## SCHEDULE 1 TO THE MSBASE FOUNDATION GOVERNANCE PACKAGE:

## MSBASE/MGBASE DATA PROCESSING AGREEMENT (INCLUDING SCC)

This personal data processing agreement ("**DPA**") is entered into on this day

BETWEEN:

(1) Institution: _____

Registration No. (if applicable): _____

Address: _____

(the "Controller" and "Data Controller"); and

(2) MSBase Foundation Ltd, ABN. no. 23 109 714 310, of Central Clinical School, Level 6, The Alfred Centre, 99 Commercial Road, Melbourne VIC 3004, AUSTRALIA (the "**Processor**" and "**Data Processor**").

The above parties are hereinafter each referred to as a "**Party**" and jointly as the "**Parties**".

### 1 INTRODUCTORY PROVISIONS

1.1 The Parties have previously, or in conjunction with this DPA, entered into an agreement concerning services relating to the MSBase Foundation's Services in accordance with the Participation Agreement, (the "**Participation Agreement**").

1.2 This DPA governs the rights and obligations of the Data Controller and the Data Processor when the Data Processor processes personal data on behalf of the Data Controller, pursuant to the Participation Agreement.

1.3 Appendix 1 only applies if and to the extent MSBase processes personal data on behalf of a Data Controller that qualifies as a controller with respect to that personal data under GDPR Laws. Annex 1 A, Annex 1 B, Annex II, and Annex III apply in respect of all Applicable Data Protection Legislation to the extent relevant.

1.4 If the information stipulated in the Participation Agreement conflicts with this DPA, this DPA shall take precedence.

1.5 This DPA aims to meet the current requirements for a DPA in accordance with Applicable Data Protection Legislation.

1.6 This DPA shall remain in force for as long as the Processor processes personal data on the Controller's behalf. This DPA applies to and covers any changes, additions, or amendments to the Participation Agreement unless the Parties enter into a new data processing agreement. If the Participation Agreement is terminated and a new contract with a similar scope and purpose to the Participation Agreement is entered into between the Parties, while a new data processing agreement is not entered into, this DPA shall apply to the new Participation Agreement. This applies also if an explicit reference is made to this DPA in a contract between the Data Controller and Data Processor.

### 2 DEFINITIONS

2.1 To the extent that the Applicable Data Protection Legislation contains terms similar to those used in this DPA, such terms shall have the same meaning as in the Applicable Data Protection Legislation.

| Term | Meaning |
|---|---|
| Applicable Data Protection Legislation | means all privacy and personal data legislation applicable to the personal data processing that is carried out under this DPA, which may include regulations and decisions of competent authorities applying the GDPR Laws. |
| Controller | means the party identified as the Controller at the start of this DPA acting as a controller under Applicable Data Protection Legislation in respect of data provided to the Processor under the Participation Agreement. |
| Data Controller | means Controller |
| Data Processor | means Processor |
| DPA | means this DPA and its appendices. |
| GDPR Laws | means the EU General Data Protection Regulation (Regulation 2016/679) (the "**GDPR**") and/or the UK General Data Protection Regulation (the "**UK GDPR**") and any EU Member State and/or UK laws made under or pursuant to the GDPR and/or UK GDPR. |
| Participation Agreement | means the agreement titled "Participation Agreement" between the parties to this DPA for the provision of the services described in that agreement |
| Processor | means the party identified as the Processor at the start of this DPA acting as a processor under Applicable Data Protection Legislation in respect of data received from the Controller under the Participation Agreement. |
| Service | means the service or services provided by the Data Processor in accordance with the Data Controller's instruction as described in this DPA and in the Participation Agreement. |
| Sub-processor | means the legal person who processes personal data on behalf of the Data Processor. |

## 3 APPENDICES AND HIERARCHY

3.1 This DPA comprises the following appendices:

| | |
|---|---|
| Standard Contractual Clauses ("**SCC**") | Appendix 1 |

3.2 In the event of a conflict between the documents, they shall take precedence in the order set forth below:

| | |
|---|---|
| Standard Contractual Clauses ("**SCC**") | Appendix 1 |
| Data Processing Agreement ("**DPA**") | |

## 4 PROCESSING OF PERSONAL DATA

4.1 The Data Processor shall ensure compliance with Applicable Data Protection Legislation as well as its obligations under this DPA when processing personal data on behalf of the Data Controller.

4.2 The Data Processor may only process personal data on behalf of the Data Controller in accordance with the Data Controller's documented instructions as set out in Annex 1 B, unless the Data Processor is, according to applicable laws and regulations, required to disclose personal data that the Data Processor processes on behalf of the Data Controller.

