MSI Data Protection Requirements

These Data Protection Requirements shall apply to all dealings between MSI Reproductive Choices and/or its affiliates and subsidiaries (**MSI**) and its commercial suppliers insofar as personal data is or may be exchanged and are incorporated into all contracts with suppliers.

1. Definitions

1.1 **Agreement**: each agreement between MSI and a Supplier.

1.2 **Applicable Laws**: all applicable laws, statutes, regulations and codes from time to time in force.

1.3 **Supplier**: each commercial supplier which enters into a contractual relationship with MSI.

1.4 **parties**: means MSI and the Supplier and each is a party.

BACKGROUND:

(i) The parties have entered into the Agreement.

(ii) Either party may process personal data on behalf of the other in connection with the Agreement and therefore be either Data Controller or Data Processor.

1.1 **DEFINITIONS:**

Data Controller or **Data Exporter:** the party which discloses or transfers the Shared Data to a Data Importer (where applicable).

Data Processor or **Data Importer:** the party which receives or accesses the Shared Data from a Data Exporter (where applicable).

Data Protection Legislation: the Data Protection Act 2018, the UK GDPR, as defined in the Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit) Regulations 2019), and /or any other applicable national data protection legislation.

End Date: the date on which the Agreement terminates or expires, whichever is the earlier.

Other Confidential Information: all information and data, in whatever medium (including in written, oral, visual or electronic form) received from or relating to the Data Controller and its affairs (or that of its affiliates or its funders) including all know-how and business, financial, commercial, technical, operational, organisational, legal, management and marketing information, whether disclosed to the Data Processor by or on behalf of the Data Controller or otherwise acquired by the Data Processor during the Term.

Purpose: has the meaning given to it in the Data Scope provisions of the Agreement.

Shared Data: any Personal Data, Sensitive Personal Data, or Other Confidential Information shared by either party under the Agreement.

Start Date: the date on which the Agreement commences.

Term: the period from the Start Date to the End Date of the Agreement, or as otherwise agreed between the parties in writing.

1.2 "*Data Subject*", "*Personal Data*", "*Sensitive Personal Data"*, "*personal data breach*", "*Processing*", and "*Supervisory Authority*" are as defined in the Data Protection Legislation.

2 DATA PROCESSING OBLIGATIONS

2.1 Shared Data. The Data Processor agrees that it:

2.1.1 shall process Shared Data only on documented instructions from the Data Controller and to the extent reasonably necessary for the Purpose as described in the Data Scope provisions of the Agreement;

2.1.2 shall ensure, in accordance with Appendix 1, that each employee accessing Shared Data is under an obligation of confidentiality on terms no less onerous than this Agreement;

2.1.3 has obtained prior written consent from the Data Controller for the publication or disclosure of any Shared Data, including a report or document which includes, references, or derives analysis from Shared Data, and will provide a copy of any such document to the Data Controller for review and assent 30 days prior to publication; and

2.1.4 not attempt to identify any Data Subject(s) from any Shared Data, by any means whatsoever, nor claim to have done so.

2.2 Compliance. During the Term of this Agreement, the parties shall comply with all of their obligations under the Data Protection Legislation.

2.3 Sub-processing. The Data Processor has the Data Controller's general authorisation for the engagement of sub-processor(s) from an agreed list (Appendix 2), to process the Shared Data. The Data Processor will provide the Data Controller with at least 30 days' prior written notice of the addition of sub-processor(s) to this list and the opportunity to object to such addition. Where the Data Processor engages a sub-processor, it shall do so by way of a written contract that is at least as onerous as this Agreement. The Data Processor shall remain fully liable for all acts and omissions of its sub-processors with respect to the Processing of Shared Data.

2.4 Requests or complaints from Data Subjects. The Data Processor shall ensure that:

2.4.1 it co-operates with the Data Controller and ensures that it has appropriate technical and organisational measures (including those described in Appendix 1) in place to assist the Data Controller to comply with any request or complaints from Data Subjects when exercising their rights under the Data Protection Legislation (the "**Data Subject Rights"**);

2.4.2 it notifies the Data Controller within two (2) business days if it receives (i) a request from a Data Subject to exercise the Data Subject Rights; or (ii) a complaint or request relating to the Data Controller's obligations under the Data

Protection Legislation, and the Data Processor shall take no further steps in relation to the same until such time that it receives written instructions to do so from the Data Controller.

