DATA TRANSMISSION AND USE AGREEMENT BETWEEN MEMBER ORGANISATIONS

OF

WORLD MARROW DONOR ASSOCIATION (WMDA)

Version 1.0, [May 18, 2019]

This Data Transmission and Use Agreement between WMDA Member Organisations ("**Agreement**") constitutes an agreement intended to govern personal data transfers between the member organisations of the World Marrow Donor Association (respectively "**Member Organisation(s)**" and "**WMDA**").

WMDA Member Organisations shall signify their intention to be bound by the Agreement by signing the accompanying signature sheet (**ANNEX 3**).

A record of each Member Organisation having signed the signature sheet will be available on the WMDA Share.

WHEREAS

1. Member Organisations maintain databases of adult donors and cord blood units available for use in hematopoietic stem cell transplantation, including data on human leucocyte antigen ("**HLA**") phenotypes and other relevant data of volunteer stem cell donors and cryopreserved cord blood units ("**CBUs**"). For purposes of this Agreement, the term "**HSC**" applies to hematopoietic stem cells from circulating blood as well as from marrow and from cord blood. Potential donors and actual donors of HSC are collectively referred to as "**Donors**".
2. Member Organisations are committed to make these data accessible to the other Member Organisations (either directly or through the WMDA), and healthcare professionals (e.g. transplant centre physicians, search coordinators) worldwide that search for a potential match for their patient ("**Patient**").
3. There are currently around 79 regular and 29 provisional WMDA Member Organisations.
4. Member Organisations wish to transfer relevant data, information, and other records relating to Patients, Donors, and CBUs ("**Data**"). ANNEX 1 sets out the scope, nature and purpose of the processing by the RECEIVING ORGANISATION, the duration of the processing, the types of Personal Data and the categories of Data Subjects.
5. The Data constitutes personal data and special categories of personal data within the meaning of the General Data Protection Regulation (EU) (2016/679) (respectively "**Personal Data**" and "**GDPR"**).
6. Member Organisations recognise the importance of protecting the privacy and confidentiality of Data exchanged to maintain the confidence and trust of Donors, Patients and regulators.
7. Each Member Organisation (the "RECEIVING ORGANISATION") that receives Data from another MEMBER ORGANISATION (the "SENDING ORGANISATION") under the terms of this Agreement shall only process Personal Data in accordance with the SENDING ORGANISATION's written instructions without having control over the purpose of and means for processing the Personal Data. A RECEIVING ORGANISATION does not make decisions concerning the use of the Data, the provision of the Data to third parties and other recipients, the duration of the storage of the Data, etc. For the avoidance of doubt, "process" and "processing" shall have the same meaning in the Agreement as in the GDPR.

AGREE AS FOLLOWS

1. Compliance with Applicable Laws

1.1 Each Member Organisation represents and warrants that all Data submission requirements, Data transmission and exchange, Data storage, use, confidentiality, access to and disclosure and Data reporting under this Agreement will comply with all data protection and privacy laws in force from time to time that apply to the exchange of Data by that Member Organisation, including without limitation, GDPR and all other local laws governing the collection, storage, use, disclosure and access to personal and health Data ("**Applicable Laws"**). All Member Organisations will co-operate as reasonably required to facilitate communication.

2. Scope of Data Exchanged

2.1 Unless otherwise agreed between Member Organisations, Data exchange will be limited to data elements required for the Purposes. Where practicable, each Member Organisation shall ensure that the Data it exchanges will be in a form that does not enable other persons outside of the SENDING ORGANISATION to identify the individual to whom the Data relates. The Data might include sensitive Personal Data: HLA results determined on DNA (genetic results), ethnicity and health-related Data (infectious disease marker results, blood group, HLA results) for, respectively, the primarily matching of Patients and Donors, to improve the accuracy of the probability matching between Patients and Donors, to improve the selection of a suitable Donor for a Patient.

3. Assurances by SENDING ORGANISATION

3.1 The SENDING ORGANISATION represents and warrants that it has obtained all licenses, permits and other certifications required under its respective governing laws to operate its respective organisation in the applicable jurisdiction(s) and will notify the RECEIVING ORGANISATION of any material change in status under applicable laws.

3.2 The SENDING ORGANISATION represents that it has obtained all necessary ethical review and governmental approval required under its respective governing laws to participate in the international exchange of the Data for hematopoietic stem cell search and transplant procedures, quality assurance purposes, and publication of organisation and search activity ("**Purposes**").