4.3 Excluding the Data Controller's right to alter its instructions in accordance with section 4.7, the Data Controller's instructions regarding the processing, follow solely from this DPA and, to the extent relevant, Appendix 1.

4.4 The Data Processor shall immediately inform the Data Controller if, in its opinion, the Data Processor has not received sufficient instructions to process personal data in accordance with its obligations pursuant to the Participation Agreement or if, in the Data Processor's opinion, an instruction infringes Applicable Data Protection Legislation, and defer the processing until further instructions from the Data Controller.

4.5 The Data Processor shall, without undue delay, inform the Data Controller about technical, organisational or financial changes, including changes in the ownership, which are likely to affect the Data Processor's capability of complying with its obligations in accordance with this DPA.

4.6 Any changes to the Data Controller's instructions shall be negotiated separately and, to be valid, documented in writing in Annex 1 B.

4.7 The Data Controller warrants the Data Processor that:

- it has the right to lawfully supply the personal data to the Data Processor and that it has a legal basis for transmitting the personal data to the Data Processor and to allow it to be processed and used for the purposes specified in the Participation Agreement.
- any personal data which it transmits to the Data Processor will be accurate and up to date and that the Data Controller shall have the sole responsibility for the legality, reliability, integrity, accuracy and quality of that data.
- it shall comply with all Applicable Data Protection Legislation (including ensuring that the instructions it provides to the Data Processor in relation to the processing and collecting of such personal data also comply with Applicable Data Protection Legislation).

## 5 THE DATA PROCESSOR'S OBLIGATIONS TO ASSIST THE DATA CONTROLLER

5.1 The Data Processor shall assist the Data Controller in fulfilling its obligations in accordance with Applicable Data Protection Legislation per the Data Controller's request and to the satisfaction of the Data Controller.

5.2 When the Data Processor assists the Data Controller in fulfilling the Data Controller's obligations under Applicable Data Protection Legislation in accordance with section 5.1 above, consideration shall be given to the type of processing it refers to, and the information available to the Data Processor. In order to avoid any misunderstandings, nothing in this section shall be interpreted as indicating that the Data Processor may act on behalf of the Data Controller. The Data Processor may only act to fulfil its obligations vis-à-vis the Data Controller.

## 6 SECURITY AND CONFIDENTIALITY

6.1 The Data Processor undertakes to take appropriate technical and organisational measures to protect the personal data being processed under this DPA in accordance with Applicable Data Protection Legislation. The Data Processor shall ensure that its service fulfils the requirements of the principles of privacy by design and privacy by default in line with the Applicable Data Protection Legislation as set out in the Participation Agreement and this DPA.

6.2 The Data Processor has implemented the technical and organisational measures set out in the instruction and undertakes not to substantially change these or otherwise change the security measures in a way that results in a lower level of information security than the one intended in section 6.1 and the instruction provided in Annex 1 B. Also, the MSBase Information Security Policy is provided to the Data Controller as part of the MSBase governance package and it provides information about the details of the technical and organisational security measures implemented by the Data Processor.

6.3 The Data Processor is obliged to immediately inform the Data Controller if the Data Processor considers that the implemented security measures no longer comply with the requirements set out in the Applicable Data Protection Legislation and wait for further instructions from the Data Controller.

6.4 The Data Processor undertakes not to, without the Data Controller's prior written consent, disclose or otherwise make personal data processed under this DPA available to any third party, except for approved sub-processors engaged in accordance with this DPA.

6.5 The Data Processor shall be obliged to ensure that only such staff and other Data Processor representatives that directly require access to personal data in order to fulfil the Data Processor's obligations in accordance with this DPA have access to such information. The Data Processor shall also ensure that the personnel understand what confidentiality obligation entails.

6.6 The Data Processor's obligations under this section 6 shall apply even if the DPA otherwise ceases to apply.

## 7 PERSONAL DATA BREACHES

7.1 The Data Processor shall without undue delay, and no later than within 24 hours, after finding out about a personal data breach, notify the Data Controller.

7.2 A notification pursuant to section 7.1 shall include all information which may reasonably be required by the Data Controller to fulfil its obligations under Applicable Data Protection Legislation. Such information includes e.g. a description of:

i. the nature of the personal data breach, categories of and the approximate number of data subjects affected, categories of and the approximate number of categories of personal data included;

ii. likely consequences as a result of the data breach; and

iii. a description of the measures taken to rectify the personal data breach or to mitigate its potential adverse effects.

7.3 If and to the extent it is not possible to provide all the information at the same time, the information may be provided in instalments without undue further delay.

