MASTER SERVICES AGREEMENT

This standard contract for AWS Marketplace consists of a Master Services Agreement ("**MSA**") with Collective Minds Radiology AB, a company limited by shares incorporated in Sweden under company registration number 559120-7187 (“**CMRAD**”), with address Svärdvägen 5, 182 33, Danderyd, Sweden. More specifically, it sets forth the terms and conditions applicable to the license and the services provided by CMRAD to the Party subscribing to the Product in the AWS Marketplace (“**Buyer**” or “**Institution**”), which will be hereinafter considered also as the “**Institution**” in the MSA Terms and Conditions. Institution/Buyer and CMRAD may be referred to collectively as the “**Parties**” or individually as a “**Party**”.

When the Buyer/Institution purchases a Subscription, as described in the applicable Product Listing and the corresponding purchase transaction, it may be for the Product deployed in the Buyer’s/Institution’s Computing Environment and/or Product deployed via SaaS Service through the CMRAD Platform (hereinafter the “**Services**”).

Both Parties are signing this MSA to set up an indefinite framework for the performance of the Services by CMRAD, whether paid or provided free of charge, as agreed in each Service Order or Subscription to the Product in the AWS Marketplace (“**AWS Subscription**”).

This MSA, along with any referenced documents such as the Data Processing Agreement (DPA), outlines the terms and conditions that govern the provision of the Services by CMRAD to the Institution as described in each applicable Service Order/AWS Subscription. By using the Services, the Institution agrees to be bound by the MSA and its following terms and conditions for CMRAD's SaaS solutions and Services.

CMRAD will fulfill the Services and/or the AWS Subscription to the Institution/Buyer. An AWS Subscription, its pricing, and its term (if not on demand) are set forth in the AWS Product Listing. Additional information concerning the Product and included services that are included or referenced in the AWS Product Listing are a part of the AWS Product Listing; such information may include but is not limited to the intended geographic use of the Product, any technical requirements for the use of the Product, Support Services (which may vary by geography), information regarding Open Source Software and a description of Licensor’s security practices.

Each AWS Subscription is subject to and governed by this MSA, the applicable AWS Product Listing, the Privacy and Security Terms for SaaS Service Subscriptions, and any amendments to any of the foregoing as may be agreed upon by the Parties in accordance with Clause 21 of the MSA terms and conditions, which together constitute the entire agreement between Institution/Buyer and CMRAD (the “Agreement” or “MSA”). Each Service Order/AWS Subscription is a separate agreement between the Institution/Buyer and CMRAD.

This MSA is executed as of the last date of signature by the duly authorized representatives of each party, referred to as the "Effective Date". The Parties acknowledge that they can legally bind themselves through this MSA, including its Terms and Conditions and the attached DPA. As of the Effective Date, the undersigned will have caused this MSA to be executed and delivered by their respective duly authorized officers.

MSA TERMS AND CONDITIONS

1. INTERPRETATION

1.1 The definitions and rules of interpretation in this clause apply in the MSA.

Affiliate: Any company or entity that controls, is controlled by, or is under common control with the Institution and is authorized to use the Services.

Authorized User(s): Any agents, employees, or independent contractors of the Institution, including employees, medical doctors, researchers, professionals, and undergraduate and postgraduate medical students, among others, who are authorized by the Institution and CMRAD to create an account into the CMRAD Platform, use the Services and the Documentation, as further described in this MSA and in the relevant Service Order/AWS Subscription. The User subscriptions refer to the subscriptions purchased or made available to the Institution that enable its Authorized Users to access and use the Services, access the Platform through User accounts, and access the relevant Documentation in accordance with the MSA.

Business Day: a day other than a Saturday, Sunday, or public holiday in Sweden.

Commencement Date: The Commencement Date for the MSA is the Effective Date, which is the last date of signature of the MSA. For the Services, the Commencement Date refers to the date mentioned in each Service Order/AWS Subscription as the effective date on which the Services will start and bind the Parties. This information is detailed in each relevant Service Order/AWS Subscription.

Confidential Information: proprietary or confidential information that is either clearly labeled or identified as such per the terms of this MSA.

Consortium Agreement: A consortium agreement is a binding agreement between partners of a research project and/or beneficiaries of any kind of grant, public, or private funding to set out the rights and obligations amongst those partners. A Consortium Agreement applicable to this MSA and a Service Order must be as specified in each relevant Service Order.

Data Processing Agreement or DPA: The agreement that governs the processing of personal data under the terms of this MSA and any of its Service Orders/AWS Subscriptions.

Documentation: any documents or information made available to the Institution by CMRAD either (i) online via www.cmrad.com or such other web address notified by CMRAD to the Institution from time to time or (ii) by email from time to time, which in each case sets out the user instructions for the Services.

Effective Date: Refers to the date on which this MSA becomes legally binding and operational, marked by the signature of the last Party to sign, thereby completing the execution process. This date establishes when the terms and conditions set forth in the MSA, including any related Service Orders / AWS Subscriptions and Data Processing Agreements, officially take effect and start governing the Parties' relationship.

Fees: the amounts payable by the Institution to CMRAD for the Services when applicable) for the Services, as detailed in each Service Order/AWS Subscription.

Institution: The entity identified in this MSA and any Service Order/AWS Subscription engaging CMRAD for Services.

Institution Data: Data submitted by the Institution and/or its Affiliates and/or its Authorized Users to CMRAD's Platform (either as data Controller or data Processor) or by CMRAD on behalf of the Institution (as Data Processor) for the purpose of receiving or facilitating the provision of the Services, which may or may not contain personal data. Such data may contain anonymous or personal data, typically in a pseudonymized format.

Initial Service Period: The initial term of service as specified in each Service Order/AWS Subscription.

MSA: Stands for the "Master Services Agreement," which consists of an indefinite overarching framework agreement between CMRAD and the Institution. This agreement outlines the terms and conditions of CMRAD's services to the Institution (including data processing activities under a DPA), whether paid or unpaid, outlining the terms and conditions governing their business relationship, as detailed in each Service Order/AWS Subscription.

Platform: The digital interface or environment provided by CMRAD where the Services are accessed and used by the Institution and Authorized Users

Quotation Documents: refers to any appendix or appendixes accompanying a Service Order/AWS Subscription, delineating comprehensive financial and/or informational details pertaining to costs and payments for the Services.

Renewal Period: The period described in each Service Order/AWS Subscription following the Initial Service Period.

Service Order: means a document (including its schedules, annexes, and appendices, if any) detailing specific Services to be provided to the Institution by CMRAD under the terms of the MSA. The Service Order also includes any AWS Subscription consisting of the purchase of the CMRAD products/Services in the AWS Marketplace.

Service Period: Refers to the combined duration of the Initial Service Period and any subsequent Renewal Periods as specified in each Service Order/AWS Subscription. This term defines the total time during which the Services are to be rendered under the MSA.

Services: any services provided by CMRAD to the Institution under this MSA, whether free or paid, as outlined in each Service Order/AWS Subscription.

"**Service-Level Agreement**" or "**SLA**": CMRAD's general Service Level Agreement and support services policy in relation to the Services as made available either at (i) https://about.cmrad.com/SLA or such other website address as may be notified to the Institution from time to time; or (ii) by email from time to time.

Software: Software, code, or applications used or provided by CMRAD as part of the Services or to enable the provision of the Services (SaaS).

Third Party: Any person or entity not a Party to the MSA, DPA, or a Service Order/AWS Subscription, excluding Affiliates.

User Account: Definition outlining the authorized access granted to Authorized Users of the Platform, including user authentication and authorization details, as part of the User Subscription.

User subscription: the subscriptions purchased or made available to the Institution that enable its Authorized Users to access and use the Services, access the Software through user accounts, and access the relevant Services and Documentation in accordance with the MSA and a Service Order/AWS Subscription.

Virus/es: Any software, code, file, or program designed to disrupt, damage, or impair the operation of computer software, hardware, or networks. This includes elements that degrade telecommunications services, equipment, and network operations or interfere with access to or the operation of programs and data. Effects may include altering, erasing, or rearranging data or programs. Examples include worms, trojan horses, and other similar malicious entities.

Vulnerability: Any weakness within the computational logic, such as in software or hardware components, that can be exploited to negatively impact the confidentiality, integrity, or availability of a system. The term "Vulnerabilities" refers collectively to all such weaknesses.

