DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is an agreement between AIRS Medical, Inc. ("**AIRS**" or "**Processor**") and Customer ("**Controller**"), and is an integral part of and subject to the terms and conditions of the Limited Evaluation Agreement or the Subscription Agreement, as applicable (each individually, the "Agreement"), governing the use of the AIRS Evaluation Product or the AIRS Service, respectively. Controller and Processor may be referred to in this DPA individually as a "Party" or collectively as "Parties."

This DPA shall be effective as of the date of Customer's accepting this Agreement (the "**DPA Effective Date**").

Capitalized terms used but not defined in this DPA shall have the meaning given to them in the Limited Evaluation Agreement/Subscription Agreement, or in GDPR (as defined below).

1. Subject of the DPA

The Processor is an AI tech company based in Republic of Korea. The core product of the Processor is SwiftMR, an MRI enhancement software built upon deep leaning technology that can be used to run MRI exams at accelerated scan times. The Processor is providing SwiftMR to the Controller in form of a cloud-based Software-as-a-Service solution in accordance with the Agreement between the Controller and the Processor. For the provision of SwiftMR it is necessary that the Processor is processing personal data on behalf of the Controller ("**Controller Data**"). This DPA governs the rights and obligations of the Parties with regard to the data processing in connection with the provision of SwiftMR.

2. Scope of the commissioning

2.1. The Processor shall process the Controller Data on behalf and in accordance with the instructions of the Controller within the meaning of Art. 28 GDPR. The Controller remains the controller in terms of data protection law.

2.2. The processing of Controller Data by the Processor occurs in the manner and the scope and for the purpose determined in **Appendix 1** to this DPA; the processing relates to the types of personal data and categories of data subjects specified therein. The duration of the processing corresponds to the duration of the Agreement and, in addition, to the duration for which the parties are subject to legal retention obligations.

2.3. The Processor reserves the right to anonymize or aggregate the Controller Data so that it is no longer possible to identify individual data subjects and to use it in this form for the purpose of demand-oriented design, further development and optimization as well as the provision of the service agreed in accordance with the Contract. The parties agree that anonymized or aggregated Controller Data in accordance with the above provision shall no longer be considered Controller Data within the meaning of this agreement.

2.4. The processing of Controller Data by the Processor shall in principle take place inside the European Union or another contracting state of the European Economic Area (EEA). The Processor is nevertheless permitted to process Controller Data in accordance with the provisions of this DPA outside the EEA if he informs the Controller in advance about the place of data processing and if the requirements of Art. 44 to 48 GDPR are fulfilled or if an exception according to Art. 49 GDPR applies.

3. Right of the Controller to issue instructions

3.1. The Processor processes the Controller Data only in accordance with the instructions of the Controller, unless the Processor is legally required to do otherwise by EU or Member State law to which the Processor is subject. In the latter case, the Processor shall inform the Controller of that legal requirement before processing, unless that EU or Member State law prohibits such information on important grounds of public interest.

3.2. The instructions of the Controller are in principle conclusively stipulated and documented in the provisions of this DPA and the Contract. Individual instructions which deviate from the stipulations of this DPA and the Agreement or which impose additional requirements shall require the Processor´s consent and must be documented by the Controller. Additional costs incurred by the Processor as a result thereof shall be borne by the Controller. Instructions of the Controller shall be made in writing.

3.3. The Processor shall ensure that the Controller Data is processed in accordance with the instructions given by the Controller. If the Processor is of the opinion that an instruction given by the Controller infringes the provisions of this DPA or applicable data protection law, the Processor shall notify the Controller immediately. The Processor is after correspondingly informing the Controller entitled to suspend the execution of the instruction until the Controller confirms the instruction. The Parties agree that the sole responsibility for the processing of the Controller Data in accordance with the instructions lies with the Controller.

4. Legal Responsibility of the Controller

4.1. The Controller is solely responsible for the permissibility of the processing of the Controller Data. Should third parties assert claims against the Processor based on the processing of Controller Data in accordance with this agreement, the Controller shall indemnify the Processor from all such claims upon first request.

4.2. The Controller shall inform the Processor immediately and completely if during the examination of the of the Processor´s results he finds errors or irregularities with regard to data protection provisions or his instructions.

4.3. On request, the Controller shall provide the Processor with the information specified in Art. 30 para. 2 GDPR, insofar as it is not available to the Processor himself.