7.4 Data Processor shall assist Data Controller with any information reasonably required to fulfil its data breach notification requirements.

## 8 SUB-PROCESSORS

8.1 The Data Processor has the Data Controller's general authorisation for the engagement of sub-processors from the list in Annex III. Prior to the Data Processor making changes to that list through addition or replacement of sub-processors, the Data Processor shall notify the Data Controller of such change ("Initial Notice") at least 14 days in advance of any such change. If the Data Controller initially objects to an additional or replacement of a sub-processor:

- the Data Processor shall provide the Data Controller with any additional information reasonably requested by the Data Controller to enable the Data Controller to assess whether the use of the proposed sub-processor will ensure the Data Processor's compliance with this DPA and the Applicable Data Protection Legislation;
- subsequently, if the Data Controller (acting reasonably) can demonstrate to Data Processor that such compliance will not be maintained through the proposed sub-processor, the Data Controller shall be entitled to terminate the Agreement on 28 days' written notice.

8.2 Where Data Processor authorises any sub-processor as described in clause 8.1, the Data Processor shall:

- restrict the Sub-processor's access to Data Controller's personal data only to what is necessary to maintain the Services or to provide the Services to Data Controller in accordance with Annex 1 B and Data Processor will prohibit the Sub-processor from accessing the personal data for any other purpose.
- enter into a written contract with the Sub-processor that requires it to comply with the same data processing obligations as those contained in this DPA, and, upon the Data Controller's written request, provide the Data Controller with copies of such contracts; and
- be accountable to the Data Controller for the acts or omissions of any Sub-processor as if such acts or omissions were acts or omissions of the Data Processor.

8.3 If the Data Processor intends to engage or replace a Sub-processor, the Data Processor shall inform the Data Controller in writing when providing the Data Controller with an Initial Notice in accordance with clause 8.1.

The information about the Sub-processor shall as a minimum include:

(i) company name,

(ii) company registration number (or equivalent),

(iii) head office (address and country),

(iv) categories of personal data and data subjects, as well as

(v) where the personal data will be processed.

8.4 The Data Controller recognises and accepts that the Data Processor, in accordance with what is stated in Annex III, is engaging Microsoft Azure Australia ("Microsoft") as an approved Sub-processor, and that the Data Processor has entered into a data processing agreement with Microsoft based on Microsoft's standard data processing agreements. Provided that and to the extent it does not cause Data Controller or Data Processor to be in breach of any Applicable Data Protection Legislation, Data Processor shall not be obligated to enforce on Microsoft other obligations regarding the processing of personal data other than what is contained in the Microsoft standard data processing agreement that has been entered into between Microsoft and the Data Processor.

**9 TRANSFERRING PERSONAL DATA TO A THIRD COUNTRY**

9.1 By using the Services of the Data Processor, the Data Controller transfers personal data to Australia. The Data Controller agrees to the transfer of personal data to, or access to personal data from Australia or other locations outside the EU/EEA, as provided in Annex 1 B.

9.2 To the extent that the GDPR Laws apply:

9.2.1 the Parties accept and enter into the EU Commission's Standard Contractual Clauses in accordance with Appendix 1;

9.2.2 the Data Processor undertakes to enter into the EU Commission's Standard Contractual Clauses with its Sub-processors; and

9.2.3 the Data Controller's and the Data Processor's rights and obligations are regulated in the EU Commission's Standard Contractual Clauses when the processing of personal data entails transferring of personal data to countries outside the EU/EEA. The rights and obligations stipulated in the Standard Contractual Clauses are supplemented by this DPA.

9.3 The Data Processor shall inform the Data Controller if an adequate level of protection can no longer be guaranteed for the transfer of personal data to, or access from, a country outside the EU/EEA or if the transfer or processing can, in any other way, be considered contrary to the Applicable Data Protection Legislation. Furthermore, in such instances, the Data Processor shall immediately take steps to ensure that personal data can continue to be processed in accordance with the applicable Data Protection Legislation and inform the Data Controller of the measures taken.

**10 REQUEST FOR INFORMATION AND DISCLOSURE OF PERSONAL INFORMATION**

10.1 In cases where a data subject or other third-party requests information from the Data Processor in respect of processing of personal data which belongs to the Data Controller, the Data Processor shall refer such data subject or third party to the Data Controller.

10.2 In the event a public authority requests the type of data as set forth in subsection 10.1, the Data Processor shall immediately inform the Data Controller of the request and the

Data Processor and the Data Controller shall, in consultation, agree on a suitable course of action.