4. Processing of Data by RECEIVING ORGANISATION on instruction of SENDING ORGANISATION

4.1 The RECEIVING ORGANISATION will only process Data received from the SENDING ORGANISATION at the SENDING ORGANISATION's written instructions solely for the Purposes and as provided in this Agreement.

Purposes

4.2 The Purposes are set by the SENDING ORGANISATION and the RECEIVING ORGANISATION is not entitled to make any decisions concerning the Purposes.

Data quality assurance

4.3 The SENDING ORGANISATION is responsible for the quality of the Data provided to the RECEIVING ORGANISATION.

Disclosure to third parties

4.4 On behalf of the SENDING ORGANISATION the RECEIVING ORGANISATION will disclose Data to third parties for the Purposes and in accordance with the requirements set forth herein. On behalf of the SENDING ORGANISATION the Data will be shared with:

- Staff members of the RECEIVING ORGANISATION, to the extent necessary;
- Healthcare affiliated professionals with bonafide need to search for international Donors and obtain Data;
- (IT) service providers maintaining and developing RECEIVING ORGANISATION's services, to the extent data processor agreements have been concluded with these (IT) service providers in accordance with clause 4.6.

(the "**Users**")

4.5 RECEIVING ORGANISATION may use anonymous Data for purposes of internal studies, analysis and presentation to advance understanding in blood and marrow transplant. Any external publication will require permission of the SENDING ORGANISATION.

Sub-processor

4.6 SENDING ORGANISATION authorises RECEIVING ORGANISATION to engage another processor to process the Data (a "**Sub-Processor**"). In the event that RECEIVING ORGANISATION chooses to make any changes to its Sub-Processors, RECEIVING ORGANISATION will provide a 60-day written notice to all SENDING ORGANISATIONS of the change prior to the change. Should a SENDING ORGANISATION object to the change, the SENDING ORGANISATION will have the right to opt-out or de-list their Data. RECEIVING ORGANISATION must enter into an agreement with each of its Sub-Processors that imposes at least the same data protection obligations on the Sub-Processor as set out in this Agreement (including, where applicable, the protections set out at Clause 10.2 below). As between the SENDING ORGANISATION and the RECEIVING ORGANISATION, the RECEIVING ORGANISATION shall remain fully liable for all acts and omissions of any Sub-Processor appointed by the RECEIVING ORGANISATION pursuant to this clause.

SENDING ORGANISATION's prior consent

4.7 RECEIVING ORGANISATION may not provide Data to other than those described in Clause 4.4 or any Sub-Processor appointed under Clause 4.6, unless the SENDING ORGANISATION has given its documented instructions to that end.

Storage

4.8 RECEIVING ORGANISATION will not keep the Data for longer than is necessary for the Purposes for which the Data are processed. In case Union or national laws or regulations provide for a certain retention periods, RECEIVING ORGANISATION may retain the Data for that period of time.

5. Technical and organisational measures

5.1 The RECEIVING ORGANISATION undertakes to implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to secure the Data from unauthorized access, loss or any form of unlawful processing. Bearing in mind the state of the art and the costs of implementation, the security measures must be based on the WMDA Standards 2020 at a minimum. The RECEIVING ORGANISATION ensures that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it).

5.2 The RECEIVING ORGANISATION must limit access to and processing of the Data to those employees or other authorised representatives who need access to, or to process, such Data in order to conduct their work in connection with the Data. The RECEIVING ORGANISATION will ensure that unauthorized personnel do not have access to the Data and/or the data processing applications. The RECEIVING ORGANISATION certifies that all members of staff authorised to access the Data are obliged to observe confidentiality in respect of the Data of which they become aware.

5.3 The RECEIVING ORGANISATION will restrict access to the Data, and any other identifiable or anonymous data derived from the Data, to any third party, except for the furtherance of the Purposes in those instances in which access to the Data is consistent with applicable law and regulation and except for as stipulated in clause 4.4 – 4.7.

6. Demonstrating compliance

6.1 The RECEIVING ORGANISATION makes available to the SENDING ORGANISATION information necessary to demonstrate compliance with the obligations laid down in this Agreement. WMDA Standards (chapter 5 of WMDA 2020 Standards) will constitute a RECEIVING ORGANISATIONS' reasonable documentation to demonstrate compliance. Expenses necessary for demonstrating compliance to this Agreement, and achieving the requirements of the WMDA Standards, are costs that the RECEIVING ORGANISATION must bear. RECEIVING ORGANISATION will allow SENDING ORGANISATIONS to contribute to audits, including inspections, conducted by the SENDING ORGANISATION or another auditor mandated by the SENDING ORGANISATION. Any costs of additional audits that extend beyond the requirements in this agreement, those audit costs will be borne by SENDING ORGANISATION, unless it appears that RECEIVING ORGANISATION has infringed laws or regulations (including those concerning personal data protection) or if RECEIVING ORGANISATION has failed to comply with the obligations of this Agreement, and/or errors are found in the findings which must be attributed to RECEIVING ORGANISATION. In such cases, the cost of the audits will be borne by RECEIVING ORGANISATION. The SENDING ORGANISATION shall give RECEIVING ORGANISATION a thirty (30) days prior written notice of the audits, as well as of the