4.4. If the Processor is required to provide information to a governmental body or person on the processing of Controller Data or to cooperate with these bodies in any other way, the Controller is obliged at first request to assist the Processor in providing such information and in fulfilling other cooperation obligations.

5. Requirements for personnel and systems

The Processor shall only grant persons access to Controller Data insofar as this is necessary for the fulfillment of a specific task by this person (need-to-know principle). The Processor shall obligate all persons who process Controller Data to maintain confidentiality with regard to the processing of Controller Data in writing and provide evidence of this obligation to the Controller upon request.

6. Security of processing

6.1. The Processor implements necessary, appropriate technical and organizational measures, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the Controller Data, as well as the different likelihood and severity of the risk to the rights and freedoms of the data subjects, in order to ensure a level of protection of Controller Data appropriate to the risk in accordance with Art. 32 GDPR. **Appendix 3** of this DPA lists the technical and organizational measures that the Processor has implemented in order to be able to guarantee adequate security of the data processing.

6.2. The Processor shall have the right to modify technical and organizational measures during the term of the Agreement, as long as they continue to comply with the statutory requirements.

6.3. The Processor shall be permitted to implement alternative adequate technical and organizational measures provided that the security level of the technical and organizational measures specified in **Appendix 4** is not impaired.

7. Engagement of further processors

7.1. The Controller grants the Processor the general authorization to engage further processors with regard to the processing of Controller Data. Further processors engaged at the time of conclusion of the agreement result from **Appendix 2**.

7.2. The Processor shall notify the Controller of any intended changes in relation to the engagement or replacement of further processors 4 weeks prior to an intended change. The Controller has the right to object to the engagement or replacement of a further processor. Insofar as the Controller does not object within 14 days after receipt of the notification, the further subprocessor shall be deemed as accepted by the Controller. If the Controller objects, the Processor is entitled to terminate this agreement with a notice period of 2 months.

7.3. The agreement between the Processor and the further processor must impose the same obligations on the latter as those set out in this DPA by way of a written contract. Should the further processor fail to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for ensuring that the further processor complies with all obligations.

8. Data subjects' rights

Taking into account the nature of the data processing, the Processor shall support the Controller with appropriate technical and organizational measures in order to fulfil its obligation to respond to requests, made by a data subject, to exercise their rights as set out in Chapter III of the GDPR (taking into account data subjects' rights with regard to ensuring transparency; the right of access to personal data; right of rectification; right to erasure of data; right to limitation of the processing; right of notification in the event of rectification, erasure, and restriction of the processing; the right to data portability; right of objection; the rights in the event of auto-mated individual decisions).

9. Notification and support obligations of the Processor

9.1. The Processor shall support the Controller upon request in complying with the obligations specified in Art. 32 to 36 GDPR, with due regard to the nature of the processing and the information available to them (ensuring security of processing, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject, data protection impact assessment, and prior consultation).

9.2. If the Processor becomes aware of a personal data breach within the meaning of Art. 4 No. 12 GDPR and the breach concerns Controller Data, the Processor shall notify the controller without undue delay after becoming aware of such an incident. The Processor shall provide the Controller with sufficient information to enable the Controller to comply with any possible notification or information obligations with respect to the supervisory authority as well as with respect to the data subjects. The information should contain, to the extent possible, a description of the nature of the breach, the measures taken or proposed by the Processor to remedy the breach and, where appropriate, measures to mitigate their potential adverse effects.

10. Deletion and return of Controller Data

10.1. The Processor shall delete or return the Controller Data upon termination of this DPA, unless the Processor is obligated by EU or Member State law to further store the Controller Data.

10.2. The deletion of Controller Data must be confirmed to the Controller in writing or in a documented electronic format, stating the date.

11. Evidence and audits

11.1. The Processor shall provide the Controller, at the latter´s request, with all information required and available to the Processor to prove compliance with his obligations under this DPA.

11.2. The Controller shall be entitled to audit the Processor with regard to compliance with the provisions of this DPA, in particular the implementation of the technical and organizational measures; including by means of on-site inspections.

11.3. In order to carry out inspections in accordance with Section 11.2., the Controller is entitled to access the business premises of the Processor in which Customer Data is processed within the usual business hours (Mondays to Fridays from 10 a.m. to 6 p.m. local time) after timely advance notification in accordance with Section 11.5 at his own expense, without disruption of the course of business and under strict secrecy of the Processor´s business and trade secrets.