1.1 Clause headings shall not affect the interpretation of this Master Services Agreement.

1.2 A person includes an individual, corporate, or unincorporated body (whether or not having a separate legal personality).

1.3 A reference to a company shall include any company, corporation, or other body corporate, wherever and however incorporated or established.

1.4 Unless the context otherwise requires, words in the singular shall include the plural and, in the plural, shall include the singular.

1.5 Unless the context otherwise requires, a reference to one gender shall include a reference to the other gender.

1.6 A reference to a statute or statutory provision is a reference to it as it is in force as of the date of the MSA.

1.7 A reference to a statute or statutory provision shall include all subordinate legislation made as of the date of the MSA under that statute or statutory provision.

1.8 References to clauses are to the clauses of this Master Services Agreement.

2. APPLICATION OF TERMS AND CONDITIONS

2.1 The agreement between the Parties, as part of the MSA, consists of the following documents:

2.1.1 the Master Services Agreement ('MSA'), which is composed of these Terms and Conditions;
2.1.2 the Data Processing Agreement ('DPA');
2.1.3 any Service Order/AWS Subscription signed between the Parties under this MSA and
2.1.4 the Documentation.

2.2 Each Service Order/AWS Subscription entered into by the Parties in connection with the Services shall form a separate agreement incorporating the MSA.

2.3 This MSA and its terms and conditions take precedence over any other agreements, orders, conditions, or documentation related to the Services, whether they are written or implied, including but not limited to Service Orders/AWS Subscriptions, Quotations, SLAs, or those implied by law, trade custom or practice, or course of dealing. This means that in case of any conflict, inconsistency, or ambiguity over any other documentation related to the services provided, this MSA is considered as the primary governing authority.

2.4 Notwithstanding the above, when it comes to the specifics of personal data handling, instructions, and protection, the provisions of the DPA shall take precedence over those of the MSA and any other related documents. This ensures that the handling of personal data is governed by the most stringent and protective measures as outlined in the DPA.

2.5 The terms of any applicable Consortium Agreement signed between the Parties as part of the Services of a signed Service Order/AWS Subscription shall take precedence.

3. SERVICES

3.1 CMRAD shall, during the Service Period established in each Service Order/AWS Subscription, provide the Services and make available the Documentation to the Institution on and subject to the terms of this MSA.

3.2 CMRAD shall use commercially reasonable endeavors to make the Services available 24 hours a day, seven days a week, within specifications provided in our SLA.

3.3 As part of the Services and at no additional cost to the Institution, CMRAD will provide the Institution with CMRAD's standard support services in accordance with the SLA in effect at the time when the Services are provided unless otherwise agreed in the Service Order/AWS Subscription. CMRAD may amend the SLA at its own discretion from time to time. CMRAD offers enhanced service level agreements support services and separately at an additional cost to the Institution.

4. LICENSE, CONDITIONS OF USE AND PROHIBITIONS

4.1 Subject to the terms of each signed Service Order/AWS Subscription and, where applicable, the Institution's payment of the fees set forth in the applicable Service Order/AWS Subscription, CMRAD grants the Institution a non-exclusive, non-transferable license to use the Services. This right allows the Institution to permit its Authorized Users to use the Services and access the Documentation during the Service Period specified in each Service Order/AWS Subscription, provided that the Institution complies with the terms of the MSA. The Institution does not have the right to grant sub-licenses.

4.2 The Institution recognizes that access to the Services -unless otherwise agreed in a Service Order/AWS Subscription- may require up to five Business Days from the Commencement Date of each Service Order/AWS Subscription to set up initially. Additionally, the use of the Services is always subject to the Institution's compliance with the MSA and its DPA.

4.3 The Institution acknowledges that an Authorized User may use the Services only after

4.3.1 has accepted CMRAD's mandatory terms of service, privacy, and any other required user policies in order to register for and use the Platform and
4.3.2 where required, has successfully completed the CMRAD registration process by providing the necessary documentation and evidence; and

4.4 In relation to the Authorized Users, the Institution undertakes the following:

4.4.1 to ensure that Authorized Users understand and are able to comply with CMRAD's terms of use and/or the rules and policies set forth on the CMRAD Platform, such as the prohibition against attempting to identify a patient with the data contained on the Platform, uploading malicious information, uploading identifiable patient information that cannot be pseudonymized or anonymized, or sharing or attempting to share patient data with unauthorized third parties or outside of the Platform.
4.4.2 that CMRAD will process the personal data of Authorized Users in its capacity as Data Controller, complying with all legal obligations under applicable laws, including GDPR.
4.4.3 That the maximum number of Authorized Users that it authorizes to access and use the Services and the Documentation shall not exceed the number of Authorized Users specified in the Service Order(s) or otherwise agreed with CMRAD;
4.4.4 that it will not allow or suffer any User account to be used by more than one individual Authorized User unless it has been reassigned in its entirety to another individual Authorized User, in which case the prior Authorized User shall no longer have any right to access or use the Services and/or Documentation;
4.4.5 that each Authorized User understands and acknowledges that to use the Platform and Services, they must create a

secure password must keep their password strictly confidential, and shall never leave their device unattended when logged on to the Platform;

4.4.6 that shall maintain a written, up-to-date list of current Authorized Users and provide such list to CMRAD within 5 Business Days of CMRAD's written request at any time or times;

4.5 The Institution shall permit CMRAD or CMRAD's designated auditor to audit the Services at CMRAD's request. Any such audit may be conducted no more than twice per year at CMRAD's expense, and this right shall be exercised with reasonable notice in a manner that does not unreasonably interfere with the Institution's normal operations.

4.5.1 if any of such audits reveal that any password has been provided to any individual who is not an Authorized User, then without prejudice to CMRAD's other rights, the Institution shall promptly disable such passwords, and CMRAD shall not issue any new passwords to any such individual; and

4.5.2 if any of the audits reveal that the Institution has underpaid Fees to CMRAD (when applicable), then without prejudice to CMRAD's other rights, the Institution shall pay to CMRAD an amount equal to such underpayment as calculated in accordance with the prices set out in the Service Order/AWS Subscription within 10 Business Days of the date of the relevant audit.

4.6 The Institution shall not:

4.6.1 Introduce, permit access, store, distribute, or transmit any Viruses or Vulnerabilities into CMRAD's network and Platform.

4.6.2 Access, store, distribute, or transmit material that is unlawful, fraudulent, harmful, defamatory, obscene, infringing, harassing, racially or ethnically offensive; conduct, facilitate, or depict illegal activities, including but not limited to sexually explicit images, promotion of violence, or content discriminatory towards race, gender, opinion, religious belief, sexual orientation, or disability.

4.6.3 Engage in actions or upload material or information that intentionally causes confusion, disseminates false information within the research or health community, or puts at risk patients' privacy by uploading compromised or prohibited material by itself or through an Authorized User.

4.6.4 Identify or attempt to re-identify a patient from the information contained in the Platform when there is no legal basis or requirement to do so, by itself or through an Authorized User. If there is a legal basis or requirement for such actions, CMRAD must be notified beforehand and grant authorization to ensure no other rights are violated.

4.6.5 Copy, modify, create derivative works from, republish, download, display, transmit, or distribute any portion of the Software and/or Documentation; not decompile, reverse engineer, or otherwise alter any part of the Software; use the Services and/or the Software, Platform, or the Documentation to build competing products, provide services to third parties, or extend access beyond authorized limits under this MSA and any Service Order/AWS Subscriptions.

4.6.6 Commercially exploit or make the Services and/or Documentation available to any third party, except as explicitly permitted under this MSA and any Service Order/AWS Subscription.

CMRAD reserves the right, without liability to or prejudice of its other rights towards the Institution, to disable the Institution's or the Authorized User's access to any material that breaches the provisions of this clause.

4.7 The Institution agrees to use all reasonable endeavors to prevent any unauthorized access to or use of the Services and/or Documentation. In the event of any such unauthorized access or use, the Institution shall promptly notify CMRAD.

5. EXTENSION OF LICENSE TO USE THE SERVICES

5.1 The Institution may request an extension of the Services and/or licenses at any time by signing a Service Order/AWS Subscription setting out the terms of such extension and payment terms, if applicable. Such Service Orders/AWS Subscriptions, including the DPA and these Terms and Conditions, will be part of this MSA.