10.3 The Data Processor shall not act on behalf of the Data Controller.

10.4 The Data Processor shall not disclose or make any personal data which belongs to the Data Controller available unless the Data Processor is under legal obligation or court or public authorities' order to disclose the information.

10.5 If an obligation to disclose information as stipulated in 10.4 above emerges, the Data Processor shall immediately inform the Data Controller of such situation and request confidentiality in conjunction with such disclosure.

## 11 AUDIT AND DOCUMENTATION

11.1 The Data Processor undertakes to document and keep records of the measures taken by the Data Processor in order to comply with its obligations under this DPA and Applicable Data Protection Legislation.

11.2 The record shall contain, at a minimum, the following information:

a) Name and contact details of the Data Processor and the Data Controller, including the contact details of the data protection officers of the Data Processor and the Data Controller, where applicable;

b) The purposes of the processing;

c) A description of the data subjects and of the categories of personal data;

d) The categories of processing which have been, and are being, carried out on behalf of the Data Controller;

e) The envisaged time limits for erasure of the different categories of data;

f) Specification of the transfer of personal data to a third country, outside the EU/EEA or international organisation, the legal basis for the transfer, and when applicable, a transfer impact assessment including a description of the technical and organisational security measures;

g) A general description of the technical and organisational security measures taken by the Data Processor.

11.3 The Data Controller shall be entitled to take measures necessary to verify that Data Processor is able to comply with its obligations under this DPA, and that the Data Processor has in fact undertaken the measures to ensure such compliance. Data Processor undertakes to make available to the Data Controller all information and all assistance necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including on-site inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

11.4 If an audit pursuant to this section 11 indicates that the Data Processor has breached its obligations under this DPA or Applicable Data Protection Legislation, the Data Processor shall, without undue delay, remedy such deficiency.

## 12 COMPENSATION

12.1 In light of the formulation of the Services, the Data Processor shall be entitled to compensation for processing of personal data required by the Data Controller in accordance with what is stated in this clause 12.

12.2 The Data Processor will be entitled to reasonable compensation on a time and materials basis in accordance with the then hourly rates in Data Processor's rate card to the extent the Data Controller

i. requires the Data Processor to assist the Data Controller in accordance with clauses 5.1, 10.1 or 7,

ii. requires any audit in accordance with clause 11, and/or

iii. requires measures to be made following upon completion of processing in accordance with clause 14.

The right to compensation only applies to the extent the measure is not already part of the Services or the Services' functionality.

12.3 In case of changed instructions in accordance with clause 4.7, the Data Processor shall be entitled to compensation for any documented additional costs for the performance of the Services which are due to the change, unless the change is caused by general demands on the Services that cannot be specifically attributed to the Data Controller, e.g. amendments or changes to applicable legislation or industry standards. The Data Processor shall further not be entitled to compensation to the extent the change otherwise corresponds to the obligations that a supplier of similar services as the Services normally can be expected to offer to its Centres on reasonable terms and conditions.

**13 LIABILITY**

13.1 A party shall be fully liable for and indemnify the other party for any claims attributable to any damage caused by and losses incurred as a result of the other party not fulfilling its obligations under this DPA or Applicable Data Protection Legislation.

13.2 In case of claims from data subjects arising from a breach by the other party of this DPA or breach of Applicable Data Protection Legislation the party who has been held liable for (or otherwise incurred liability in relation to) the claim shall be entitled to regressively recover the share of such losses which, according to the Applicable Data Protection Legislation, is attributable to the other party, and a fair share of the litigation costs which that party has incurred in relation to such dispute with the Data Subjects.

13.3 A party who is subject to claims from a Data Subject shall:

i. without undue delay notify the other party in writing of stated claims, if it is probable that claims against the other party pursuant to this clause 13 may be made,

ii. under negotiation or trial in court and before any settlement or other arrangement with the Data Subject allow the other party

a. to get access to the Data Subject’s and the party’s pleadings and any other correspondence; and

b. to comment on these, which are also reasonably taken into account to the extent that the comments may have an impact on the size of the claim for damage.

13.4 A party’s liability to pay for damages under this clause 13 also applies after the DPA otherwise has been terminated.

## 14 MEDIATION

14.1 The parties shall endeavour to settle any dispute arising out of or relating to this agreement, including with regard to its existence, validity or termination, by mediation administered by the Australian Disputes Centre (ADC) before having recourse to arbitration or litigation.

14.2 The mediation shall be conducted in accordance with the ADC Guidelines for Commercial Mediation operating at the time the matter is referred to ADC (the Guidelines).