2.5 Assistance. The Data Processor shall provide relevant information and assistance requested by the Data Controller to demonstrate the Data Processor's compliance with its obligations under the Agreement and assist the Data Controller in meeting its obligations under applicable data protection and privacy laws including (but not limited to): (i) registration and notification obligations; (ii) accountability; (iii) ensuring the security of the Shared Data; and (iv) carrying out and documenting privacy and data protection impact assessments and conducting related consultations with data protection authorities.

3 TRANSFER OF SHARED DATA

3.1 Where the transfer of Shared Data is subject to the EU General Data Protection Regulation ((EU) 2016/679) ("**EU GDPR**") the parties agree:

3.1.1 "**2021 SCCs**" means the 2021 EU Standard Contractual Clauses (Module 2 Controller to Processor) ((EU) 2021/914) available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en, together with the Data Scope provisions of the Agreement and Appendix 1.

3.1.2 "**Adequacy Decision**" means a decision adopted by a competent authority with jurisdiction over the Data Processor declaring that a jurisdiction meets an adequate level of protection of Personal Data.

3.1.3 The 2021 SCCs will apply to any transfer of Shared Data that is subject to the EU GDPR (or was subject to the EU GDPR prior to its transfer to the Data Controller) to a Data Processor located outside of the European Economic Area.

3.1.4 Notwithstanding the foregoing, the 2021 SCCs will not apply to the extent the transfer of Shared Data is covered by an Adequacy Decision.

3.1.5 For the purpose of:

(a) Clause 9 of the 2021 SCCs, the parties agree that subcontracting will be in accordance with clause 2.3 of this Schedule;

(b) Clause 17 of the 2021 SCCs, the parties agree that the 2021 SCCs will 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 Ireland;

(c) Clause 18 of the 2021 SCCs, the parties agree that any dispute arising from the 2021 SCCs will be resolved by the courts of Ireland; and

(d) Annex I.C of the 2021 SCCs, the parties agree that Ireland's Data Protection Commission is the competent supervisory authority.

3.2 Where the transfer of Shared Data is subject to the laws of the United Kingdom (including the UK GDPR), the parties agree:

3.2.1 **"UK 2021 SCCs Addendum**" means the International Data Transfer Addendum to the 2021 SCCs;

3.2.2 the provisions of the UK 2021 SCCs Addendum, including **Error! Reference source not found.** 'Mandatory Clauses', shall apply in full;

3.2.3 for the purposes of Table 1 of the UK 2021 SCCs Addendum, the names of the parties, their roles and their details shall be as set out in **Error! Reference source not found.**;

3.2.4 for the purposes of Tables 2 and 3 of the UK 2021 SCCs Addendum, the terms of this Agreement, including the information set out in the Data Scope provisions of the Agreement and 0, shall apply;

3.2.5 for the purposes of Table 4 of the UK 2021 SCCs Addendum, neither party may end the UK 2021 SCCs Addendum; and

3.2.6 notwithstanding the foregoing, the UK 2021 SCCs Addendum will not apply to the extent the transfer is covered by an Adequacy Decision.

4 DATA RETENTION AND DELETION

The Data Processor shall immediately cease processing and ensure that any Shared Data is returned to the Data Controller or destroyed (by either secure shredding or permanent deletion from hardware, software and servers) in the following circumstances: (i) upon termination of the Agreement; and (ii) once processing of the Shared Data is no longer necessary for the Purpose, and in each case shall confirm this in writing with the Data Controller.

5 PERSONAL DATA BREACHES

5.1 If the Data Processor becomes aware of any personal data breach affecting the Shared Data, the Data Processor shall:

5.1.1 record the details of the suspected personal data breach in a security incident log and undertake an initial investigation immediately into the suspected personal data breach;

5.1.2 notify the key contact for the Data Controller within forty eight (48) hours after becoming aware of that event and take no further steps in relation to the same until it receives written instructions from the Data Controller;

5.1.3 fully co-operate with the Data Controller in the course of the investigation and any subsequent corrective actions arising therefrom, including any report to and investigation by the relevant Supervisory Authority and/or notification to any affected Data Subjects; and

5.1.4 following consultation with the Data Controller, implement any measures necessary to restore the security and integrity of any compromised Shared Data.