5.2 If the Institution wishes to increase the number of Authorized Users permitted to access the Services and Documentation under a Service Order/AWS Subscription or requests that CMRAD authorize an additional organization to access the Services and Documentation, the Institution shall notify CMRAD in writing. CMRAD will evaluate such requests and respond to the Institution with an approval or rejection. If CMRAD approves the request, CMRAD shall provide such additional access to the Services and Documentation within five (5) business days of CMRAD's approval of the Institution's request.

5.3 If CMRAD approves the request, the Institution shall pay CMRAD the applicable fees for such additional extension, as outlined in the relevant Service Order/AWS Subscription, within 30 days of the date of CMRAD's invoice, unless the payment of fees is not applicable.

6. DATA PROTECTION

6.1 The Parties will process any personal data in accordance with the provisions of applicable legislation (e.g., 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 -General Data Protection Regulation-).

6.2 The processing of personal data conducted in the framework of this Agreement will involve the processing of personal data by CMRAD of Authorized Users data, as a Data Controller, through a registration procedure in which the Authorized Users will be adequately informed about the processing of their personal data, and when applicable, consent to the processing activities. More information on the processing of personal data by CMRAD is provided at www.cmrad.com (Privacy Policy).

6.3 Furthermore, to perform the Services described in this MSA, CMRAD may have to process personal data, which will be uploaded to the Collective Minds Platform on behalf of the Institution as a Data Processor. This data may come from different sources (e.g., the Institution, hospitals, clinics, trusts, etc.), and the Institution will act as the Data Controller. In those cases:

6.3.1 Any processing of personal data conducted by CMRAD in connection with this MSA and any of its Service Orders or under a Consortium Agreement shall be governed by the terms of the Data Processing Agreement ("DPA") attached to this MSA as Annex 1, which forms an integral part of this MSA.

6.3.2 In case personal data has to be transferred from the EU to a Third Country(s), in the absence of an adequacy decision, the Parties will implement appropriate data protection safeguards, such as the signature of the EU Commission Standard Contractual Clauses (SCC), which will be attached to this MSA along with the DPA attached hereto.

6.3.3 Before the Institution transfers Personal Data to CMRAD or permits CMRAD to access Personal Data located in a jurisdiction that requires an International Data Transfer Mechanism, the Institution will notify CMRAD of the

relevant requirement, and the Parties will work together in good faith to fulfill the requirements of that International Data Transfer Mechanism. The Parties will institute and comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Law.

7. THIRD-PARTY PROVIDERS

7.1 The Institution acknowledges that the Services may enable or facilitate access to third-party website content, correspondence with third parties, and/or purchase products and services from third parties through third-party websites, and it does so entirely at its own risk.

7.2 CMRAD does not make any representations, warranties, or commitments and is not liable for any content or use of any third-party website, services, or any transaction entered into by the Institution with any such third-party. Any contract or transaction with a third-party is solely between the Institution and such third-party, and not CMRAD. It is recommended that the Institution carefully reviews the terms and conditions and the privacy policies of any third-party services or websites before using them. CMRAD does not endorse or approve any third-party website or the content of any third-party website made available through the Services.

8. CMRAD'S OBLIGATIONS

8.1 CMRAD undertakes that the Services will be performed substantially in accordance with the terms of each signed Service Order/AWS Subscription, this MSA and its terms and conditions, and CMRAD's SLA, and with reasonable skill and care.

8.2 The foregoing obligation shall not apply to the extent of any non-conformity caused by the use of the Services contrary to CMRAD's instructions or by any modification or alteration of the Services by any party other than CMRAD or CMRAD's duly authorized contractors or agents. If the Services do not conform to the foregoing obligation, CMRAD shall, at its expense, use all reasonable commercial efforts to promptly correct such non-conformity or provide the Institution with an alternative means of achieving the desired performance. Such correction or replacement shall be the Institution's sole and exclusive remedy for any breach of the obligation set forth in this clause.

8.3 CMRAD does not warrant that:

8.3.1 the Institution's use of the Services will be uninterrupted or error-free.
8.3.2 that the Services, Documentation and/or the information obtained by the Institution through the Services will meet the Institution's requirements.
8.3.3 the Software or the Services will be free from Vulnerabilities or Viruses.

8.4 CMRAD is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Institution acknowledges that the Services and Documentation may be subject to limitations, delays, and other problems inherent in the use of such communications facilities.

8.5 The MSA shall not prevent CMRAD from entering into similar agreements with third parties or from independently developing, using, selling, or licensing documentation, products, and/or services that are similar to those provided under the MSA and any of its Service Orders/AWS Subscriptions.

8.6 CMRAD warrants that it has and will maintain all necessary licenses, consents, and permissions for performing its obligations under this MSA and any of its Service Orders/AWS Subscriptions.

8.7 CMRAD shall follow the procedures for back-ups and logs of Institution Data as set out in the Service Order/AWS Subscription. In the event of any loss or damage to Institution Data, the Institution's sole and exclusive remedy against CMRAD shall be for CMRAD to use reasonable commercial endeavors to restore the lost or damaged Institution Data from the latest backup of such Institution Data maintained by CMRAD in accordance with the back-up procedure described in the Service Order/AWS Subscription. CMRAD shall not be responsible for any loss, destruction, alteration, or disclosure of Institution Data caused by any third party (except those third parties sub-contracted by CMRAD to perform services related to Institution Data maintenance and back-up for which it shall remain fully liable.

9. INSTITUTION'S OBLIGATIONS

9.1 The Institution shall:

9.1.1 provide CMRAD with:

9.1.1.1 all necessary cooperation in relation to the MSA and
9.1.1.2 all necessary access to such information as may be required by CMRAD in order to provide the Services, including but not limited to Institution Data, security access information, and configuration services.

9.1.2 When applicable under the terms of a Service Order/AWS Subscription, pay the Services under the terms agreed under the Services Order and this MSA.
9.1.3 Without affecting its other obligations under the MSA, comply with all applicable laws and regulations with respect to its activities under the MSA.
9.1.4 Carry out all other Institution responsibilities set out in the MSA in a timely and efficient manner. If there are any delays in the Institution's provision of such assistance as agreed by the Parties, CMRAD may adjust any agreed timetable or delivery schedule as reasonably necessary.
9.1.5 Ensure that Authorized Users use the Services and Documentation in accordance with the terms and conditions of this MSA and the relevant Service Order/AWS Subscription and remain responsible for any breach of the MSA or any Service Order/AWS Subscription by any Authorized User.
9.1.6 Obtain and maintain all necessary licenses, consents, and permissions for CMRAD, its contractors, and agents to perform their obligations under the MSA and relevant Service Orders/AWS Subscriptions, including, without limitation, the Services.
9.1.7 Ensure that its network and systems comply with the relevant specifications provided by CMRAD from time to time.
9.1.8 to the extent permitted by law and except as otherwise expressly provided in the MSA or in the relevant Service Order/AWS Subscription, to be solely responsible for procuring, maintaining, and securing its network connections and telecommunications links from its systems to CMRAD's data centers, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Institution's network connections or telecommunications links or caused by the internet.

9.2 The Institution shall own all rights, titles, and interests in and to all Institution Data and shall be solely responsible for its legality, reliability, integrity, accuracy, and quality.

10. FEES AND PAYMENT

10.1 Unless otherwise specified or agreed to in the relevant Service Order/AWS Subscription, the Institution must pay the Fees to CMRAD in accordance with this MSA and the terms of each Service Order/AWS Subscription.

10.2 In the cases where the payment of fees is applicable, CMRAD shall invoice the Institution in accordance with the invoice schedule set out in the Service Order/AWS Subscription.

10.3 In cases that payments are applicable, if CMRAD has not received payment within 30 days after the due date and without prejudice to any other rights and remedies of CMRAD:

10.3.1 CMRAD may, without liability to the Institution, disable the Institution's password, account, and access to all or part of the Services, and CMRAD shall be under no obligation to provide any or all of the Services while the invoice(s) concerned remain unpaid; and

10.3.2 Interest shall accrue daily on such due amounts at the statutory interest rate for payment default under Swedish law, commencing on the due date and continuing until fully paid, whether before or after judgment.

10.4 All amounts and fees stated or referred to in a Service Order/AWS Subscription:

10.4.1 must be made in the currency indicated on each Service Order/AWS Subscription, except where otherwise expressly agreed.

10.4.2 are subject to the terms of this MSA and the relevant Service Order/AWS Subscription, non-cancellable and non-refundable.