14.3 The terms of the Guidelines are hereby deemed incorporated into this agreement.

14.4 This clause shall survive termination of this agreement.

## 15 MEASURES IN CONNECTION WITH THE TERMINATION

15.1 When this DPA expires, the Data Processor shall, at the Data Controller's request and per the Data Controller's instructions, permanently delete, or return in a format that the Data Controller chooses, all personal data processed in accordance with the DPA to the Data Controller, unless the Data Processor is required by law to save a copy of the personal data.

15.2 In this context, deletion means that the personal data is deleted in accordance with the industry standard in force at any given time in order to make it impossible for the data to be recreated using technology or method known at the time of deletion. This shall also apply to personal data that has been processed for logging and security purposes.

_____

## APPENDIX 1

## STANDARD CONTRACTUAL CLAUSES FOR TRANSFER OF PERSONAL DATA

### STANDARD CONTRACTUAL CLAUSES Transfer controller to processor

SECTION I

***Clause 1***

**Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

***Clause 2***

**Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### *Clause 3*

### Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module Two: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Module Two: Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### *Clause 4*

### Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### *Clause 5*

### Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

### *Clause 6*

### Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

### *Clause 7*

### Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## SECTION II – OBLIGATIONS OF THE PARTIES

### *Clause 8*

### Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

### *Clause 8.1* Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

### *Clause 8.2* Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

### *Clause 8.3* Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### *Clause 8.4* Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

### *Clause 8.5* Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

### *Clause 8.6* Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### *Clause 8.7* Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

### *Clause 8.8* Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### *Clause 8.9* Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

### *Clause 9*

### Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

### *Clause 10*

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

**Data subject rights**

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

***Clause 11***

**Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

***Clause 12***

**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### *Clause 13*

### Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

### *Clause 14*

### Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

## Clause 15

## Obligations of the data importer in case of access by public authorities

### *Clause 15.1* Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

### *Clause 15.2* Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of

destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

### *Clause 16*

### Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

### *Clause 17*

### Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of [enter country].

***Clause 18***

**Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of [enter country]

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

_____

## ANNEX I A.

### LIST OF PARTIES

**Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. Centre name: _____

   Address: _____

   Contact person's name, position and contact details:

   - Principal Investigator: _____
   - Centre Authority *(optional)*: _____
   - Where applicable, Data Protection Officer/representative in the EU:

   Activities relevant to the data transferred under this DPA:

   Registration, collection, storing, processing and distribution of personal data for the purposes described in Annex 1 B.

   Signature: _____ Date: _____

   Name: _____ Position: _____

   Role (controller/processor): Controller

2. .....

**Data importer(s):** *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: MSBase Foundation Ltd.

   Address: Central Clinical School, Level 6, The Alfred Centre

   99 Commercial Road

   Melbourne VIC 3004, AUSTRALIA

   Contact person's name, position and contact details:

   - Prof Helmut Butzkueven; Managing Director; info@msbase.org
   - Rein More; Data Protection Officer; dpo@msbase.org

   Activities relevant to the data transferred under this DPA:

   Registration, collection, storing, processing and distribution of personal data for the purposes described in Annex 1 B.

   Signature: _____ Date: _____

   Name: Helmut Butzkueven Position: Managing Director

   Role (controller/processor): Processor

## ANNEX I B.

## DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

Centre Patients

MSBase/MGBase Members

*Categories of personal data transferred*

**Centre Patients – MSBase Registry Minimum Dataset**

Patient profile information (Patient GUID, Gender, Month and year of birth, Date of MS onset), Centre visits (Visit Date, KFS, EDSS), Paraclinical tests (Test date, Test type), Relapses (Relapse Date, CNS region, Information on corticosteroids), Treatments (Treatment ID, Start date, End date)

**Centre Patients – MGBase Registry Minimum Dataset**

Patient profile information (Patient GUID, Gender, Month and year of birth), MG Diagnosis (Disease category, Date of onset), Visit information (MRS, MGC, MGFA, MGFA PIS, MG-ADL), Paraclinical tests (Test date), Exacerbation (Date of onset, Symptoms, Treatment site), Treatment (Treatment type, Start date, End date)

**Centre Patients – MSBase/MGBase Registry Comprehensive Data Dictionary (optional data fields)**

Available to download from the Members Resources section of the MSBase and MGBase Registry websites (www.msbase.org; www.mgbase.org)

**MSBase/MGBase Member's User Profile Data Fields**

Title, First name, Last name, Email, Birth year, Gender, Country of practice, Preferred phone, Profession/Role, University/Medical School, Year of highest medical degree, EDSS certification, Affiliation for publication purposes

**MSBase/MGBase Member's Centre Profile Data Fields**

Centre name, Hospital, Department, Street Address, City, Country, Postal code, Primary phone, Fax

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

The operations of the MSBase Foundation require processing of sensitive data in large scale. Thus, all processing activities are structured in a manner which protects sensitive data in an appropriate manner. As such, the technical and organizational measures taken to protect the personal data processed by the MSBase Foundation in general are designed to primarily protect sensitive data, but the same measures are applied to all processing activities. There are thus no additional security measures which only apply to processing of sensitive data. More information about the security measures may be found in Annex II.