11.4. The Processor is entitled, at his own discretion and taking into account the legal obligations of the Controller, not to disclose information which is sensitive with regard to the Processor´s business or if the Processor would be in breach of statutory or other contractual provisions as a result of its disclosure. The Controller is not entitled to get access to data or information about the Processor´s other customers, cost information, quality control and contract management reports, or any other confidential data of the Processor that is not directly relevant for the agreed audit purposes.

11.5. If reasonable, the Controller shall inform the Processor in good time (usually at least two weeks in advance) of all circumstances in relation to the performance of the audit. The Controller may carry out one audit per calendar year. Further audits are carried out against reimbursement of the costs and after consultation with the Processor, unless the audit has been expressly instructed by the competent supervisory authority or if the audit is required due to a data breach.

11.6. If the Controller commissions a third party to carry out the audit, the Controller shall obligate the third party in writing the same way as the Controller is obliged vis-à-vis the Processor according to this Section 11 of this DPA. In addition, the Controller shall obligate the third party to maintain secrecy and confidentiality, unless the third party is subject to a professional obligation of secrecy. At the request of the Processor, the Controller shall immediately submit to him the commitment agreements with the third party. The Controller may not commission any of the Processor´s competitors to carry out the audit.

11.7. Notwithstanding the Controller's right to conduct audits (including on-site inspections), the Parties agree that prior to any on-site inspection, to avoid unnecessary on-site inspections, the Parties will consult with each other and discuss whether alternative evidence of compliance with the obligations under this DPA may be provided by the Processor, e.g., an appropriate, up-to-date audit certificate or report by an independent body (e.g. auditor, reviewer, data protection officer, IT security department, data protection auditors or quality auditors), or by appropriate IT security or data protection certification. If such alternative evidence is available, the parties agree that such alternative evidence shall be preferred over the on-site inspection, provided the alternative evidence adequately enables the Controller to verify compliance with the contractual obligations and that there are no compelling reasons to the contrary in the individual case (e.g., an administrative order by the competent supervising authority).

12. Contract term and termination

The term and termination of this DPA shall be governed by the term and termination provisions of the Agreement. A termination of the Agreement automatically results in a cancellation of this DPA. An isolated termination of this DPA is excluded.

13. Liability

13.1. The Processor´s liability under this agreement shall be governed by the disclaimers and limitations of liability provided for in the Agreement. As far as third parties assert claims against the Processor which are caused by the Controller´s culpable breach of this DPA or one of his obligations as the Controller in terms of data protection law affecting him, the Controller shall upon first request indemnify and hold the Processor harmless from these claims.

13.2. The Controller undertakes to indemnify the Processor upon first request against all possible fines imposed on the Processor corresponding to the Controller´s part of responsibility for the infringement sanctioned by the fine.

14. Local law specifics

In case there apply necessary requirements to those set out in this DPA under local laws to which the Controller is subject, such requirements are included in **Appendix 4** to this DPA. The additional requirements set out in **Appendix 4** to this DPA are only applicable on an individual basis per country.

15. Final provisions

15.1. In case individual provisions of this DPA are ineffective or become ineffective or contain a gap, the remaining provisions shall remain unaffected. The Parties undertake to replace the ineffective provision by a legally permissible provision which comes closest to the purpose of the ineffective provision and that thereby satisfies the requirements of Art. 28 GDPR.

15.2. In case of conflicts between this DPA and other arrangements between the Parties, in particular the Agreement, the provisions of this DPA shall prevail.

Appendix 1 Purpose, type and extent of the processing of Controller Data, types of personal data and categories of data subjects

Purpose of data processing	Processing of Personal Data in connection with Controller’s use of AIRS Limited Evaluation and/or Subscription Service under the terms and conditions of the Limited Evaluation Agreement or the Subscription Agreement.
Type and extent of data processing	• Retrieving, altering, transmitting and destroying MRI DICOM files through SwiftMR • Collecting and storing usage data and user feedback on product/service
Categories of personal data	• personally identifiable information (e.g. patient name, patient ID, user name, user ID) • statistical or other usage data observed on the product (e.g. via analytics, services etc.)
Categories of data subjects	Controller’s patients and employees

Appendix 2 Further Processors

1. Third-Party Sub-Processors

Company	Purpose	Applicable Service	Data Processing Location
Amazon Web Services, Inc.	Hosting & Infrastructure	Used as on-demand cloud computing platforms and APIs	For customers in EU: Germany
Salesforce	CRM functionality	Used to store product usage and case history of customers	Japan

2. AIRS Affiliate Sub-Processors

To help AIRS deliver the Subscription Service, we engage AIRS Affiliates as Sub-Processors to assist with our data processing activities. By agreeing to the DPA, you agree all of these Sub-Processors may have access to Customer Data.