10.4.3 are exclusive of value-added tax, which shall be added to CMRAD's invoice(s) at the appropriate rate.

10.5 CMRAD reserves the right to adjust the Fees annually on the anniversary of the Commencement Date in accordance with changes to the Swedish Producer Price Index (PPI). Should the PPI be negative, the Fees will remain unchanged.

11. PROPRIETARY RIGHTS

11.1 The Institution acknowledges and agrees that CMRAD and/or its licensors own all intellectual property rights in the Services and the Documentation. Except as expressly stated herein, the MSA does not grant the Institution any rights to, under, or in any patents, copyrights, Software, database rights, trade secrets, trade names, trademarks (whether registered or unregistered), or any other rights or licenses in respect of the Services, including CMRAD's Platform, or the Documentation.

11.2 CMRAD confirms that it has all the rights in relation to the Services and the Documentation that are necessary to grant all the rights it purports to grant under and in accordance with the terms of this MSA.

12. CONFIDENTIALITY

12.1 Each Party may be given access to Confidential Information from the other Party in order to perform its obligations under the MSA. A Party's Confidential Information shall not be deemed to include information that:

12.1.1 is or becomes publicly known other than through any act or omission of the receiving Party.

12.1.2 was in the other Party's lawful possession before the disclosure.

12.1.3 is lawfully disclosed to the receiving Party by a third party without restriction on disclosure or

12.1.4 is independently developed by the receiving Party, which independent development can be shown by written evidence.

12.2 Subject to this clause, each Party shall hold the other's Confidential Information in confidence and not make it available to any third party or use it for any purpose other than implementing the MSA.

12.3 Each Party shall take all reasonable steps to ensure that the other's Confidential Information to which it has access is not disclosed or distributed by its employees or agents in violation of the terms of the MSA and its Service Orders/AWS Subscriptions.

12.4 A Party may disclose Confidential Information to the extent such Confidential Information is required to be disclosed by law, by any governmental or other regulatory authority, or by a court or other authority of competent jurisdiction, provided that, to the extent it is legally permitted to do so, it gives the other Party as much notice of such disclosure as possible and, where notice of disclosure is not prohibited, it takes into account the reasonable requests of the other Party in relation to the content of such disclosure.

12.5 The Institution acknowledges that details of the Services and the results of any performance tests of the Services constitute CMRAD's Confidential Information.

12.6 CMRAD acknowledges that Institution Data is the Confidential Information of the Institution.

12.7 The above provisions shall apply during the term of the MSA and for five (5) years following termination of the MSA, however arising.

13. INDEMNITY

13.1 The Institution shall defend, indemnify, and hold harmless CMRAD against claims, actions, proceedings, losses, damages, expenses, and costs (including without limitation court costs and reasonable legal fees) arising out of or in connection with the Institution's use of the Services and/or Documentation, provided that:

13.1.1 CMRAD provides reasonable cooperation to the Institution in the defense and settlement of such claim at the Institution's expense and

13.2 CMRAD shall defend the Institution, its officers, directors, and employees against any claims alleging that the Institution's use of the CMRAD Platform and Services infringes upon any Intellectual Property Rights. This obligation to defend is limited to the intellectual property rights of the CMRAD Platform and Services and does not extend to any content, including Institution Data, provided or uploaded to the Platform by the Institution. The obligations of CMRAD under this section are contingent upon the following:

13.2.1 The Institution has given prompt notice of any such claim.

13.2.2 the Institution does not make any admission or otherwise attempt to compromise or settle the claim and provides reasonable cooperation to CMRAD in the defense and settlement of such claim at CMRAD's expense and

13.2.3 CMRAD is given sole authority to defend or settle the claim.

13.3 In the defense or settlement of any claim, CMRAD may procure the right for the Institution to continue using the Services and replace or modify them so that they become non-infringing. If such remedies are not reasonably available, or CMRAD has failed to take action within 30 days of being notified of the claim by the Institution, then either Party may terminate the MSA on five (5) Business Days' notice to the other Party without any additional liability or obligation for CMRAD or other additional costs to the Institution.

13.4 In no event shall CMRAD, its employees, agents, and subcontractors be liable to the Institution to the extent that the alleged infringement is based on:

13.4.1 a modification of the Services or Documentation by anyone other than CMRAD (other than with CMRAD's approval); or

13.4.2 the Institution's use of the Services or Documentation in a manner contrary to the written instructions given to the Institution by CMRAD or

13.4.3 the Institution's use of the Services or Documentation after written notice of the alleged or actual infringement from CMRAD or any relevant authority.

14. LIMITATION OF LIABILITY

14.1 Except as expressly and specifically provided in the MSA:

14.1.1 the Institution assumes sole responsibility for results obtained from the use of the Services and the Documentation by the Institution and for conclusions drawn from such use. CMRAD shall not be held liable for any damage caused by misunderstandings, misinformation, errors, or omissions in any information, instructions, or scripts provided to CMRAD by the Institution in connection with the Services or any actions taken by CMRAD at the Institution's direction.

14.1.2 all warranties, representations, conditions, and all other terms of any kind whatsoever implied by statute or common law are, to the fullest extent permitted by applicable law, excluded from the MSA and

14.1.3 the Services and the Documentation are provided to the Institution on an "as is" basis.

14.2 Subject to clause 14.1, CMRAD is liable for damage arising from any negligence by CMRAD in providing the Services, however:

14.2.1 CMRAD shall in no event be liable for (i) any indirect, special, incidental, punitive, exemplary, or consequential costs, damages, charges, or expenses (ii) any loss or corruption of data or information, business, or profits (whether direct or indirect) however arising under this MSA and/or any Service Orders/AWS Subscriptions, regardless of legal theory; and

14.2.2 CMRAD's total aggregate liability for all claims arising in connection with the performance or contemplated performance of this MSA and any associated Service Orders/AWS Subscriptions shall not exceed 80% of the total Fees paid by the Institution to CMRAD in the respective 12-month period commencing on the Commencement Date or on each anniversary thereof.

14.3 Unless a Party notifies the other Party that it intends to make a claim regarding an event within the notice period, the other Party shall have no liability for that event. The notice period for an event shall start on the day on which the Party wishing to make a claim became, or ought reasonably to have become, aware of the event having occurred (as opposed to it becoming aware of its having grounds to make a claim in respect of it) and shall expire 6 months from that date. The notice must be in writing and must identify the event and the grounds for the claim in reasonable detail. In addition, hereto, any claim of an Institution must be commenced within one (1) year starting from the day on which the Institution became, or ought reasonably to have become, aware of the event having occurred upon which the claim is based. There shall be no right to any remedy for the Institution for any claim not asserted within the afore-mentioned periods.

14.4 Nothing in the MSA excludes the liability of the Institution for any breach, infringement, or misappropriation of CMRAD's Intellectual Property Rights.

15. DURATION AND TERMINATION

15.1 Both the MSA and its associated DPA shall be effective as of the Effective Date and shall continue to be effective indefinitely until either Party expressly terminates them by written notice. The MSA will not take effect without an active Service Order/AWS Subscription or the processing of CMRAD data on behalf of the Institution.

15.2 Each Service Order/AWS Subscription shall commence on the Commencement Date and continue for the Initial Service Period. Unless terminated by either Party as specified herein, the Service Orders/AWS Subscriptions will automatically renew for successive 12-month periods (each a **Renewal Period**). Termination requires written notice from either Party to the other at least 30 days before the end of the Initial Service Period or any Renewal Period (**Service Period**), at which point the applicable Service Orders/AWS Subscriptions, and if appropriate, the MSA will terminate upon the expiry of the current period.

15.3 Without affecting any other right or remedy available to it, either Party may terminate the MSA and/or a Service Order/AWS Subscription, with immediate effect by giving written notice to the other Party, if:

15.3.1 the other Party fails to pay any amount due under the MSA or Service Order/AWS Subscriptions on the due date for payment and remains in default not less than 30 days after being notified in writing to make such payment.

15.3.2 the other Party commits a material breach of any other term of the MSA and (if such breach is remediable) fails to remedy that breach within a period of 30 days after being notified in writing to do so.

15.3.3 the other Party suspends, or threatens to suspend, payment of its debts, is unable to pay its debts as they fall due, admits inability to pay its debts, or is deemed unable to pay its debts within the meaning of the Swedish Bankruptcy Act (SFS 1987:672).