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

Personal data is transferred on continuous basis or periodically at the discretion of the data controller.

*Nature of the processing*

Registration, collection, storing, processing and distribution of personal data for the purposes described below.

*Purpose(s) of the data transfer and further processing*

i. Provisioning of the web-based MSBase and MGBase Registries and the locally installed MSBase Data-entry Software (MDS), and to provide operational and administrative support, enabling Centers and their Principal Investigators to conduct analyses and studies using the MSBase/MGBase Registry Platform.
ii. System development and testing to ensure quality of Services provided in accordance with i) above.
iii. Maintenance and care of registry platforms.
iv. Transfer of data to third parties as part of any research project or other relevant data sharing initiative that the Data Controller wishes to pursue, as further instructed on a case-by-case basis in relation to the specific recipient and purpose of the transfer.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

The MSBase Foundation and sub-processors will store the data for as long as permitted by the Data Controller. If the MSBase Foundation can no longer identify a Data Controller, the relevant data will be deleted.

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

i. Microsoft Azure

Microsoft Azure Cloud hosts the SQL database that stores the pseudonymized (codified) patient data of patients that have been consented by the Centre. Once a patient record has been consented, they are "enrolled", and the codified data is pushed up to the MSBase/MGBase Registry from Authenticated MSBase/MGBase registered centres. This pseudeonymised (codified) patient data is currently retained indefinitely but can be removed at any point in time that a Centre decides to either unenroll a single patient record OR cease participation in the MSBase/MGBase Registry. These requests are submitted in writing to the MSBase Foundation and are described in the Participation Agreement.

ii. Kiandra IT

Kiandra have developer and system administrator accounts to the production environment containing the MSBase/MGBase Registry, (Azure Cloud, via the Microsoft Azure Portal) Access is primarily granted for development and maintenance activities as well as configuration and server management. Access is tightly controlled and documented. Kiandra are only able to read / delete data from the SQL database where Registry data is stored, via a well defined Support Process which includes a Ticket logged by an MSBase Foundation Administrator in the Service Desk Tool. All

requests are tracked, stored and extractable for reference. Kiandra has no access to personal patient data at a Centre, with the exception that a Kiandra Developer may be "exposed" to such data during a Virtual / Online Meeting, for the purposes of supporting a Centre. Kiandra and all its employees are subject to a Non-disclosure / Confidentiality Agreement signed between Kiandra and the MSBase Foundation.

iii. Icometrix & University of Sydney MRI repository

Patient consent is required for participation. Anonymised QMRI (Quantitative MRI) Metrics from Icometrix and University of Sydney QMRI Metrics are pushed to the MSBase Registry and matched against the already existing MSBase Patient ID. There is no personal identifiable information in any of the records which are then stored indefinitely in the MSBase Registry.

iv. ProSynergie Sarl

Prosynergie provides IT Support services to develop and maintain the iMed Application. Prosynergie have no access whatsoever to the MSBase Registry or any of the pseudonymised patient data stored in it. In some instances, only where required and as needed, Prosynergie Technical Lead may be exposed to patient data for the duration of a support call with a Centre that may be experiencing issues within iMed, or for the purposes of upgrading the iMed application. Duration is short, <1 week and intermittent. Prosynergie and all its employees are subject to a Non-disclosure / Confidentiality Agreement signed between Prosynergie and the MSBase Foundation.

.....

## ANNEX I C.

**COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

[enter the competent supervisory authority/ies]

## ANNEX II

## TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

*Measures for:*

a) *Ensuring ongoing confidentiality*

- MSBase Foundation has a Confidentiality Agreement which must be signed and adhered to by all MSBase Foundation Staff, Contractors, Researchers, Board and Scientific Leadership Group members. Confidential and sensitive information is then handled by the good judgement of staff (having regard for privacy and health record laws)

b) *Protection of data during transmission*

- The MSBase/MGBase Registry is hosted in a private Microsoft Azure tenancy. The Azure Database is protected by an IP firewall, and it leverages Azure Key Vault for the storage of all Keys required to allow end-to-end encryption.
- The MSBase/MGBase Registry database is encrypted at Rest, using Windows Azure's SQL Transparent Data Encryption (TDE). This helps to protect against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups, and transaction log files at rest.
- Data is transit is protected via TSL 1.2.
- TDE encrypts the storage of the entire database with the 256-bit AES algorithm and uses a symmetric key called the database encryption key. The built-in server certificate is unique for each SQL database server, and Microsoft automatically rotates these certificates at least every 90 days. (Per Azure's security)
- These keys are maintained in Microsoft Azure Key Vault Manager. No other copies are maintained.
- Exported data is pasword protected by the relevant Administrator or PI doing the export. The password for the exported (zip) files is emailed separately for additional security.

