the Processor retain the Personal Data after the termination of this Data Processing Agreement.

8.2 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 Controller, the Processor shall irrevocably destroy or cause to be destroyed the Personal Data, or restore them to the Controller. At the request of the 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 Controller of this fact at once. In such cases, the Processor shall guarantee that it shall treat the Personal Data confidentially and that it shall cease Processing them.

9. AUDIT RIGHTS

9.1 Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this Data Processing Agreement, and shall allow for and contribute to audits, including inspections, by the Controller or an auditor mandated by the Controller in relation to the Processing of the Personal Data.

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

10. LIABILITY

10.1 In addition to the Agreement, the Parties are each responsible and liable for their own actions. The Parties 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 Data Processing Agreement 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 The Parties shall ensure that their liability is sufficiently covered.

11. DATA TRANSFER

11.1 Unless it has been granted prior explicit written permission to do so by the Controller, the Processor shall not process Personal Data outside of the scope of the applicable Data Protection Laws.

11.2 When the Agreement is executed by Nico.LAB International Limited or Nicolab Inc., Processor is authorized to engage NICo-Lab B.V. established in the Netherlands, in the context of the provision of the services. Where required, the Parties shall adopt appropriate additional (contractual) safeguards to ensure an adequate level of protection of the Personal Data.

12. GENERAL TERMS

12.1 Each Party must keep this Data Processing Agreement and information it receives about the other Party and its business in connection with this Data Processing Agreement ("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 Data Processing Agreement;
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 Data Processing Agreement 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 Data Processing Agreement at any time. Nicolab will notify the Customer of updates with notifications to Customers who have provided their email address for such purpose and by posting the update of the Data Processing Agreement on www.nicolab.com. The Customer should review this Data Processing Agreement periodically.

12.5 An amendment shall become effective thirty (30) days after notifying the Customer. If Customer does not consent to an amendment notified by Nicolab, the Customer shall inform Nicolab thereof in writing no later than thirty (30) days after receiving the notification of the amendment.

13. GOVERNING LAW AND JURISDICTION

13.1 This Data Processing Agreement shall be governed and construed solely in accordance with the laws of the country in which Nicolab 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	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
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 and/or AWS and Stream.io
Retention period	Patient data: 30 days The log record is kept as long as the contract with Customer is valid but not longer than 6 years

**Special categories of Personal Data as defined in Data Protection Laws applicable to the operations under this Data Processing Agreement.*