15.3.4 the other Party commences negotiations with all or any class of its creditors with a view to rescheduling any of its debts or makes a proposal for or enters into any compromise or arrangement with its creditors other than for the sole purpose of a scheme for a solvent amalgamation of that other Party with one or more other companies or the solvent reconstruction of that other Party.

15.3.5 the other Party applies to a court for or obtains reconstruction/reorganization.

15.3.6 a petition is filed, a notice is given, a resolution is passed, or an order is made for or in connection with the winding up of that other Party other than for the sole purpose of a scheme for a solvent amalgamation of that other Party with one or more other companies or the solvent reconstruction of that other Party.

15.3.7 an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is given or if an administrator is appointed over the other Party (being a company, Partnership or limited liability partnership);

15.3.8 the holder of a qualifying floating charge over the assets of that other Party (being a company or limited liability partnership) has become entitled to appoint or has appointed an administrative receiver.

15.3.9 a person becomes entitled to appoint a receiver over the assets of the other Party, or a receiver is appointed over the assets of the other Party.

15.3.10 a creditor or encumbrancer of the other Party attaches or takes possession of, or a distress, execution, sequestration, or another such process is levied or enforced on or sued against, the whole or any part of the other Party's assets and such attachment or process is not discharged within 14 days.

15.3.11 any event occurs, or proceeding is taken, with respect to the other Party in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned in clauses 15.3.3 to clause 153.10 (inclusive); or

15.3.12 the other Party suspends, ceases, or threatens to suspend or cease carrying on all or a substantial part of its business.

16. CONSEQUENCES OF TERMINATION

16.1 On termination of the MSA for any reason:

16.1.1 All licenses granted under the MSA shall immediately terminate, and the Institution shall immediately cease all use of the Services and/or the Documentation.

16.1.2 Aach Party shall return and make no further use of any equipment, property, Documentation, and other items (and all copies of them) belonging to the other Party.

16.1.3 Any rights, remedies, obligations, or liabilities of the Parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the MSA that existed at or before the date of termination, shall not be affected or prejudiced.

17. FORCE MAJEURE

17.1 CMRAD shall have no liability to the Institution under the MSA if it is prevented from or delayed in performing its obligations under the MSA or from carrying on its business by acts, events, omissions, or accidents beyond its reasonable control, including without limitation, strikes, blackouts, lock-outs or other industrial disputes (whether involving the workforce of CMRAD or any other Party), failure of a utility service or transport or telecommunications network, unforeseen or inevitable event, pandemic, epidemic, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or subcontractors.

18. VARIATION

18.1 No variation of the MSA shall be effective unless it is in writing and signed by the Parties (or their authorized representatives).

19. WAIVER

19.1 No failure or delay by a Party to exercise any right or remedy provided under the MSA or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

20. SEVERANCE

20.1 If any provision or part-provision of the MSA is or becomes invalid, illegal, or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of the MSA.

21. ENTIRE AGREEMENT

21.1 Except for the specific terms of any Consortium Agreement that prevail over this MSA, the MSA constitutes the entire agreement between the Parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations, and understandings between them, whether written or oral, relating to its subject matter.

21.2 Each Party acknowledges that in entering into the MSA, it does not rely on, and shall have no remedies in respect of, any statement, representation, assurance, or warranty (whether made innocently or negligently) that is not set out in the MSA.

21.3 Each Party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in the MSA.

21.4 Nothing in this clause shall limit or exclude any liability for fraud established in this MSA or the Master Services Agreement.

22. NO PARTNERSHIP OR AGENCY

22.1 Nothing in the MSA is intended to or shall operate to create a partnership between the Parties or authorize either Party to act as agent for the other, and neither Party shall have the authority to act in the name or on behalf of or otherwise to bind the other in any way (including, but not limited to, the making of any representation or warranty, the assumption of any obligation or liability and the exercise of any right or power).

23. THIRD-PARTY RIGHTS

23.1 The Parties confirm that the MSA is not intended to and shall not give rise to any rights to any third party beyond what is established explicitly by this MSA and or any of its Service Orders/AWS Subscriptions, including the terms of a Consortium Agreement that apply to Service Order/AWS Subscription.

24. NOTICES

24.1 Any notice required to be given under the MSA shall be in writing and shall be delivered by hand or sent by pre-paid first-class post or recorded delivery post to the other Party at its address set out in the MSA or such other address as may have been notified by that Party for such purposes or sent by e-mail to the email address set out in the Service Order/AWS Subscription.

24.2 Any notice shall be deemed to have been received:

24.2.1 if delivered by hand at the time the notice is left at the proper address.

24.2.2 if sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second Business Day after posting; and

24.2.3 if sent by email, if and when the recipient notifies the receipt of the email, which shall not be unreasonably withheld, provided for the avoidance of doubt that an automatic “read receipt” email sent from the recipient to the sender shall not constitute an acknowledgment of receipt of or reply to such email for purposes of this Clause 24.2.3.

24.3 This clause 24 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

25. EXTERNAL COMMUNICATIONS

25.1 The Parties may publicize or disclose the existence of their cooperation under the MSA and use each other's logos on their websites to acknowledge the relationship between them, provided that such use is consistent with the confidentiality obligations under the MSA and ensures that no confidential information is disclosed. If either Party wishes to limit the scope of this clause, it may do so by written request or by specifying the scope of this right in a Service Order/AWS Subscription.

26. ASSIGNMENT

26.1 Subject to clause 25.2, neither Party shall assign, transfer, charge, sub-contract, or deal in any other manner with all or any of its rights or obligations under the MSA without the prior written consent of the other Party.

26.2 CMRAD may engage a subcontractor to perform the Services and its other obligations under the MSA.

27. GOVERNING LAW AND JURISDICTION

27.1 The MSA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of Sweden without reference to its conflict of laws rules.

27.2 Each Party irrevocably agrees that the general courts of jurisdiction in Sweden, with the District Court of Stockholm as the court of first instance, shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with the MSA or its subject matter or formation (including non-contractual disputes or claims).

Data Processing Agreement

This data processing agreement ("**DPA**") is made in the Effective Date (as established in the MSA and/or the Service Order/AWS Subscription),

by and between:

(1) **Collective Minds Radiology AB**, a company limited by shares incorporated in Sweden under company registration number 559120-7187 ("**Processor**"), with address Svärdvägen 5, 182 33, Danderyd, Sweden;

and

(2) **Institution**, as defined in MSA and its Service Orders or AWS Subscription (hereinafter referred to as the "**Controller**"),

Each a "Party" and together the "Parties"

BACKGROUND AND SCOPE

(1) This Data Processing Agreement (DPA) is an integral part of the Master Services Agreement ("MSA") between the Controller (the "Institution") and the Processor ("CMRAD"). It applies to all Service Orders/AWS Subscriptions executed under the MSA. It governs the processing of Personal Data performed as part of the Services provided under the MSA and any of its Service Orders/AWS Subscriptions.

(2) By entering into the MSA, the Processor (CMRAD) agrees to this DPA on behalf of itself and, where required by applicable Data Protection Legislation, on behalf of its Authorized Affiliates (as defined below). This DPA is effective if and to the extent that CMRAD processes Personal Data in the context of the Services provided to the Controller and its Authorized Affiliates under a signed Service Order/AWS Subscription.

(3) This DPA governs all data processing relationships between the Parties insofar as the Processor (CMRAD) processes Personal Data on behalf of the Controller (the Institution or its Affiliates). It is designed to ensure that such processing meets the requirements of applicable Data Protection Legislation, including the GDPR.

1. Definitions

1.1. In addition to the concepts defined in the text for the MSA, these definitions shall, regardless of whether they are used in the plural or singular, in definite or indefinite form, have the following meaning when entered with capital letters as the initial letter.

Affiliate(s): This term refers to any Controllers affiliate(s) that are subject to the data protection laws and regulations of the European Union (as clarified below) and are permitted to use the Services.

Controller: As defined in Article 4 (7) GDPR, the controller refers to the Institution under this DPA.

Data Breach: Has the meaning as per Article 4 (12) GDPR.

Data Protection Legislation: Refers to all applicable privacy and personal data protection legislation, along with any other legislation (including regulations and directives) applicable to the Processing carried out in accordance with the MSA and the Service Orders/AWS Subscriptions, including the EU legislation, such as the General Data Protection Regulation ("GDPR").

Data Subject: The identified or identifiable natural person to whom Personal Data relates, as per Articles 4 and 4 (1) GDPR.