c) *Protection of data during storage*

- The section above regarding TDE encryption also applies to protection of data during storage in the MSBase Registry in Azure.
- MSBase/MGBase Centres maintain full control over their own data at their premises, the MSBase Foundation recommends that Centres ensure adequate SQL backup processes to protect their data, reducing the reliance on the availability of the Registries data.

*d) Ensuring physical security of locations at which personal data are processed*

- The MSBase/MGBase Registry platform is hosted in the Microsoft Azure South East Australia data Centre. This is a secure facility and incorporates all the security controls required for meeting ISO27000, and SOC-1 and SOC-2 reporting requirements. Public access to the data halls where the servers reside is not possible under any circumstances, and Microsoft Australia employs a host of physical and logical access controls to ensure that unauthorised physical access to hardware and virtual machines is not possible. Microsoft technicians who are authorised to physically access hardware do not have access to the virtual machines or the data stored by clients. All access-related activities are fully logged and audited as part of Microsoft's ISO 27000 and SOC-2 certifications. A SOC-3 report (which is a publicly available summary of the SOC-2 report) is available from Microsoft.
- Physical access to the Registry infrastructure (being hosted in Microsoft's data Centres) is not possible
- More detail around physical security is detailed in the MSBase Foundation Information Security Policy Document

*e) Ensuring events logging*

- The online registry maintains basic created/modified and "date logged in" audits. The online registry uses Azure OOTB "out of the box" events logging and Azure Application Insights.

*f) Measures for internal IT and IT security governance and management*

- Responsibility for information security is detailed further in the relevant section in the MSBase Foundation InfoSec Policy
- Responsibility for User accounts is detailed further under the "User Accounts" section in the MSBase InfoSec Policy
- Device use: The Monash Acceptable Use Policy has been adopted by the MSBase Foundation as if it were its own.
- External share drives such as Dropbox are configured to be restricted to "eyes only" permissions for the relevant audience.
- Furthermore, Information is classified into three classifications: 1) Public, 2) Confidential and 3) Sensitive and this is further detailed in the MSBase InfoSec Policy

*g) Measures of pseudonymisation and encryption of personal data*

- The Registries store only de-identified clinical data and does not store clinical data that could be used to identify a specific individual. The Data Entry System at each registered MSBase/MGBase Centre ingests Sensitive, personally identifiable data and this patient data is de-identified in both the XML file (from iMed) and the JSON file (from MDS) *before* sending it from the MSBase/MGBase Centre to the Registry. Data, once received by the Registry is re-classified as Confidential.

*h) Measures for ensuring availability and resilience of processing systems and services*

- As the MSBase Foundation uses Azure Cloud services, Azure supports high availability for most of its services including Azure VMs, SQL

Database and Azure Load Balancer. MSBase Registry in Azure has a recorded "up-time" with a reliability factor of 99.94% (at the time of writing this). . The MSBase/MGBase Registry is a highly available system - the only time the production system may be offline (temporarily) is during a major deploy.

- Azure Application Insights have also been configured to measure Failed Requests, and monitor Server Response Time, Server Requests and Availability

*i) Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

- The MSBase/MGBase Registry Azure SQL Database have been configured to execute "point in time backup procedures" with 30-day retention. A full Disaster Recovery (DR) plan has not yet been documented, but is planned to be implemented, configured and added to the planned MSBase Foundation Azure document.

*j) Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

- The MSBase Foundation undertakes an annual security assessment audit including full penetration testing across all MSBase/MGBase systems as well as vulnerability scanning. "Quick" vulnerability scans using free tools by the developer are done at each major release of the software.
- Recommended configurations implemented in line with Microsoft Azure Defender in Azure Portal. Recommended actions from the Azure portal are monitored on a regular basis.

*k) Measures for certification/assurance of processes and products*

- In accordance with the recently developed MSBase Foundation IT Project Management Methodology, several quality assurance "gates" have been implemented including QA testing and procedures documented by the software developer, integration testing automated into the Azure DevOps pipeline,
- User Acceptance Testing (This phase has been documented in the MSBase Foundation IT Project Management Methodology)
- Once a product, functionality, feature, or change has been released into Production, release notes are provided, and these are signed off in writing by the MSBase Foundation upon acceptance – usually via email.