Company	Purpose	Location
AIRS Medical USA, Inc.	Service & Support	United States

Appendix 3 Technical and organizational measures

The Processor shall take the following measures:

1. Pseudonymization

Pseudonymisation ensures that personal data can only be assigned to a specific person if additional information is called in. The following measures are implemented to ensure pseudonymisation:

- The data subject's patient name and ID will be removed from the MRI DICOM file prior to uploading the file to the Processor's software and will be replaced by a unique identifier ID.

2. Encryption measures

Encryption protects the data from unauthorized access by third parties. Data is protected by encryption during transport and storage. Specifically, the following measures are in place:

- The transmission of data between the Controller and the Processor is only carried out in encrypted form (secure data transmission via SSL, TLS). The permitted encryption procedures are selected according to current technological standards.
- If data is stored on hard disk, it is always encrypted according to the current technological standards.

3. Measures to ensure confidentiality

In addition to encryption, other measures are taken to ensure the confidentiality of personal data. A regular distinction is made between measures for physical access, system access and data access control:

(a) Physical access control

Physical access control measures ensure that unauthorised persons cannot gain physical access to buildings or individual rooms in which personal data is processed. In particular, the following measures are in place:

- physical access-controlled and fenced area
- centrally authorized access for physical access control
- burglar alarm system
- video surveillance system (internal and external)

(b) System access control

The system access control measures ensure that unauthorized use of the systems processing personal data is not possible. In particular, the following measures are in place:

- personal and individual user log-in when logging into the system or company network
- authorization process for system access authorizations
- limitation of authorized users
- password procedures (high complexity due to corresponding keys)
- token
- two-factor authentication
- logging of system access
- firewall

(c) Data access control

The data access control measures ensure that only authorized persons can process the respective personal data within the system. Specifically, employees are only given data access to the personal data that they require to carry out their tasks in the Processor's company. In particular, the following measures are in place:

- administration and documentation of differentiated authorizations
- annual re-certifications of the authorisations
- logging of data access
- profiles/roles

4. Measures to ensure integrity

To protect personal data against unlawful or unwanted alteration or deletion, technical and organizational measures are taken to ensure integrity. In particular, the following measures are in place:

- data access rights
- ensuring integrity by encrypting stored data
- system-side logs
- functional responsibilities, organizationally defined responsibilities

5. Measures to ensure and restore availability

Personal data is protected from accidental or deliberate destruction, or loss, by measures to ensure and restore availability. The measures are chosen in such a way that potentially damaging events that could result in the loss of data (e.g. viruses, overheating) are averted preventively, and also, in the event of an incident, so as to restore the data as comprehensively as possible. In particular, the following measures are in place:

- security concept for software and IT applications
- installation of an uninterruptible power supply (UPS)
- protection against malware
- firewall
- contingency plan

6. Measures to ensure resilience

In order to prevent unauthorized access, or the loss or alteration of personal data, data processing systems must be resilient. Specifically, the following measures are in place:

- redundant power supply
- sufficient capacity of IT systems and equipment

7. Measures to ensure effectiveness control

The effectiveness control measures are used to regularly review the implemented security measures. If measures are no longer up-to-date or, for other reasons, are no longer sufficient, they will be rectified or replaced. In particular, the following measures are in place:

- procedures for regular inspections/audits

8. Instruction control / contract control

In principle, the measures of instruction and contract control serve to ensure that the processor adheres to the instructions of the Controller when rendering his services, as well as to regularly check the activities of the further contractors involved and to ensure that they only process the personal data in accordance with the instructions given. At present, the Processor engages the further processors mentioned in **Appendix 2**. The Processor has obligated and sensitised his own employees to confidentiality.