DPA: Means this Data Processing Agreement and per the meaning in Article 28 GDPR.

DPIA: Data Protection Impact Assessment (DPIA), as defined under Article 35 of the GDPR.

GDPR: Means 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).

Instruction(s): It consists of the documented instructions provided by the Controller to the Processor, as defined by the GDPR and as per Art. 28(3)(a), that, among other aspects, defines the object, duration, type, and purpose of the Personal Data processing, as well as the categories of Data Subjects and special requirements that apply to the Processing.

MSA: Stands for the Master Services Agreement, the overarching contract under which the Processor provides Services to the Controller, processes data on behalf of the Controller (as governed by this DPA) outlining the terms and conditions that govern their business relationship.

Personal Data: Has the meaning as per Article 4 (1) GDPR.

processing: Has the meaning as per Article 4 (2) GDPR.

Processor: This term has the meaning as per Article 4 (8) GDPR. Under this DPA, it refers to Collective Minds Radiology AB and its subsidiaries.

pseudonymization / pseudonymized: The processing of Personal Data in a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, as long as such additional information is kept separately, as defined in Article 4(5) of the GDPR.

Services: Refer to the operations, functions, or tasks provided by the Processor to the Controller under the MSA, either paid or free of charge, as detailed in each Service Order/AWS Subscription.

Sub-processor: Means another processor engaged by the Processor for carrying out specific processing activities on behalf of the Controller, normally consisting of a third-party service provider.

Third Country: Any country outside the EU/EEA that does not have an adequacy decision by the European Commission under the GDPR.

Third Party: Any natural or legal person, public authority, agency, or body other than the Data Subject, Controller, Processor, and persons who, under the direct authority of the Controller or Processor, are authorized to process Personal Data.

1.2. Terms and expressions not defined in this DPA shall have the same meaning as in the GDPR unless otherwise clearly stated in the DPA or the context obviously requires otherwise.

2. Processing of personal data and purpose

2.1. This DPA and its Instructions govern the Processor's processing of Personal Data on behalf of the Controller or its Affiliates. These documents form part of the broader framework established by the MSA and aim to protect the freedoms and rights of the Data Subjects in accordance with Article 28(3) of the GDPR.

2.2. The Controller authorizes the Processor to conduct Personal Data processing activities strictly in accordance with the written Instructions outlined in this DPA. The Processor is permitted to process Personal Data only for purposes explicitly defined under the MSA and the signed Service Orders/AWS Subscriptions within the scope of the current DPA Instructions. Any processing outside of these parameters requires prior express approval from the Controller.

2.3. Each Party is responsible for complying with the applicable Data Protection Legislation in connection with its role and responsibilities towards its processing of Personal Data.

2.4. This DPA, along with its Instructions and the list of potential Sub-processors, regulates the Processor's processing of Personal Data on behalf of the Controller. These documents are integral components of the broader MSA framework and are designed to safeguard the freedoms and rights of Data Subjects as stipulated by Article 28(3) of the GDPR.

2.5. The Controller hereby authorizes the Processor to process Personal Data strictly according to the written Instructions provided in this DPA, which, along with the signed Service Orders/AWS Subscriptions, is part of the MSA. The Processor is allowed to process Personal Data solely for the purposes explicitly defined in the MSA and associated Service Orders/AWS Subscriptions and only within the limits of the current DPA Instructions. Processing beyond these boundaries requires the Controller's prior approval.

2.6. Each Party is responsible for adhering to applicable Data Protection Legislation relative to its respective roles and responsibilities in processing Personal Data.

3. Obligations of the Controller

3.1. The Controller undertakes to ensure that there is a legal basis for the Processing at all times and for establishing adequate Instructions with regard to the nature of the Processing so that the Processor and any Sub-processor can fulfill their tasks according to this DPA and the MSA, as well as any signed Service Orders/AWS Subscriptions.

3.2. The Controller shall, without unnecessary delay, inform the Processor of changes in the Processing that affect the Processor's obligations pursuant to this DPA and/or the applicable Data Protection Legislation.

3.3. The Controller is responsible for informing Data Subjects, as necessary or required, about the Processing and protecting the rights of Data Subjects, pursuant to the applicable Data Protection Legislation, as well as taking any other action incumbent on the Controller according to Data Protection Legislation.

4. Obligations of the Processor

4.1. The Processor undertakes to Process the Personal Data under the MSA strictly in accordance with this DPA, the MSA along with its Service Orders/AWS Subscriptions, the specified Instructions, and the applicable Data Protection Legislation, remaining continuously informed throughout the duration of this DPA.

4.2. The Processor must implement measures to protect Personal Data from any processing activities incompatible with this DPA, the MSA along with its Service Orders/AWS Subscriptions, the Instructions, and the applicable Data Protection Legislation. This includes limiting access to Personal Data to those individuals or organizations who require it to perform the Services and ensuring all Processor's employees and collaborators are bound by confidentiality and privacy obligations, either contractual or statutory.

4.3. If the Processing Instructions are unclear, contravene the applicable Data Protection Legislation, or are inadequate, the Processor must immediately inform the Controller. When necessary, and with the Controller's approval, the Processor will suspend processing until revised Instructions are received unless the Controller directs otherwise. Should the Controller amend the Instructions, the Processor will promptly communicate any related cost implications, if applicable. Additionally, the Processor may propose changes if the Instructions conflict with GDPR or any other applicable Data Protection Legislation; in this case, the Controller will be responsible for reviewing and collaboratively confirming the necessary amendments with the Processor.

4.4. The Processor will assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the Processor.

4.5. The Processor will promptly inform the Controller of any complaints, notices, or communications related to processing Personal Data and provide necessary cooperation and assistance as outlined in this DPA. This includes assisting the Controller with the relevant Data Breach notifications, in the relevant DPIA, assessments, or other types of relevant assessments required to the Controller, and, when necessary, consulting supervisory authorities in case of high-risk processing activities.

4.6. In the event of a Data Breach affecting the Personal Data processed on behalf of the Controller under this DPA, the

Processor must promptly notify the Controller and assist with any resulting obligations as specified under applicable Data Protection Legislation and this DPA.

5. Security measures

5.1. The Processor shall implement and maintain all measures required pursuant to Article 32 of the GDPR, as detailed in the Instructions of this DPA, to ensure a level of security appropriate to the risk. These measures include, but are not limited to:

(a) Pseudonymization and encryption of Personal Data;
(b) Ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
(c) Restoring the availability and access to Personal Data in a timely manner after a physical or technical incident;
(d) Regularly testing, assessing, and evaluating the effectiveness of all technical and organizational security measures.

5.2. The Processor must continuously ensure that there are technical and organizational in place in order to maintain the required confidentiality, integrity, availability, and resilience. This includes regular verification and updates as necessary to meet the requirements of this DPA and any new security requirements or Instructions specified by the Controller after the signing of this DPA.

5.3. Any added or revised security requirements from the Controller post-signature of this DPA will be treated as new Instructions, requiring prompt evaluation and implementation by the Processor to ensure continued compliance with the GDPR and Data Protection Legislation.

5.4. Access or processing to Personal Data under this DPA and MSA shall be strictly limited to relevant individuals and/or organizations, governed by robust authorization control systems. The Processor commits to continuously logging access to Personal Data as required by this DPA and the MSA in accordance with the Instructions provided.

6. Secrecy/duty of confidentiality

6.1. The Processor and all individuals or organizations working under its management must maintain confidentiality and professional secrecy throughout the Processing. This includes binding confidentiality obligations, either through specific agreements or existing legally sanctioned duties of confidentiality.

6.2. The Processor shall promptly inform the Controller of any interactions with supervisory authorities concerning the Processing of Personal Data under this DPA.

6.3. If a Data Subject, supervisory authority, or third-party requests information about the Processing, the Processor must notify the Controller and refrain from disclosing any information without the Controller's written consent, unless otherwise required by law.

7. Information, Audits and inspections

7.1. Upon the Controller's written request, the Processor shall provide all necessary information to demonstrate compliance with the data protection obligations outlined in this DPA. This includes facilitating audits and inspections by the Controller or an independent third party, as specified under Article 28(1) of the GDPR. The Processor will assist by providing documentation, access to facilities, and technical systems necessary for reviewing compliance with this DPA, the Instructions, and the GDPR. All involved individuals must adhere to confidentiality obligations as required by law or contractual duty.