outside auditor mandated by SENDING ORGANISATION. RECEIVING ORGANISATION may, within seven (7) days after the notice, object on reasonable grounds to the auditor engaged. An audit may take place once a year as well as in the event of a concrete suspicion of misuse of Data. The RECEIVING ORGANISATION shall cooperate with such audits and shall not impose any conditions on its cooperation other than the SENDING ORGANISATION's auditors signing a commonly used and not unnecessarily onerous confidentiality statement (unless they are already held to confidentiality under their employment relationship with the SENDING ORGANISATION).

6.2 With regard to the foregoing, RECEIVING ORGANISATION will promptly notify the SENDING ORGANISATION if, in its opinion, an instruction infringes the provisions of the GDPR or other statutory provisions.

6.3 Where applicable, RECEIVING ORGANISATION will assist the SENDING ORGANISATION at all times to meet the obligations pursuant to the GDPR. More specifically RECEIVING ORGANISATION will assist the SENDING ORGANISATION to meet the obligations relating to the rights of the data subjects such as, but not limited to, the right of access, rectification, erasure or restriction of processing and the right to object. RECEIVING ORGANISATION will promptly, and in any case, within 5 days, notify the SENDING ORGANISATION of any communication from a data subject regarding the processing of their Personal Data, or any other communication (including from a supervisory authority) relating to either's obligations under GDPR in respect of the Personal Data.

6.4 RECEIVING ORGANISATION will assist the SENDING ORGANISATION at all times to meet the obligations pursuant to the GDPR, in particular with the security of Personal Data and, if applicable, with carrying out a data protection impact assessment.

7. Breach Notification

7.1 RECEIVING ORGANISATION will report any incident in regard to security and Personal Data breaches without undue delay, and in any case within 72 hours, to the SENDING ORGANISATION, such report will include all information reasonably required by the SENDING ORGANISATION to comply with its obligations under the GDPR.

7.2 If RECEIVING ORGANISATION becomes aware of a Personal Data breach, it will take all reasonable measures necessary to prevent further access to and spreading of Data. To this end, RECEIVING ORGANISATION will consult with the SENDING ORGANISATION and follow any of the SENDING ORGANISATION's instructions, unless SENDING ORGANISATION's instructions would violate Union or national laws and regulations to which RECEIVING ORGANISATION is bound. RECEIVING ORGANISATION will keep the SENDING ORGANISATION apprised at all times about the developments relating to the data breach and the measures that it is taking to minimise the consequences of the data breach and to prevent reoccurrence of the data breach.

7.3 Where necessary and as directed by SENDING ORGANISATION, RECEIVING ORGANISATION will cooperate with SENDING ORGANISATION in properly informing the data subjects.

8. Term and Termination

8.1 Each Member Organisation will be legally bound by this Agreement effective the date signing the signature sheet, contained in **ANNEX 3**. The Agreement will continue in force until the Member Organisation ceases to be a registered WMDA Member Organisation or until the Agreement is terminated as provided below.

8.2 Each Member Organisation may terminate this Agreement on sixty (60) days' prior written notice by means of a signed letter addressed to the WMDA clearly indicating withdrawal of its commitment to this Agreement. The WMDA will then inform all Member Organisations of the Member Organisation's withdrawal.

8.3 On termination of this Agreement, or earlier upon the request of the SENDING ORGANISATION, RECEIVING ORGANISATION must return to the SENDING ORGANISATION or dispose of, in accordance with the SENDING ORGANISATION's written instructions, all Data of the SENDING ORGANISATION pursuant to this Agreement, unless Union or national laws or regulations requires storage of the Personal Data. Representations and obligations to preserve the confidentiality of Data will survive the termination of this Agreement.

9. Data Transfers to Non-EU Countries

9.1 On behalf of the SENDING ORGANISATION, RECEIVING ORGANISATION may process Data outside the European Economic Area ("**EEA**") for the Purposes and as provided in this Agreement, particularly in respect of the provision of Data to third parties as laid down in clause 4.