Appendix 4 Local law specifics

Germany

The Parties are aware that data from the area of medical treatment that are processed under this DPA are subject to the special protection of secrecy under Section 203 of the German Criminal Code (*Strafgesetzbuch* – "**StGB**").

In addition to Sec. 5 of this DPA, the Processor shall ensure that all employees involved in the processing of the Controller's and all other persons working for the Processor (e.g. further processors) who are involved in the processing have undertaken in text form not to disclose without authorization the professional secrets of which they become aware in the course of or on the occasion of their work and that they have been informed of the possible criminal liability pursuant to Section 203 (4) StGB. The Controller points out to the Processor that a person involved in the processing is liable to prosecution pursuant to Section 203 (4) sentence 2 No. 2 StGB if they make use of another collaborating person who in turn discloses a third party secret without authorization which has become known to them in the course of or on the occasion of their work, and the person has not ensured that the other collaborating person has been obliged to maintain confidentiality.

Austria

The Parties are aware that data from the area of medical treatment that are processed under this DPA are subject to the special protection of secrecy under Section 121 of the Austrian Criminal Code (Strafgesetzbuch – "StGB"). Furthermore, the Parties are aware that such data may also be subject to special secrecy requirements applicable to medical doctors and their auxiliary personnel, pursuant to Section 54 of the Austrian Medical Doctors Act (Ärztegesetz – "ÄrzteG"), as well as the special secrecy requirements applicable to hospital personnel, pursuant to Section 9 of the Austrian Hospitals Act (Krankenanstalten- und Kuranstaltengesetz – "KaKuG").

In addition to Sec. 5 of this DPA, the Processor shall ensure that all employees involved in the processing of the Controller's and all other persons working for the Processor (e.g. further processors) who are involved in the processing have undertaken in text form not to disclose without authorization the professional secrets of which they become aware in the course of or on the occasion of their work and that they have been informed of the possible criminal liability pursuant to Section 121 (1) and (4) StGB as well as the possible administrative criminal liability pursuant to Section 199 (3) ÄrzteG.

In addition to Sec. 5 of this DPA, the Processor shall ensure that the confidentiality obligations which the persons who process Controller Data are subjected to in accordance with this clause shall survive the termination of such person's employment or other engagement with the Processor, pursuant to Sect. 6 Para 2 of the Austrian Data Protection Act.

Italy

In addition to the obligations set forth in this DPA, the Processor shall ensure that the processing of health data, genetic data, and biometric data (if any) is performed in compliance with Article 2-septies of the Legislative Decree no. 196/2003 and subsequent amendments and integrations ("the Italian Privacy Code") and by implementing any safeguards required from time to time by the Italian Data Protection Authority pursuant to said Article 2-septies, paragraph 1.

The Processor acknowledges and agrees that the rights referred under Sec. 8.1 of this DPA may also be exercised by individuals other than the data subject, in case the latter should die, pursuant to Article 2-terdecies of the Italian Privacy Code.

The Processor further acknowledges and agrees that pursuant to Article 75 of the Italian Privacy Code, the processing of personal data for the purpose of protecting data subjects, third parties, or the community's health and safety shall also be performed in compliance with healthcare sector specific rules and regulations.

The Processor shall comply with the requirements set out by the Italian Data Protection Authority's decision "Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator", issued on 27 November 2008, and subsequent amendments and integrations.

United Kingdom

The references made to the GDPR in this DPA apply mutually for the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("**UK GDPR**"), together with the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) and other data protection or privacy legislation in force from time to time in the United Kingdom.

In section 2.6 of the DPA, the United Kingdom shall be added as place of data processing in addition to the European Union and the EEA.

In sections 3.1 and 10.1 of the DPA, UK laws shall be added to the laws of the EU and its Member States in case a legal requirement for the processing of personal data derives from such laws.

The Parties are aware that NHS patient data may be processed as part of this DPA.

In addition to this DPA, the Processor shall adhere to the requirements of the Data Security and Protection Toolkit (Data Security and Protection Toolkit (dsptoolkit.nhs.uk)), which is required for suppliers processing NHS patient data.

The Processor’s contact details for its relevant individual responsible for data protection are as follows:

- Contact person’s name, position: Yunmyeong Kim, Chief Privacy Officer
- Contact details: 13-14F Keungil Tower, 223 Teheran-ro, Gangnam-gu, Seoul, 06142, Republic of Korea