7.2. The Processor will conduct an annual review of the security measures to ensure they meet the requirements of this DPA and the GDPR. The results can be made available to the Controller upon request.

7.3. The Controller's audit requests must include reasonable notice and be preceded by a clearly defined audit plan detailing the scope and objectives agreed upon by both Parties. Alternative verification methods, such as evaluations or audits by independent third parties, would also be considered.

7.4. The Processor will facilitate supervision by supervisory authorities or other legal authorities when required, notifying the Controller as appropriate and providing the necessary means for these authorities to carry out their supervisory roles according to applicable laws, even if such actions conflict with other provisions of this Agreement.

7.5. The Processor must ensure that any Sub-processors give the Controller similar audit and inspection rights as those agreed between the Controller and the Processor, to the extent feasible in light of the circumstances and the function performed by the Sub-Processor.

8. Handling of Data Subjects' rights

8.1. Upon the Controller's instruction, the Processor shall promptly (without undue delay) take necessary actions to correct or delete Personal Data if the processing is found to be inaccurate or to comply with Data Subjects' rights requests under the GDPR. For deletion requests, the Processor is permitted to continue processing the Personal Data solely as part of the deletion process and as required by applicable laws.

8.2. If the Processor receives a request from a Data Subject relating to their rights under the GDPR, and the request pertains to Personal Data processed under the Services, the Processor will promptly notify the Controller. The Processor will inform the Data Subject that their request has been forwarded to the Controller and will not undertake any direct actions to address the request, ensuring that all responses are managed by the Controller.

8.3. The Processor will assist the Controller in fulfilling Data Subjects' rights requests by providing appropriate technical and organizational support, as far as this is feasible, considering the nature of the Processing.

9. Personal Data Breaches

9.1. The Processor shall notify the Controller without undue delay upon becoming aware of a personal Data Breach affecting Personal Data under this DPA. The Processor will provide the Controller with all necessary information to meet any obligations to report the Authorities or inform Data Subjects of the Data Breach under the GDPR. This information shall include:

(e) The nature of the Personal Data and, if possible, the categories and the number of Data Subjects affected, as well as the categories and number of Personal Data categories affected.
(f) The probable consequences of the Data Breach.
(g) Measures that have been taken or planned, as well as measures to mitigate the potential negative effect of the Personal Data Breach.

9.2. If it is not possible for the Processor to supply the entire description at the same time, the description may be supplied in

stages without additional unnecessary delay. If it is not possible for the Processor to provide the full description at the same time, the description may be provided in installments without unnecessary further delay.

9.3. If any physical or technical incident compromises the accessibility or integrity of Personal Data, the Processor shall restore access and functionality to the affected data within a reasonable timeframe, as stipulated under Article 32.1.c of the GDPR.

10. Sub-processors

10.1. The Processor may engage Sub-processors to carry out specific processing activities on behalf of the Controller. Prior to engaging a Sub-processor, the Processor will ensure that the Sub-processor is capable of fulfilling its obligations under Data Protection Legislation, particularly the GDPR. The Processor is committed to maintaining an up-to-date list of Sub-processors available to the Controller at all times via https://about.cmrad.com/data-processors.

10.2. The Processor will inform the Controller in advance of any intended changes regarding the addition or replacement of Sub-processors, providing details such as the Sub-processor's identity, the type of data processed, and the categories of affected data subjects. The Controller has thirty (30) days from receipt of the notification to object to the engagement of the new Sub-processor based on reasonable data protection concerns.

10.3. If the Controller raises an objection to the use of a new Sub-processor by the Processor, and the Processor is unable to make a reasonable adjustment within thirty (30) days to avoid using the objected Sub-processor, the Controller has the right to terminate the relevant Services along with the MSA, including this DPA. The Controller must provide thirty (30) days' written notice before terminating the Services.

10.4. The Processor is required to have a written agreement with every Sub-processor to impose the same data protection obligations on the Sub-processor as those imposed on the Processor under this DPA. Such agreement must also require appropriate technical and organizational measures to be taken to ensure the protection of the Personal Data that is processed.

10.5. The Processor remains fully responsible for any acts or omissions of its Sub-processors and will ensure that all Sub-processors agree to obligations consistent with the provisions of this DPA. Upon terminating the use of a Sub-processor, the Processor will ensure that the Sub-processor either returns or destroys all Personal Data in accordance with this DPA requirements and/or any instructions provided by the Controller.

10.6. The Processor will promptly inform the Controller of any significant issues arising from the Sub-processor's failure to comply with their obligations related to Personal Data Processing.

10.7. The Processor shall ensure that the Controller can exercise its right to audit Sub-processors to the extent possible or instruct the Sub-processor to erase or return the Personal Data in specific circumstances, such as insolvency or if the Processor ceases operations.

11. Localization and transfer of personal data to a Third Country

11.1. The Processor shall ensure that all Personal Data is handled and stored within the EU/EEA or in jurisdictions recognized as adequate by the GDPR or the applicable Data Protection Legislation. Any transfer of Personal Data under the GDPR to Third Countries or international organizations requires prior approval from the Controller.

11.2. Transfers must only occur under conditions that comply with the GDPR and other applicable Data Protection Legislation. This includes ensuring appropriate safeguards are in place and that all contractual obligations or legal mechanisms used to protect Personal Data during transfer meet or exceed the standards set forth in the GDPR.

11.3. The Processor agrees not to transfer any Personal Data outside the agreed territories without confirming the presence of adequate protections as required by Data Protection Legislation.

11.4. The Processor is responsible for ensuring that any Personal Data transferred to a Third Country for processing adheres strictly to this DPA, documented Instructions from the Controller, and the full spectrum of Data Protection Legislation.

12. Indemnity and limitation of liability

12.1. Each Party shall bear any fines imposed on them pursuant to Article 83 of the GDPR or under any other applicable Data Protection Legislation. The responsibility for the fines will fall on the Party named explicitly as the recipient of such sanctions.

12.2. In the event of a compensation claim related to data processing that may affect both Parties, the Party receiving the claim must promptly notify the other Party, providing full details and relevant documentation. Both Parties shall cooperate to prevent or minimize potential damage or loss resulting from such a claim.

12.3. Liability for damages caused by processing that infringes the GDPR or any applicable Data Protection Legislation shall be assigned to the Party responsible for the damage or infringement. The Processor will be liable only if it has not complied with the obligations of the GDPR specifically directed to processors or if it has acted outside or contrary to the lawful Instructions of the Controller and/or this DPA.

12.4. A Party shall be exempt from liability if they can demonstrate that they were not responsible in any way for the event giving rise to the damage.

12.5. Compensation for damages to a Data Subject resulting from a breach of this DPA or the applicable Data Protection Legislation shall be governed by Article 82 of the GDPR.

12.6. If either Party becomes aware of circumstances potentially detrimental to the other Party, they must immediately inform the other Party and engage in active collaboration to mitigate any possible damage or loss.

13. Renegotiation, Term, and Termination

13.1. This DPA becomes effective upon signing and will remain in force if the Processor processes Personal Data under the MSA and its Service Orders/AWS Subscriptions or any Consortium Agreement. Either Party may terminate this DPA with thirty (30) days' notice.

13.2. Each Party may request renegotiation of the DPA if there is a major change in ownership of the other Party or if significant changes in applicable Data Protection Legislation or interpretation thereof affect the Processing materially. Renegotiation does not affect the efficacy of the DPA unless agreed upon in writing by both Parties.

13.3. Provisions of this DPA that should survive termination, including, but not limited to, obligations regarding the handling of Personal Data, confidentiality, and Data Protection, shall continue in full force and effect post-termination.

13.4. If the Processor fails to comply with the DPA, the Controller is entitled to suspend its obligations under the DPA until the Processor remedies the breach and the resolution is accepted by the Controller.

14. Completion of Services

14.1. Upon termination of the MSA, the Processor shall cease processing Personal Data on behalf of the Controller, except where mandated by any relevant applicable law or Data Protection Legislation to retain Personal Data. If the Services do not automatically terminate the processing, the Controller shall instruct the Processor to either:

a) Delete, or
b) Return

to Controller all Personal Data processed under the MSA and this DPA.

14.2. The obligations related to secrecy and the duty of confidentiality shall continue to apply even after the cessation of the MSA and the DPA.

14.3. Until such data is deleted or returned, the Processor is required to continue complying with all provisions of the MSA and this DPA. Any processing of Personal Data by the Processor after the data is returned or deleted shall be regarded as unauthorized unless expressly agreed to or instructed by the Controller.