9.2 If a SENDING ORGANISATION is situated inside the EEA and the RECEIVING ORGANISATION is located outside the EEA, the following applies. In the absence of an adequacy decision by the European Commission for the designated country or territory, the transfer will be governed by the standard contractual clauses, appended to this Agreement as **ANNEX 2**. To the extent one or more provisions of **ANNEX 2** may conflict with one or more terms of this Agreement, **ANNEX 2** shall prevail. For the purposes of **ANNEX 2**, the SENDING ORGANISATION is considered the "Data exporter" and the RECEIVING ORGANISATION considered the "Data importer".

10 Choice of law and forum

10.1 This Agreement shall be governed by the laws of the Netherlands except that ANNEX 2 to this Agreement shall be governed by the laws of the data exporter.

10.2 If the parties have entered into the standard contractual clauses at ANNEX 2, any dispute between the parties to this Agreement will be referred to the courts of the data exporter. Where the standard contractual clauses have not been entered into by the parties, the courts of The Hague in the Netherlands shall have the non-exclusive jurisdiction to settle any dispute, whether contractual or arising from unlawful act, arising out of this Agreement.

ANNEX 1

DATA PROCESSING

This ANNEX 1 includes certain details of the processing of the Personal Data as required by Article 28(3) GDPR (or equivalent provisions of any Data Protection Legislation).

Subject matter and duration of the Processing of the Personal Data

The subject matter and duration of the processing of the Personal Data are set out in the Agreement.

The nature and purpose of the Processing of the Personal Data

Each Party will process Donor and Patient Personal Data in order to facilitate the search for potential suitable donors of hematopoietic stem cells and to enable the transfer of Personal Data for transplantation purposes.

The types of the Personal Data to be Processed

Personal Data (including names, addresses, telephone numbers, email contact details).

Special category Personal Data (including health information, genetic information, ethnic information and racial information).

The categories of Data Subject to whom the Personal Data relates

Donors, Patients

The obligations and rights of the Controller

The obligations and rights of the Controller are set out in the Agreement and this ANNEX 1.

ANNEX 2

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

(the data **exporter**)

And

(the data **importer**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[1]

(1) The data importer agrees and warrants:

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against its third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case, the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9
Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

EEA Member Organisation that is transferring Donor and Patient Personal Data in order to facilitate the search for potential donors of HSC

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Non-EEA Member Organisation
Data subjects

The personal data transferred concern the following categories of data subjects (please specify):
Donors and Patients

Categories of data

The personal data transferred concern the following categories of data (please specify):

personal data (including names, addresses, telephone numbers, email contact details
Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

health information, genetic information, ethnic information and racial information

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Processing activities in order to facilitate the matching necessary for stem cell donor selection. The Data might include sensitive Personal Data: HLA results determined on DNA (genetic results), ethnicity and health-related Data (infectious disease marker results, blood group, HLA results) for, respectively, the primarily matching of Patients and Donors, to improve the accuracy of the probability matching between Patients and Donors, to improve the selection of a suitable Donor for a Patient.

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Compliance with the WMDA Standards (available on the WMDA's website), including (1) the adoption of a credible security framework (e.g., ISO 27001), and (2) ongoing oversight of cyber risks by data importer's highest governance committee.

ANNEX 3

SIGNATURE SHEET TEMPLATE

DATA TRANSMISSION AND USE AGREEMENT BETWEEN WMDA MEMBER ORGANISATIONS

Undersigned Member Organisation of the World Marrow Donor Association ("**WMDA**"), in signing this signature sheet, acknowledges that it has read and understood the contents of the 'Data Transmission and Use Agreement between WMDA Member Organisations v1.0' ("**Agreement**") and declares to be bound by the Agreement whenever it shares Personal Data with another Member Organisation having also signed this signature sheet.

As a result, any transfer of Personal Data between undersigned Member Organisation and any other Member Organisation having also signed this signature sheet, will be governed by the Agreement, including, when applicable, the standard contractual clauses therein contained.

A record of each WMDA Member Organisation having signed this signature sheet is kept by WMDA and available on WMDA Share.

Agreed and signed on 7/19/2020 in Place

JMDP

Address line 1: Hirose2nd Bldg,7F
Address line 2: 3-19,Kandanishikicho, Chiyoda,, Tokyo,1010054,
Postal code: 101-0054
State/Province
Country: JAPAN

On behalf of the organisation:

Name (written out in full): Yoshihisa Kodera
Title: President

Signature:

DocuSigned by:
Yoshihisa Kodera
83A6214211B7493...

Other information necessary in order for the contract to be binding (if any):

Please note that JMDP cannot introduce GRID for the time being.