6 INDEMNITY

6.1 Without prejudice to any liability or indemnity clause in the Agreement, the Data Processor shall indemnify and keep the Data Controller indemnified against all actions, claims, demands, proceedings, damages, costs, charges and expenses (including reasonable legal expenses) whatsoever in respect of any breach of this Agreement.

7 TERMINATION

7.1 Without prejudice to any termination clause in the Agreement, the Data Controller may terminate the Agreement (i) for any reason by giving fourteen (14) days' notice, or (ii) immediately where the Data Processor commits a material breach of this Schedule and (if such breach is remediable) fails to remedy that breach within a period of seven (7) days after being notified to do so.

7.2 If Shared Data remains in the possession or control of the Data Processor following termination or expiry of the Agreement, this Schedule shall continue to apply until such Shared Data is returned to the Controller or permanently destroyed by the Data Processor.

7.3 Termination or expiry of the Agreement shall not affect any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of this Schedule which existed at or before the date of termination or expiry.

7.4 On termination or expiry of the Agreement, the following clauses of these Data Protection Requirements shall continue in force: clause 6 (Indemnity), clauses 7.1 and 7.3 (Termination) and clause 8 (General).

8 GENERAL

8.1 <u>Assignment and other dealings</u>. The Data Processor shall not assign, transfer, mortgage, charge, subcontract, declare a trust over or deal in any other manner with any of its rights and obligations under this Schedule, unless as otherwise provided for in this Agreement. The Data Controller may at any time sub-contract, assign, mortgage, charge, declare a trust over or deal in any other manner with any or all of its rights under this Schedule.

8.2 <u>Entire agreement</u>. These Data Protection Requirements supersede any clauses relating to data protection in the Agreement unless expressly stated by the parties in writing.

8.3 This Schedule, the Agreement and its other Schedules, if any, constitute the entire agreement between the parties.

8.4 Notice. Any notice or communication given to a party under or in connection with these Data Protection Requirements shall be in writing and shall be delivered by hand or by pre-paid first-class post or other next Business Day delivery service at its registered office (if a company) or its principal place of business (in any other case) with a copy by email to legal@msichoices.org.uk. This clause does not apply to the service of any proceedings or any documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

Appendix 1 – Security Standards

1 Security and Training

1.1 The Data Processor shall implement appropriate technical and organisational measures to ensure the security of the Shared Data against unauthorised or unlawful processing, to protect it against a personal data breach and to assist the Data Processor's obligations in respect of the same and Data Subject Requests.

1.2 The Data Processor warrants that it has in place appropriate technical and organisational security measures in order to:

1.2.1 prevent unauthorised or unlawful processing of the Shared Data and the accidental loss or destruction of, or damage to, the Shared Data; and

1.2.2 ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the Shared Data to be protected.

1.3 In respect of the employees of the Data Processor who are provided with access to the Shared Data, the Data Processor will take such steps which shall include but not be limited to:

1.3.1 taking reasonable steps to ensure the reliability of such persons;

1.3.2 ensuring that such persons are informed of the confidential nature of the Shared Data and are under an obligation of confidentiality in relation to the same no less onerous than this Schedule;

1.3.3 have undertaken training relating to the handling of Personal Data; and

1.3.4 are aware of their obligations and those of the Data Processor under the Data Protection Legislation and the Agreement.

1.4 The level, content and regularity of training referred to in clause 1.3.3 shall be proportionate to the staff members' role, responsibility and frequency with respect to their handling and processing of the Shared Data.

1.5 In return for having access to Shared Data, the Data Processor shall comply with the following procedures for saving and storing Shared Data:

1.5.1 where applicable, employees accessing CLIC data will adhere to the 'Use of CLIC data for research' Guidance Note (provided upon request);

1.5.2 datasets are saved on one of the following:

(a) password-protected and firewalled servers or computers in a physically protected area; and
(b) encrypted laptops or USBs only.

1.5.3 analytic output must be separated from raw data, and contain no client- or participant-identifiable data; and

1.5.4 where applicable, any CLIC analytical output must adhere to the guidance on small cell sizes set out in the ‘Use of CLIC data for research’ Guidance Note, to avoid deductive disclosure.

1.6 Routine service data will be deleted from local servers in a time-frame agreed by the research partners.