15. Notifications within this DPA

15.1. All notifications related to this DPA, including termination or Data Breaches, must be communicated to the designated contact person of the other Party via email or another expressly agreed-upon method.

16. Contact

16.1. Each Party shall appoint a contact person for the administration of this DPA and for cooperation on data protection matters. Contact details shall be mutually exchanged and updated as necessary to facilitate communication.

Controller: Institution *(as defined in MSA and its* Service Orders/AWS Subscriptions*)*
Name: As established in the MSA and/or the relevant Service Order/AWS Subscription
Email: As established in the MSA and/or the relevant Service Order/AWS Subscription
Phone: As established in the MSA and/or the relevant Service Order/AWS Subscription

16.2. If a change occurs in the contact person, the Party shall inform the counterparty immediately.

17. Governing law and disputes

17.1. When interpreting and applying this DPA, Swedish law and the GDPR shall apply with the exception of the choice of law rules. Any dispute arising out of the DPA that the Parties cannot resolve on their own shall be settled by a competent Swedish court.

17.2. All disputes or proceedings arising out of or in connection with this DPA shall be conducted in English, and both Parties agree to use English in all written and oral communications related to such disputes or proceedings.

18. Signatures

18.1. The Parties agree that execution of this DPA is made by industry-standard electronic signature software and/or by exchanging executed signature pages in .pdf format via email shall have the same legal force and effect as the exchange of original signatures and that in any proceeding arising under or related to this DPA, each Party hereby waives any right to raise any defense or waiver based upon execution of this DPA by means of such electronic signatures or maintenance of the executed agreement electronically.

IN WITNESS WHEREOF, the Parties have caused this DPA to be executed and delivered by their respective duly authorized officers as of the Effective Date.

DPA Instructions (Appendix)

This Appendix forms part of the Controller's written Instructions to the Processor as regards the Processing of Personal Data required for the Processor to provide the Services under the MSA.

Categories of Data Subjects	The processing of Personal Data concerns the following categories of Data Subjects: ● Patients. ● Participants in research projects or clinical trials. ● Other types of participants in research projects, clinical trials, or other kinds of healthcare activities.
Special Categories of Personal Data	The Personal Data processed concerns the following special categories of Personal Data: ● Data concerning Data Subject's health, such as pathology or radiological images or diagnosis information. ● *(ONLY WHEN APPLICABLE – Which requires to be specifically agreed in a Service Order/AWS Subscription, and subject to adequate and robust technical and organizational measures) Pieces of genomic data under the framework of a research project under a Service Order/AWS Subscription.*
The Processing includes the following types of Personal Data	Personal Data is processed concerning the following categories of Personal Data: ● Patient data only to the extent necessary to aid the Institution to pseudonymize or anonymize such data pursuant to the Services under the MSA and a Service Order/AWS Subscription. ● Health data, such as pathology or radiological images. ● *(ONLY WHEN APPLICABLE – Which requires to be specifically agreed in a Service Order/AWS Subscription, and subject to adequate and robust technical and organizational measures) Pieces of genomic data under the framework of a research project under a Service Order/AWS Subscription.* ● Direct or Indirect identifiers, such as: - Patient's Age (approximate / K-anonymity generalization) - Patient's Weight (approximate / K-anonymity generalization) - Patient's Size (approximate / K-anonymity generalization) - Patient's biological sex.
The time period in which data was processed or stored	The Processor does not determine the duration for which data is stored on the Platform. Data retention is governed by the terms specified in the Services and the MSA, including the time periods established in each Service Order/AWS Subscription, as well as compliance with applicable legal retention requirements (e.g., clinical trials). The Controller/Institution maintains full control over its data at all times and has the authority to retain or remove it as needed.
Processing purposes and activities	The main purpose is to deliver services within clinical consultation, education, and research as per the MSA and any of its signed Service Orders/AWS Subscriptions linked to the MSA. The Personal Data shall only be processed for the following purposes and activities, only when required as part of the MSA and a signed Service Order/AWS Subscription: ● To either anonymize or pseudonymize patient images and data or to assist the Controller in doing so. ● To store pseudonymized or anonymized images and data on behalf of the Controller to provide the Services. ● To assist authorized users of the Controller in making difficult or complex decisions, such as in the radiology or pathology fields.

	• To provide support for clinicians through mentorship from experienced professionals, such as radiologists and other specialized health care professionals. • To create and maintain online learning resources for training schemes for professionals and students (e.g., radiology or pathology training and/or resources). • For educational purposes, such as enable and maintain the educational platform and workspaces can be used either for events, courses, educational groups, or other general reference cases. • To enable collaborative research study workflows, including data transfer, data curation, and data analysis. • Enabling, facilitating, and maintaining the performance of research projects and clinical trials as part of the services. • To get clinical opinions on patient cases from healthcare professionals. • Examine individual patient case data to determine a possible diagnosis. • Use the data as a structured source of clinical references for the benefit of healthcare professionals. • Enable training, analysis, and/or development of AI tools. • Enable the Institution to transfer cohorts of data to local environments. • To improve and develop the Services or new services and to analyze the Institution's use of the Services, limited to the duration of the provision of the Services; • To ensure the technical functioning of the Services and to prevent the use of the Services. • To enforce the terms of the MSA, including protecting the rights, property, and safety of the Institution and third parties; • To respond to any queries the Institution raises with CMRAD and to provide Institution support in relation to the provisioning of our services; and • To fulfill requirements by law / to comply with the law.
Security measures, access, and logging requirements	The Processor shall implement technical and organizational measures *inter alia*: **Access** The Processor only gives access to the Personal Data based on the Controller's preferences when uploading or based on what is needed for that person to conduct his or her tasks. **Logging Requirements**: The Processor must maintain detailed logs of user activity and the processing of Personal Data. These logs should clearly document what actions were taken, who accessed the Personal Data, and the duration for which the logs are retained. Access to these logs is restricted to authorized personnel only, and logs must be regularly reviewed to detect and respond to unauthorized access. **Physical safety** Appropriate and adequate measures shall be taken to ensure the physical security of IT spaces, such as, but not limited to, access protection, fire protection, protection against power outages, theft protection, and protection against vandalism. **Access protection** Computer equipment and portable storage media that are not under supervision must be locked to protect against unauthorized use and influence. Access to Personal Data must be able to be checked afterward through logs. The logs must be checked regularly in order to detect unauthorized access to Personal Data. **Servers** Access to servers is restricted. There are routines in place that ensure that important updates for operating systems and applications are installed immediately when required. **Network security and malware protection** Networks must be protected against external attacks and information loss. Wireless networks must be protected with encryption. Inbound and outbound traffic must be handled via firewalls, for example. Software that regularly scans networks for viruses, trojans, and other forms of digital intrusion should be used and kept up to date.

	Backups Personal Data is regularly transferred to backup copies, which are kept separate and well-protected so that it can be recreated after a disturbance. There are documented backup routines. **Data communication** Connections for external data communication must be protected with such technical functions that ensure that the connection is authorized. Personal data transmitted via open networks must be protected with encryption. **Extinction and deletion** There are documented routines that ensure that personal data can be deleted when it is no longer necessary for the purpose and that it cannot be recreated. **Reporting of Personal Data Breaches** Procedures are in place to detect, record, report, and remediate Personal Data breaches and other security incidents. These include specifying communication methods, identifying responsible reporting parties, and outlining information compilation processes. In the event of a Personal Data breach, the Processor must promptly notify the Controller without undue delay, investigate and rectify any organizational shortcomings that contributed to the breach, and restore the availability and access to Personal Data in a reasonable timeframe. This ensures effective communication and action are taken to mitigate the impact of any security incidents. **Reporting of malfunctions and deficiencies** There are routines in place for reporting to the Controller or the authorities any vigilances or hazardous situations that could occur where the Platform has been involved. **Penetration tests** The Processor carries out periodic penetration tests. **Process for software development** The Processor has implemented a process for software development that follows an accepted method and that includes appropriate manual and automated testing. **Staff training** The requirements that apply to employees with access to systems are defined by the system owner. The requirements must relate to both safety and competence and must be documented and communicated. Employees must be trained regularly (at least once a year) in data protection. **Documentation of measures** The implementation and verification of all security measures are documented in our ISO 27001 compliance documentation and our IT Security White Paper, which can be made available upon the controller's request.