*l) Measures for ensuring data minimisation*

- The MSBase and MGBase registries collect a highly specified, fully defined dataset, this is the minimum data required to fulfill the scientific mission of the MSBase/MGBase Investigators.

*m) Measures for ensuring data quality*

- Data quality is ensured using in-built checks and validations within the Data-entry Systems. Only explicitly defined data fields are able to be ingested into the Registry.

*n) Measures for ensuring limited data retention*

- Data Retention duration is determined by the Data Controller. If we are unable to identify a Data Controller, the Data is deleted.

*o) Measures for ensuring accountability*

- All Data Processing are specified in Data Processing Protocols, which are agreed to by the Data Controllers. Data processing activities are logged and these logs are audited annually by the Scientific Leadership Groups of MSBase and MGBase, which are the bodies representing the Data Controllers. The Data Protection Officer is able to ensure that the relevant data protocols have been followed correctly.

*p) Measures for allowing data portability and ensuring erasure*

- For data portability, we provide options to centres who will be able to direct how we access their data if necessary and always comply with a centre's request and ensure we follow their stipulated processes and procedures.
- Any centre who requests erasure can have all their data "hard-deleted" from the MSBase/MGBase Registry. This would be done via a formal written request from the Centre or its PI. The MSBase Foundation would log a support ticket with its technology partner who would do a hard-delete of centre's data. Proof can be provided after the fact that such a request has been fulfilled.

*q) Measures for user identification and authorization*

- MSBase/MGBase Registry members go through a sign-up process prior to being accepted as registry users. The MSBase Foundation Operations team manually check the eligibility and validity of Principal Investigators and their centres before approving membership requests. Only the lead neurologist at a centre may assume the role of Centre PI and authorize the contribution of consented patient data. Once verified, a PI and their Centre Authority must also read and execute the required governance documentation to finalise the process and commence participation in the Registry.

*Table of Documents referenced above:*

| **Sections Covered** | **Document Title** | **Date/version** |
|---|---|---|
| Section (a) through (f) | MSBase Information Security Policy | 2019.08.28 |
| Section (g) | MSBase Pseudonymisation Process – covering iMed and MDS Applications | 2022.05.31 |

| | | |
|---|---|---|
| Sections (h) and (i) | MSBase Azure Portal Configuration, Back-up, DR, Monitoring, and Insights | 2022.06.24 |
| Section (k) | MSBase IT Project Management Process & Methodology<br>Test Strategy | |

_____

## ANNEX III

## LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

*This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).*

The controller has authorised the use of the following sub-processors:

1. Name: Microsoft Azure, Australian Business Number: 29 002 589 460

   Address: Australia Southeast Datacentre, Victoria

   - Requests for contact should be made through the MSBase Foundation Data Protection Officer, Rein More; rein.more@monash.edu

   Description of processing can be found on page 23.

2. Name: Kiandra IT, Australian Business Number: 15 070 937 656

   Address: 28/570 Bourke Street, Melbourne 3000, VIC, Australia

   Contact person's name, position and contact details:

   - Martin Cooperwaite; Director; martin.cooperwaite@kiandra.com.au

   Description of processing can be found on page 23.

3. Name: Icometrix

   Address: Kolonel Begaultlaan 1b / 12, 3012 Leuven, Belgium

   Contact person's name, position and contact details:

   - Riet De Kempeneer; DPO, General Counsel, Secretary of the Board; dpo@icometrix.com; riet.dekempeneer@icometrix.com
   - Femke Podevyn; Customer success manager; femke.podevyn@icometrix.com

   Description of processing can be found on page 24.

4. Name: ProSynergie Sàrl, Swiss Commercial Register Number: CHE-113.526.430

   Address: Rue Alexandre Gavard, 16, 1227 Carouge, Switzerland

   Contact person's name, position and contact details:

   - Lionel Chalabi; Director; lionel@prosynergie.ch

   Description of processing can be found on page 24.

5. Name: University of Sydney

   Address: The University of Sydney, City Road Camperdown 2006, NSW, Australia

Contact person's name, position and contact details:

- Michael Barnett, MSBIR Project Lead; michael.barnett@sydney.edu.au
- Heidi Beadnall, MSBIR Project Control Board; hbea6517@sydney.edu.au
- Mark Kay, Director Research Post-Award; research.support@sydney.edu.au [Executive Level contact]

Description of processing can be found on page 24.